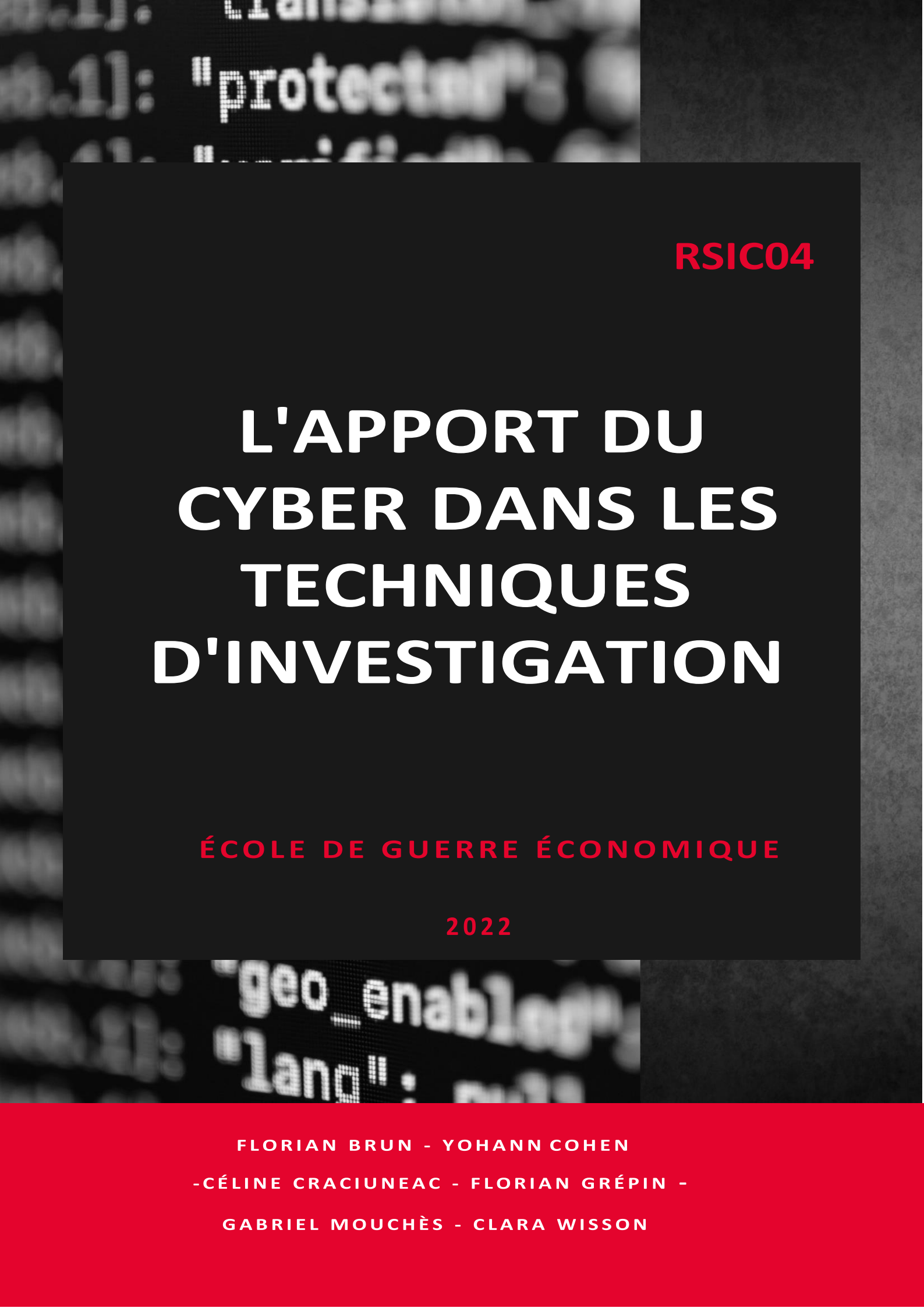


RSIC04

L'APPORT DU CYBER DANS LES TECHNIQUES D'INVESTIGATION

ÉCOLE DE GUERRE ÉCONOMIQUE

2022

FLORIAN BRUN - YOHANN COHEN

-CÉLINE CRACIUNEAC - FLORIAN GRÉPIN -

GABRIEL MOUCHÈS - CLARA WISSON

TABLE DES MATIÈRES

INTRODUCTION
PARTIE 1 - ÉTATS DES LIEUX DES MENACES & MESURES
I. Cybercriminalité, cyber attaques : une notion à géométrie variable
Hausse des attaques à but politiques et lucratives : évolution des menaces
La nécessaire évolution des modes opératoires des services d'investigation
L'action de la France contre la cybercriminalité
1. Fondements juridiques des enquêtes contre la cybercriminalité
2. Les acteurs chargés des investigations dans la lutte contre la cybercriminalité en France
3. Des résultats certains qui doivent encore être prolongés
II. Typologie des groupes criminels & modes opératoires
Les secteurs les plus touchés par les cyberattaques
Groupes cyber criminels principaux & modes opératoires
Cartographie des cyberattaques en temps réel
PARTIE 2 -LE CYBERESPACE &L'INVESTIGATION : OUTIL MULTI-DOMAINE AU SERVICE DEL'ENQUÊTEUR
I. Approche sémantique & méthodologique : l'apport pratique du cyber en investigation
Une approche méthodologique : l'apport pratique du cyber pour l'enquêteur ou l'officier de renseignement
L'investigation cyber : un domaine fragmenté corrélée aux couches de l'espace cyber
La méthodologie de l'enquête numérique et le choix des outils
II. Cyber Threat Intelligence & OSINT
Étude de cas : Focus sur les plans de guerre de Poutine en Ukraine, dévoilés grâce à l'OSINT
Les fondamentaux :
Archivage et documentation pour se prémunir des atrocités
L'importance de la crédibilité et fiabilité
Le CTI au cœur de la guerre en Ukraine
PARTIE 3 - PERSPECTIVES : ÉVOLUTIONS & ANTICIPATION DES NOUVELLES MENACES
I. Les menaces cyber : une menace exponentielle & omniprésente dans le futur
La Géopolitique, génératrice de nouvelles menaces
Le Dark Web : développement d'un marché de menaces au service des cyberattaquants
Nouveau modus operandi des cyberattaquants : Intelligence
Artificielle et Machine Learning au service de nouveaux usages
II. Les scenarios d'anticipation à l'horizon 2030
Les dangers de l'ultra connectivité : l'accélération des échanges et des menaces
Le cloisonnement des réseaux internet : l'émergence et la consolidation des réseaux internet nationaux
La réglementation européenne et internationale : les défis du renforcement réglementaire pour s'adapter aux menaces futures
III. Anticipations & moyens de défense contre les nouvelles menaces cyber
Le renforcement des moyens de défense traditionnels face aux nouvelles menaces
Les défis de la Cyber Threat Intelligence : une capacité de défense renforcée
L'OSINT : moyens de défense juridiquement limité contre les nouvelles menaces
Les infrastructures numériques et l'Union européenne, garants d'une cyberdéfense effective
Le renforcement des infrastructures pour assurer une cyberdéfense performante
Le rôle de l'Union Européenne dans le renforcement de la cyberdéfense face aux nouvelles menaces
L'avenir du facteur humain : « Exploiter le renseignement sur la menace cyber pour sensibiliser et former à la sécurité »
La multiplication du risque humain : cible privilégiée des cybercriminels
La sensibilisation sur les formes de cybercriminalité : moyen d'anticipation contre l'erreur humaine
CONCLUSION & SOURCES

ABBREVIATION

Intelligence-led policing (ILP)
Software As A Service (SAAS)
Technologies de l'Information et de la Communication (TIC)
Systèmes de Traitement Automatisé de Données (S.T.A.D.)
Sous-direction de Lutte contre la Cybercriminalité (SDLC)
Direction Centrale de la Police Judiciaire (DCPJ)
Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication (OCLCTIC)
ICC (investigateurs en cybercriminalité)
Brigade d'Enquête sur les Fraudes aux Technologies de l'Information (BEFTI)
Centre de lutte Contre les Criminalités Numériques (C3N)
Pôle Judiciaire de la Gendarmerie Nationale (PJGN)
Division Criminalistique Ingénierie et Numérique (DCIN)
Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN)
Investigateur en cybercriminalité (ICC)
Direction Générale de la Sécurité Intérieure (DGSI)
Direction Centrale du Renseignement Intérieur (DCRI)
Unité de coordination de la lutte antiterroriste (UCLAT)
Opérateurs d'Importance Vitale (OIV)
Centre d'Analyse en Lutte Informatique Défensive (CALID)
Centre d'Audit de la Sécurité des Systèmes d'Information (CASSI)
Centre des Réserves et de la Préparation Opérationnelle de Cyberdéfense (CRPOC)
Groupement de la Cyberdéfense des Armées (GCA)
Centre de Recherche et d'Analyse du Cyberespace (CRAC)
Direction du Renseignement Militaire (DRM)
Direction Nationale du Renseignement et des Enquêtes Douanières (DNRED)
Service National de Douane Judiciaire (SNDJ)
Agence nationale de la sécurité des systèmes d'information (ANSSI)
Brigade d'Enquêtes sur les Fraudes aux technologies de l'information (BEFTI)
Groupement d'Intérêt Public Action contre la Cybermalveillance (GIP ACYMA)
Advanced Persistent Threat (APT)
Cyber Threat Intelligence (CTI)
OAS (On-Access Scan)
DS (On-Demand Scan)
MAV (Mail Anti-Virus), WAV (Web Anti-Virus)
IDS (Intrusive Detection Scan)
KAS (Kaspersky Anti-Spam)
VUL (Vulnerability Scan)
RMW (Ransomware)
BAD (Botnet Activity.Detection)
Union Internationale des Télécommunications (UTI)
Renseignement d'Origine Cyber (ROC)
Renseignement d'Intérêt Cyber (RIC)
Renseignement d'Origine Source Ouverte (ROSO)
Open Source Intelligence (OSINT)
Social Media Intelligence (SOCMINT)
Partie des Socialistes de la République moldave (PSRM)
Tactiques, techniques et procédures (TTP)
Règlement général sur la Protection des Données (RGPD)
State Cyber Defense Center (SCPC)
Intelligence artificielle (IA)
Machine Learning (ML)
Agence européenne pour la cybersécurité (ENISA)
Supervisory Control and Data Acquisition (SCADA)

INTRODUCTION

Le cyber a pris une place prépondérante dans nos sociétés. Pour rappel, d'après l'Union Internationale des Télécommunications (UTI), près de 4,9 milliards d'individus sont connectés à internet dans le monde en 2021. Ce chiffre suit une courbe exponentielle pour atteindre, en Europe, 82,5 personnes connectées pour 100 habitants[1]. Ce chiffre à lui seul explique l'apparition de l'investigation cyber dans nos sociétés. Pour comprendre ce qu'est l'investigation cyber, il faut d'abord définir ce que l'on entend par cyberespace. Il n'y a pas de définition homogène du cyberespace. Chaque tentative de délimitation de ce milieu découle d'une vision politique du monde et de représentation subjective. L'Occident le considère comme un milieu sans réelles frontières, s'adossant à un système libéral permettant de créer des connexions à travers le monde en toute liberté[2]. A contrario, certains pays utilisent une sémantique bien différente pour définir leur sphère numérique. Ainsi, si l'on prend l'exemple de la Russie, on constate une divergence importante tant en termes de délimitation que de vision de ce milieu. La Russie ne parle pas de cyberespace, mais d'espace informationnel. Il englobe l'ensemble des vecteurs de l'information d'une société. Cette différence de terminologie cache une réalité complexe. La Russie ne reconnaît pas le cyberespace et sa particularité transnationale. Il est un vecteur d'informations comme un autre sur lequel l'État doit pouvoir appliquer des capacités de modération. Le nom donné au cyberespace russe, « Runet », illustre cette vision d'un espace faisant partie à part entière du territoire national.

Ainsi, afin d'obtenir une vision claire et précise de ce qu'est le cyberespace, la définition la plus pertinente semble être celle qui s'attache en premier lieu à définir ce qui compose le cyberespace. Cela permet de s'éloigner de la vision politique qui influence ce milieu. Pour ce faire la définition de Charles Thibout et André Loesekrug-Pietri[3] semble être la plus pertinente.
Ils définissent le cyber espace en trois couches :

- *Sémantique* (les flux d'informations) ;
- *Logique* (protocoles, applications, messageries, réseaux sociaux, etc.) ;
- M*atérielle*, soit les infrastructures primordiales du réseau.

L'investigation est quant à elle est définie par « *la recherche minutieuse, systématiquement poursuivie, sur quelque chose* ».[3] En réalité, les méthodes d'investigation subissent une transformation importante depuis le début des années 1990. Les phénomènes sociaux ont rapidement changé depuis le début du XX^{e} siècle. Alors qu'auparavant les forces de l'ordre devaient constater un délit, en trouver le responsable et le sanctionner puis le réhabiliter, aujourd'hui cette tâche est plus ardue. De nouveaux délits sont apparus avec l'accélération des échanges internationaux, la libération de la parole dans certaines franges de population ainsi que l'accélération de la décomposition sociale. Pour y faire face, un mouvement anglo-saxon a prôné la mise en place d'une investigation proactive intégrant les nouveaux outils à disposition de l'enquêteur. Pour ce faire, les enquêteurs se sont inspirés du monde du renseignement afin de créer l'*intelligence-led policing*[4] (ILP). Ce concept ce base sur une échelle en trois dimensions :

[1] Gaudiaut, Tristan. Infographie : Combien y a-t-il d'internautes dans le monde ? *Statista Infographies* [en ligne]. 2021 [consulté le 30 mai 2022].

[2] Desforges Alix, « Les représentations du cyberespace : un outil géopolitique », *Hérodote*, 2014/1-2 (n° 152153), p. 67-81. DOI : 10.3917/her.152.0067. URL : [3] Diplomatie n°111, Charles Thibout et André Loesekrug-Pietri, La souveraineté numérique : un enjeu majeur pour l'Europe, sept.-oct. 2021

[3] *Définition de l'investigation | Dictionnaire français | La langue française*.

[4] De Maillard, C. (s. d.). *La France et le renseignement criminel : Entre volonté et réalité, une ambition à écrire*. Cairn.info.

- Le renseignement criminel tactique qui doit aider directement à l'investigation ;
- Le renseignement criminel opérationnel qui doit aider à la décision ;
- Le renseignement criminel stratégique qui doit permettre de capitaliser de la connaissance et aider à la compréhension.

La reconstruction du cycle d'enquête s'accompagne de l'utilisation de nouveaux outils et la recherche au travers de nouvelles sources. Ici, celui qui nous intéresse plus particulièrement est l'outil cyber qui peut intervenir sur les trois échelles définies par l'ILP.

Le cyberespace est un domaine qui s'est particulièrement densifié ces vingt dernières années. Il représente une source d'information importante, et ce à plusieurs niveaux. D'une part, le cyberespace peut permettre à l'enquêteur d'appuyer l'investigation sur le terrain en recherchant des informations pouvant permettre l'avancée d'une enquête. Cela doit amener l'enquêteur à amasser des informations sur un suspect, une victime ou une organisation. De plus, le cyberespace est lui-même le théâtre de délit réalisé par ses utilisateurs que l'on nomme cybercriminels. Ces délits peuvent prendre plusieurs formes et toucher les trois couches de l'espace cyber. Ils relèvent d'un certain particularisme de par leurs difficultés d'attribution. En effet, il est particulièrement compliqué d'identifier les cybercriminels. Aujourd'hui, face à la multiplication des menaces et délits, les enquêteurs sont donc dans l'obligation de prendre en compte de nouveaux paramètres, méthodes et outils que peut apport le cyber tant d'un point de vue d'aide à l'enquêteur sur le terrain que de lutte contre la cybercriminalité.

Ainsi, la notion de cyber vient apporter son aide et ses évolutions. Alors, quel est le réel apport du cyber dans les techniques d'investigation actuelles ? Cette étude se divisera en trois parties principales.
Premièrement, un état des lieux sera établi en matière de cybercriminalité, des actions concrètes menées notamment par la France et une typologie non exhaustive des groupes criminels, de leurs modes opératoires ainsi que des outils de cartographie disponibles dans le suivi de ces menaces.
Deuxièmement, les outils transverses au service de l'enquêteur avec une approche tout d'abord sémantique et méthodologique explicitant l'apport pratique du cyber en investigation, l'association de la *Cyber Threat Intelligence* et de l'OSINT au travers d'études de cas. Troisièmement, il sera question des évolutions et de l'anticipation de ces menaces explicitées, avec un focus sur les menaces cyber sur le Dark Web, l'utilisation de l'intelligence artificielle et du Machine Learning. Par ailleurs, les scénarios d'anticipation à l'horizon 2030 permettront de comprendre les nouveaux enjeux à renforcer et quelles réglementations pourront s'avérer efficaces face à ces menaces futures. Celles-ci ouvrent de fait la porte à une volonté d'anticipation et de moyens de défense face à cette cybercriminalité, remettant parfois en cause l'avenir du facteur humain.

Partie 1 : ÉTATS DES LIEUX DES MENACES & MESURES

I. Cybercriminalité, cyberattaques : une notion à géométrie variable

A) Hausse des attaques à but politiques et lucratives : évolution des menaces

La révolution numérique, amorcée dès le milieu du XXème siècle, redéfinit le partage des connaissances et des communications entre les individus, ce qui a provoqué une redéfinition de la notion même de la criminalité[5].

Depuis les années 1990 et 2000, le cyberespace est devenu le théâtre d'attaques au service d'intérêts politiques et économiques. Elles peuvent prendre la forme d'infiltrations sur les réseaux de communication dans le but d'altérer, de prendre le contrôle ou d'espionner ces derniers, voire d'agir sur les opinions publiques au travers de campagnes d'influence en ligne. Ces menaces, visibles et invisibles, directes et indirectes, représentent un coût souvent mal estimé par les autorités, les entreprises et les citoyens.

Lorsque ces pratiques ont un objectif de profit financier, elles prennent généralement la forme d'usurpations d'identités, de détournements de cartes de crédit, de fraude informatique par le crime organisé, au travers de techniques parfois sophistiquées comme l'hameçonnage (*phishing*), l'utilisation de logiciels espions, de virus, de chevaux de Troie, de maliciels, d'outils de dissimulation d'activité, voire de réseaux d'ordinateurs zombies. Si le bénéfice recherché est de nature politique et militaire, les attaques se font plus coordonnées et correspondent au cyberterrorisme ou à la cyberpiraterie d'État, qui visent généralement la mise en danger de réseaux et d'infrastructures vitales, la perturbation des systèmes ou le ralentissement des réseaux, voire le piratage d'applications et le vol d'informations.

Cependant, il convient de noter que la frontière entre les cyberattaques perpétrées par des États et celles pratiquées par des particuliers ou des groupes criminels est de plus en plus floue. En effet, depuis les années 2000, ces pratiques sont en essor continu favorisé par la démocratisation des maliciels, désormais accessibles sous forme de services, à la manière des logiciels légaux vendus sous la forme *software as a service* (SAAS) et la professionnalisation des réseaux cybercriminels[6].

Ainsi, en 2021, l'ANSSI a référencé de 1082 intrusions avérées dans des systèmes d'information, alors que ce chiffre était de 786 en 2020, soit une hausse de 37%. Il convient de relever que ce chiffre exprime les intrusions avérées, et dissimule dans les faits un halo d'attaques non détectées. L'agence note également une "explosion du nombre de vulnérabilités 0-Day[7] exploitées", tant par des acteurs étatiques que par des groupes cybercriminels, la frontière entre ces deux types d'acteurs s'avérant bien souvent poreuse[8].

---

[5] Fortin, Francis et Olivier DELÉMONT. La criminologie de l'information : état des lieux et perspectives. *Criminologie*. 2019.

[6] Caulier, Sophy. Comment les acteurs du cybercrime se professionnalisent. *Le Monde.fr*

[7] Ces failles "du premier jour" sont des vulnérabilités informatiques non-résolues pouvant être facilement utilisée par une partie malveillante pour entrer dans un système d'information.

[8] Panorama de la menace informatique 2021. *CERT-FR - Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques*.

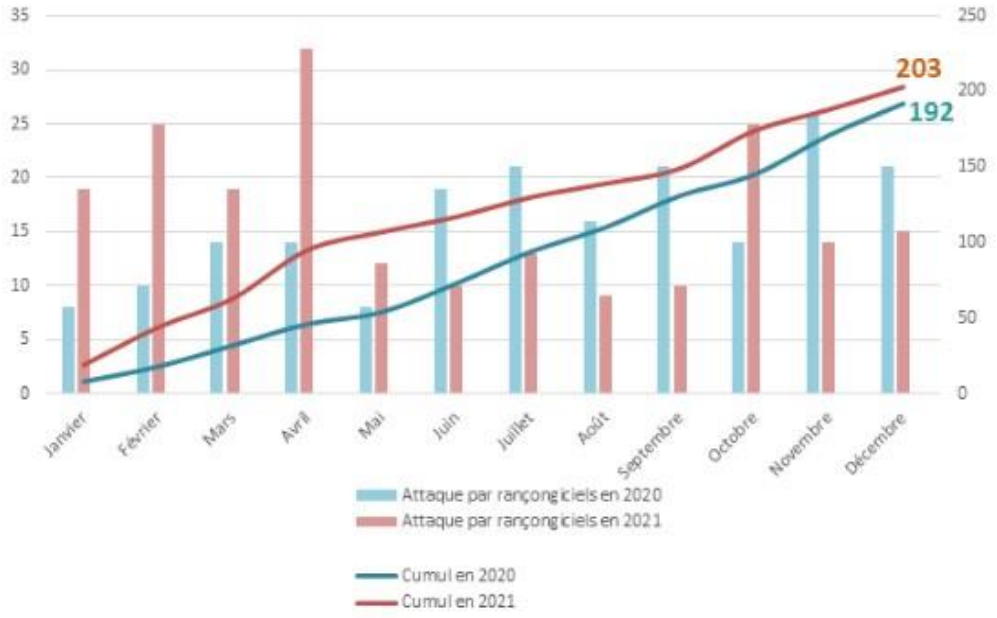


Fig. 1.2. – Statistiques concernant les attaques par rançongiciels traitées par l'ANSSI en 2020 et 2021.

Source : CERT-ANSSI, 2021

Par ailleurs, de nouvelles pratiques émergent également, s'appuyant sur l'ingénierie sociale et l'OSINT, qui facilitent les usurpations d'identité. Ainsi, aux États-Unis, le phénomène du *swatting*, qui consiste à simuler une situation nécessitant l'intervention du SWAT (unités de police d'élite aux États-Unis) pour nuire à une personne, est en augmentation. Bien que peu renseigné et probablement très marginal en France, le *swatting*[9] est puni par l'article 322-14 du Code Pénal, qui interdit : « *le fait de communiquer ou divulguer une fausse information dans le but de faire croire qu'une destruction, dégradation ou détérioration dangereuse pour les personnes va être ou a été commise* ». Ce délit est puni d'une peine pouvant aller jusqu'à deux ans de prison et 30 000 € d'amende.

B) La nécessaire évolution des modes opératoires des services d'investigation

Face aux tendances sociales, technologiques et économiques associées à l'avènement d'Internet et à la mondialisation des échanges, l'exploitation du cyberespace a amené les policiers à adapter leurs méthodes d'investigation[10]. Alors que le cyberespace est fait de flux de données immenses, l'investigateur doit être doté de matériel et de logiciels à même de traiter ces flux[11]. Alors que l'enquêteur pré-cyber devait détenir la capacité d'initier des recherches, de préparer un plan d'enquête, de procéder à l'enquête, de participer aux procédures judiciaires, d'établir et de maintenir des liens de coopération avec le public et les partenaires impliqués dans les événements de son secteur d'activité et de maintenir à jour ses connaissances, l'enquêteur informatique ou cyberenquêteur doit développer des compétences précises liées aux technologies de l'information et de la communication (TIC). Ainsi, ce dernier doit évidemment être familier des dynamiques propres aux TIC, connaître les méthodes d'extraction et de traitement des données numériques, détenir les certifications pertinentes au

[9] Estano, Nicolas. Nouvelles technologies et cyberharcèlement : l'exemple du swatting. *Criminologie*. 2019.
[10] La criminologie de l'information : état des lieux et perspectives – Criminologie. *Érudit*.
[11] Amicelle, Anthony et al. Criminology in the face of flows: reflections on contemporary policing and security. *Global Crime*, 2017.

domaine cyber et maîtriser les conditions pour agir et être reconnu au titre d'expert[12]. Cela exige de la part de l'État de former ses personnels, les formations universitaires accusant le plus souvent un retard par rapport à l'évolution des technologies, ou étant, *a minima,* mal adaptées au travail spécialisé de l'enquêteur informatique, qui ne connaît pas de réel équivalent dans le secteur privé. D'après le Centre International de Criminologie Comparée[13], le profil idoine du cyber enquêteur doit combiner plusieurs critères, dont l'expérience policière, notamment de terrain, une expertise supérieure à la moyenne au niveau informatique ainsi que des connaissances régulièrement rafraîchies et approfondies sur le domaine cyber au travers de formations. Ainsi, pour obtenir la qualité d'investigateur en cybercriminalité au sein de la Police Nationale, un fonctionnaire passe par plusieurs formations, dont celle d'investigateur en cybercriminalité, de primointervenant en cybercriminalité, d'enquêteur sur Internet et les réseaux sociaux et d'enquête sous pseudonyme[14].

C) L'action de la France contre la cybercriminalité

1. Fondements juridiques des enquêtes contre la cybercriminalité

Il convient de distinguer les infractions spécifiques aux technologies de l'information et de la communication des infractions dont la commission est liée ou facilitée par l'utilisation des technologies de l'information et de la communication. La première catégorie comprend les atteintes aux Systèmes de Traitement Automatisé de Données (S.T.A.D.) sanctionnées par les articles L.323-1 et suivants du Code pénal, ainsi que les atteintes aux droits de la personne liés aux fichiers ou traitements informatiques (art. 226-16 à 226-24 du Code pénal et Loi 78-17 du 6 janvier 1978 dite « *informatique et liberté* » modifiée par la loi 2004-801 du 6 août 2004). Les infractions liées ou facilitées par les TIC incluent quant à elles les atteintes aux mineurs (article 227-23 du Code pénal), les infractions à la loi sur la presse (loi du 29 juillet 1881), les atteintes aux personnes, notamment les usurpations d'identités pouvant être associées au phishing selon l'article 226-4-1 du Code Pénal, qui sont punies d'un an d'emprisonnement et de 15 000 € d'amende. Ces infractions incluent également les délits mentionnés à l'article Article 312-1 du Code Pénal, comme le délit d'extorsion ou de tentative d'extorsion (demande d'argent en échange de ne pas supprimer des données ou de ne pas divulguer des secrets volés), qui sont punis de sept ans d'emprisonnement et de 100 000 euros d'amende[15].

2. Les acteurs chargés des investigations dans la lutte contre la cybercriminalité en France

Pour répondre à ces menaces en forte croissance et faire appliquer la loi, la France s'est dotée d'un certain nombre d'entités disposant de capacités d'investigations informatiques. Ce recours au cyber est impératif pour lutter contre la criminalité majoritairement lieu dans le cyberespace, mais est également utile dans le cadre d'investigations sur des faits survenus en dehors du cyberespace. Ainsi, la Sous-direction de Lutte contre la Cybercriminalité (SDLC), service interministériel qui dépend de la Direction Centrale de la Police Judiciaire (DCPJ), a repris les missions de l'Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication (OCLCTIC). On ajoute à celles-ci la plateforme

PHAROS, qui permet de centraliser les signalements ainsi que l'orientation technique et judiciaire[17]. La SDLC enquête sur des infractions comme des piratages, des fraudes aux moyens de paiement ou par téléphonie ainsi que pour des escroqueries sur Internet. Au sein de la Police Nationale, les ICC (investigateurs en cybercriminalité) interviennent sur ces infractions. En 2019, ils étaient 508 réparties

[12] Policier investigateur en cybercriminalité. *Site du ministère de l'Intérieur,* 2017.
[13] Cybercriminalité : mythe ou réalité ? *Centre international de criminologie comparée.* 2017.
[14] Policier investigateur en cybercriminalité. *Page d'accueil | Police nationale*. 2022
[15] En cas d'incident. *ANSSI.*

sur tout le territoire français, dont 19 au sein de la Brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI)[18]. Celle-ci est compétente sur champ couvert par la Préfecture de police de Paris et traite les infractions relatives aux actes de piratage sur Paris et ses trois départements limitrophes (92, 93 et 94)[19].

De même, le Centre de lutte contre les criminalités numériques (C3N) de la Gendarmerie Nationale, service à compétence judiciaire nationale regroupe l'ensemble des unités du Pôle judiciaire de la Gendarmerie Nationale (PJGN). Le C3N assure également l'animation et la coordination au niveau national de l'ensemble des enquêtes menées par le réseau gendarmerie des enquêteurs numériques. Ses unités traitent directement de questions de formation, de veille et de recherche, d'investigation et d'expertise en rapport avec la criminalité et les analyses numériques, notamment au travers du Département Informatique-Électronique de la Division a remplacé en mai 2014 la Direction Centrale du Renseignement Intérieur (DCRI) ainsi que d'autres entités comme l'Unité de coordination de la lutte antiterroriste (UCLAT), poursuit les missions de protection des intérêts fondamentaux de la Nation. La DGSI traite les actes de piratage ciblant les réseaux d'État, les établissements composés de Zones à Régime Restrictif et les Opérateurs d'Importance Vitale (OIV). De la même manière, au sein du ministère des Armées, le COMCYBER dispose d'une chaîne de cyberdéfense au travers du Centre d'analyse en lutte informatique défensive (CALID), du Centre d'audit de la sécurité des systèmes d'information (CASSI), et du Centre des réserves et de la préparation opérationnelle de cyberdéfense (CRPOC). Ces services, qui forment depuis 2020 le Groupement de la cyberdéfense des armées (GCA), intègrent des profils divers comme des techniciens et des ingénieurs, disposant de compétences en rétroconception (*reverse engineering*), en audit et en cybersécurité[16]. Enfin, le Centre de recherche et d'analyse du Cyberespace (CRAC) de la Direction du Renseignement Militaire (DRM) est en mesure de mener des investigations numériques spécialisées, des recherches sur les réseaux sociaux et d'évaluer les systèmes d'armes concurrents[17].

Enfin, la Direction nationale du renseignement et des enquêtes douanières (DNRED) du ministère de l'Économie et de Finance dispose d'un bureau "Cyber douane", au sein du service national de douane judiciaire (SNDJ), qui est spécialisé dans la lutte contre les contrefaçons commercialisées sur Internet. Si sa mission ne relève pas des menaces directement liées au cyberespace, force est de constater que ce dernier est un espace privilégié pour les trafics illégaux et est devenu une plateforme de premier plan pour la contrefaçon.

Au niveau national, la Direction Générale de la Sécurité Intérieure (DGSI) du ministère de l'Intérieur, qui

[16] DEFNET 2021 | la chaîne de cyberdéfense : CALID, CASSI et CRPOC. *Ministère des Armées | ministère des Armées.*

[17] DRM. *Centre Français de Recherche sur le Renseignement.*

[17]Sous-direction de lutte contre la cybercriminalité. Cybersécurité : l'action du ministère en chiffres.

HASSID, Olivier et Christian AGHROUM. *Les entreprises et l'État face aux cybermenaces*. Paris : L'Harmattan, 2013. ISBN 9782343012339.

Criminalistique Ingénierie et Numérique (DCIN) de l'Institut de recherche criminelle de la Gendarmerie nationale (IRCGN). Il traite ainsi les infractions relatives aux atteintes aux STAD ainsi que les infractions visant les personnes et les biens. Au sein de la Gendarmerie Nationale, le cyber enquêteur est appelé NTECH. Il s'agit d'un gendarme spécialement formé à l'enquête en criminalité informatique. Il est l'homologue de l'ICC (investigateur en cybercriminalité) de la Police Nationale. La France compte environ 250 Ntech répartis entre les services de l'IRCGN, le service technique de recherches judiciaires et de documentation, mais aussi les sections et brigades de recherche de la Gendarmerie Nationale.

3. Des résultats certains qui doivent encore être prolongés

La politique de cybersécurité française se caractérise par son volontarisme. En effet, la stratégie nationale de cybersécurité vise à renforcer et structurer la filière cyber de manière à augmenter faire passer son chiffre d'affaires de 7,3 milliards d'euros en 2019 à 25 milliards en 2025, de doubler le nombre d'emplois de la filière pour atteindre 75 000 emplois à la même échéance, tout en soutenant l'émergence de licornes dans le secteur par la concertation avec l'écosystème des startups, notamment le French Tech 120, qui rassemble les plus grandes d'entre elles.

en M€	Développer des solutions souveraines	Renforcer les synergies	Soutenir l'adoption de solutions cyber	Soutien en fonds propres	Total
Part publique	290	74	156	200*	720
Part privée	225	74	20	*n.a.*	>319
Financement	**515**	**148**	**176**	**200**	**>1 039**

* Montants prévisionnel

Source : ANSSI, 2021

Les objectifs fixés sont donc quantitatifs, comme les financements publics d'un montant de 720 millions d'euros pour 2021, mais aussi qualitatifs, puisque la stratégie vise à créer un véritable écosystème de la cybersécurité par des liens entre la R&D privée et la recherche publique, tout en développant une culture de la cybersécurité au sein des entreprises. Le projet de Campus Cyber, inauguré en février 2022, en est l'exemple le plus frappant, puisqu'il rassemble les acteurs publics et privés de la cybersécurité, parmi lesquels l'ANSSI, la Police et la Gendarmerie, de manière à créer un lieu unique mutualisant les activités de veille et d'analyse, de formation et d'innovation[18].

Timeline, la définition du rôle de l'État dans le cyberespace :

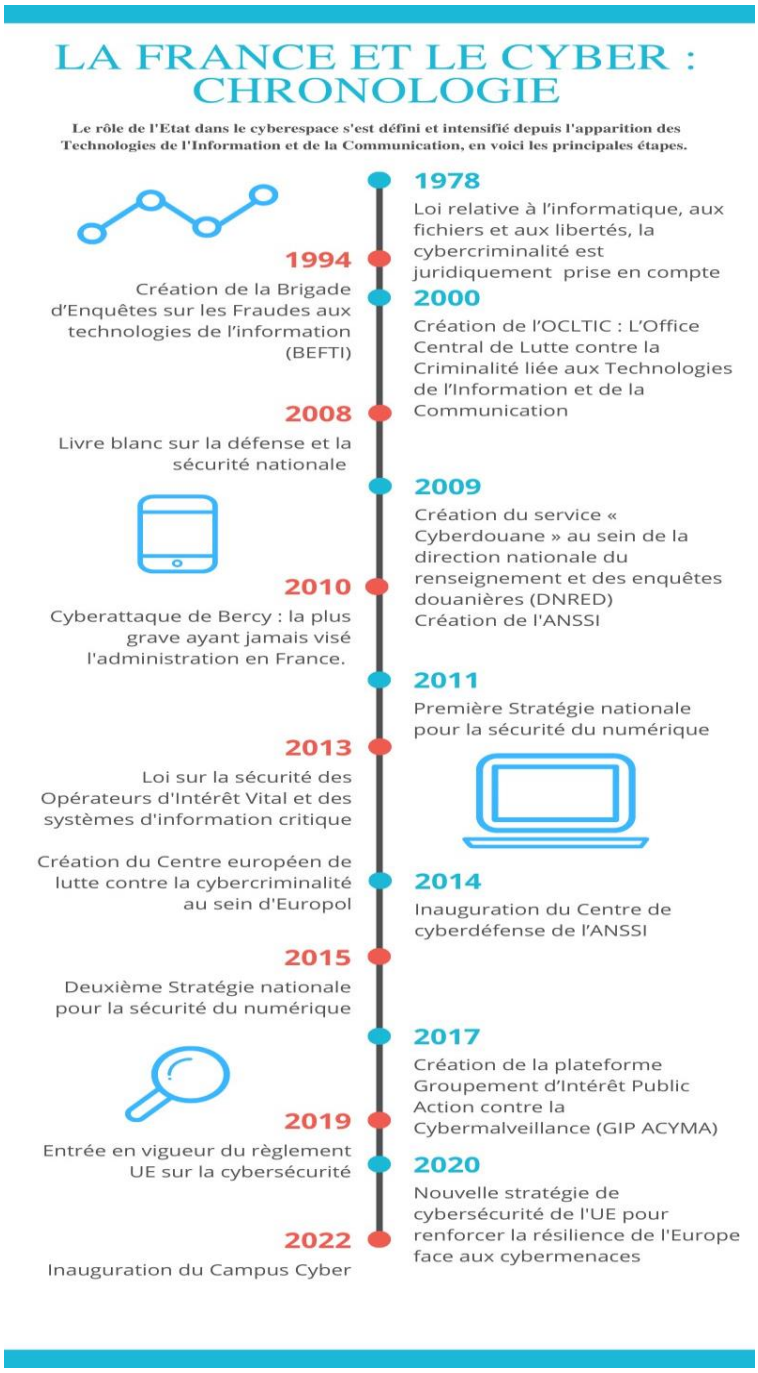
-
- 6 janvier 1978 : loi relative à l'informatique, aux fichiers et aux libertés, cybercriminalité est prise juridiquement en compte
- 1994 : Création de la Brigade d'Enquêtes sur les Fraudes aux technologies de l'information (BEFTI)
- 15 mai 2000 : création de l'OCLTIC : L'Office Central de Lutte contre la Criminalité liée aux
- Technologies de l'Information et de la Communication[19]. • 2008 : Livre blanc sur la défense et la sécurité nationale
- 2008 :
- 2009 : Création du service « Cyberdouane » est constituée de 8 analystes et de 7 personnels au sein de la direction nationale du renseignement et des enquêtes douanières (DNRED)
- Juillet 2009 : Création d'une agence nationale cybersécurité (ANSSI)
- Fin 2010: Cyberattaque de Bercy : la plus grave ayant jamais visé l'administration en France. Elle ciblait plus particulièrement la direction générale du Trésor et les informations confidentielles en lien avec le G20.
- Février 2011 : L'Anssi a déjà vu ses pouvoirs renforcés en février dernier (mais cela n'aurait pas de rapport avec la cyberattaque contre Bercy, selon l'entourage de Christine Lagarde), raccourcissant notamment les circuits décisionnels en cas d'attaque majeure.
- 2011 : 1ère Stratégie nationale pour la sécurité du numérique
- 2013 : Loi sur sécurité des OIV et des SI critiques

[18] Cybersécurité, faire face à la menace : la stratégie française.

[19] Décret n°2000-405 du 15 mai 2000 portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. *Légifrance*.

- 2013 : Création au sein d'Europol, du Centre européen de lutte contre la cybercriminalité, visant à faciliter la coopération entre États européens dans la lutte contre le cybercrime.
- 2013 : ONU reconnaît l'application au cyberespace du droit international
- 2014 : Inauguration du Centre de cyberdéfense de l'ANSSI
- 2015 : 2e Stratégie nationale pour la sécurité du numérique
- 2017 : Création de la plateforme Groupement d'Intérêt Public Action contre la
- Cybermalveillance (GIP ACYMA)[20]
-
- Juin 2019 : Entrée en vigueur du règlement UE sur la cybersécurité, qui a permis d'introduire un schéma de certification au niveau de l'UE tout en renforçant le nouveau mandat de l'Agence de l'UE pour la cybersécurité.
- Décembre 2020 : Commission européenne et le Service européen pour l'action extérieure ont présenté une nouvelle stratégie de cybersécurité de l'UE pour renforcer la résilience de l'Europe face aux cybermenaces[21].

[20] Notre plateforme. *Assistance aux victimes de cybermalveillance*. 2019.
[21] Cybersécurité : comment l'UE lutte contre les cybermenaces. *Home - Consilium* .2022



Infographie réalisée par Gabriel Mouchès

II. Typologie des groupes criminels & modes opératoires

L'arrivée du cyber dans la criminalité a élargi le champ d'action de groupes criminels et a généré de nouvelles menaces en quelques années, ainsi que de nouveaux moyens technologiques et de nouveaux modes opératoires à contrer pour les autorités françaises. La cybercriminalité exige un tout aussi haut niveau d'organisation et reprend les schémas « *classiques* » que l'on connaît en termes de criminalité. Il est donc important de dresser un panorama par la typologie suivante via, dans un premier temps, l'évolution du cyber dans les secteurs les plus touchés par la cybercriminalité ; ensuite, une identification des principaux groupes d'*Advanced Persistent Threat* (APT), de leur origine et mode opératoire ; et enfin les outils de cartographie de ces menaces.

A) Les secteurs les plus touchés par les cyberattaques

Le secteur financier

La cybercriminalité dans le secteur financier a explosé ces dernières années avec des institutions toujours plus fragilisées par ces cyberattaques. Celles-ci voient leur intégrité de plus en plus menacée. L'évolution des méthodes d'attaques oblige les entreprises et institutions à se doter de mesures pérennes et donc développer leur capacité d'analyse de ces menaces. Le secteur est le plus ciblé par les cybercriminels subissant 300 fois plus d'attaques que les autres secteurs selon le rapport Global Wealth 2019 de Boston Consulting Group[22]. Il y a tout juste 10 ans, cette criminalité se comptait déjà en millions de dollars de perte pour des pays tels que les ÉtatsUnis, la Chine ou encore la Turquie.[23] Désormais, elle représenterait une perte de 10% du résultat des banques au niveau mondial, c'est-à-dire 100 milliards de dollars.[24]

Elle touche de près la criminalité classique avec des faits de corruption, de blanchiment d'argent et d'escroquerie utilisant des moyens sophistiqués. À la manière d'une entreprise, les groupes criminels créent leur propre business model en faisant appel à des hackers et ainsi augmenter considérablement leur force d'impact et de revenus. Les outils cyber développés dans le cadre d'investigations permettent désormais de pouvoir identifier les acteurs de cette criminalité financière et d'analyser les signaux faibles laissés par les groupes. Europol dresse chaque année un rapport intitulé *Internet Organised Crime Threat Assessment* dans le but d'apporter une vision large des menaces cyber criminelles existantes et leur impact concret sur chaque secteur.

Dans le secteur financier, ces menaces se constituent de risques de fraude, attaque par déni de service DDoS, de vol de données et de blanchiment via les cryptomonnaies. Dans le cadre de cette lutte contre la cybercriminalité financière, un programme a été créé en 2014 : la *Joint Cybercrime Action Taskforce* par Europol. Son action se base sur le renseignement et la coordination des pays contre ces menaces. Plus généralement, cette taskforce traite de sujets financiers, mais également de pédopornographie en ligne et de crimes transnationaux.

Le secteur technologique

On ne peut plus nier l'évolution technologique aujourd'hui et son intégration dans nos objets du quotidien. Il est prédit par l'institut français IDATEE DigiWorld qu'en 2030, près de 35 milliards d'objets connectés seront utilisés[29], impliquant de fait une montée en puissance de la cyber criminalité. La numérisation des services et industries telles que celle du jeu vidéo ou encore logiciel comporte un niveau de risque considérable au vu des points d'entrées multiples.

Ce développement entraîne inévitablement une menace sur l'industrie, subissant des attaques logicielles ou encore une atteinte à leurs données sensibles et à leur propriété intellectuelle. Par le biais de nouvelles technologies telles que l'IA, développé en fin d'études dans l'aspect prospective de cette

[22] Mercourt, L. (2022, 29 mars). *Les enjeux de la cybersécurité dans les banques et assurances*. Freelance.com.

[23] Bohic, C. (2014, 10 juin). *Sécurité IT : Le poids économique de la cybercriminalité*. ITespresso.fr.

[24] Dubois, M. (2022, 17 février). *Une attaque informatique géante, ce cauchemar redouté par les banques du monde entier*. Ouest France.

[24] Franceinfo & Fayolle, M. (2021, 24 avril). *La santé, nouveau terrain de jeu des pirates informatiques*. Franceinfo.

29 Rioux, P. (2018, 6 février). Internet des objets : 35 milliards d'appareils connectés en 2030 selon l'Institut Idate. ladepeche.fr.

30 Francois, M. (2021, 18 mai). Comment évoluer vers l'industrie 4.0 en se protégeant des cyberattaques.

étude, le secteur technologique et industriel permettra une interconnexion des environnements et des mesures toujours plus strictes, à l'ère de l'industrie 4.0. [30] Il est tout d'abord nécessaire d'implanter le cadre technique avant d'arriver aux outils d'investigation utilisés aujourd'hui et de faciliter la prise en charge des entreprises touchées. En 2021, le secteur industriel fut le plus touché par la cybercriminalité avec une hausse de 641% du nombre d'attaques au dernier trimestre 2021.

Le secteur éducatif

Le secteur de l'éducation est devenu une cible facilement atteignable et stratégique pour les cybercriminels. En effet, la démocratisation de l'apprentissage en ligne, les données à exploiter, l'apport financier ainsi que le manque de sensibilisation à cette problématique, font de ce secteur l'un des plus impactés par la cybercriminalité. La pandémie de Covid n'a fait qu'accroître les menaces cyber sur ce dernier. En effet, il a été nécessaire de rapidement mettre en place de nouveaux moyens pour concevoir l'éducation et se protéger contre des attaques de type ransomwares, principal risque à prendre en compte. Au vu du nombre de terminaux connectés utilisés par universités, écoles, professeurs, élèves, il est très difficile de pouvoir sécuriser l'ensemble au global et ainsi limiter les actions malveillantes. De plus, la sensibilisation est un enjeu clé pour cet acteur puisqu'après une étude menée par la société anglaise Immersive Labs, les attaques par ransomware sont les plus difficiles à gérer par les groupes d'intervention. Ainsi, ce secteur est le plus apte à payer la rançon du fait de l'ascendant psychologique exercé par les cybercriminels, devant les groupes du secteur financier et du gouvernement. Les écoles sont une mine d'or pour les attaquants puisqu'ils peuvent avoir accès à des données touchant à la propriété intellectuelle, à l'intégrité physique et numérique au global, et ont une surface d'attaque si large qu'ils peuvent donc user de nombreux subterfuges pour atteindre leurs objectifs.

Le secteur gouvernemental

Les gouvernements sont une cible privilégiée des cyber attaquants notamment par leur profit financier, mais surtout de par leur visibilité et leur impact. Ainsi, les administrations nationales sont régulièrement attaquées par le biais de moyens classiques tels que le phishing, l'ingénierie sociale ou les ransomwares. En France, on observe en 2020 une augmentation de 50% des attaques contre les collectivités visant les entreprises, administrations ou encore les citoyens.
Dans ce sens, l'ANSSI prévoyait donc un plan de relance de 136M d'euros afin de limiter au maximum l'impact de ces cyberattaques sur ce secteur. Par ailleurs, ces mesures visent à faciliter les investigations et favoriser donc une connaissance mutuelle entre les services et les autorités. Évoqué dans la partie suivante, de nombreux groupes cyber criminels agissent parfois directement sous le contrôle d'un État ou d'un organisme de l'État. Cela rend l'investigation cyber bien plus difficile étant donné les enjeux diplomatiques qui en découlent également. Cependant, comme on peut le constater en ce moment avec le conflit entre la Russie et l'Ukraine, certaines attaques sont directement attribuées à la Russie, lors de la cyber attaque contre le satellite européen Ka-Sat le 24 février dernier, utilisé pour les communications de l'armée ukrainienne.

Le secteur sanitaire

Impactant fortement le système sanitaire et hospitalier, l'arrivée de la Covid-19 a également vu exploser son niveau de cyber attaques, adaptant les mêmes techniques utilisées pour des crimes à visée économique, mais dans ce cas, plus spécialisés dans le vol de données sensibles médicales et pharmaceutiques. Ils peuvent en effet avoir accès à des renseignements médicaux tels que le numéro de sécurité sociale, antécédents médicaux, adresses et tirer profit de la vulnérabilité de la transition digitale du secteur de la santé. S'appuyant également sur une pression psychologique, les criminels sont capables de mettre en danger de mort tout un écosystème hospitalier ou pharmaceutique. Les attaques se font principalement via le phishing, ransomwares ou attaques DDoS . Pour lutter contre ce

phénomène, les équipes d'investigation doivent se doter également d'outils pointus et prioriser ce secteur, dans un monde de plus en plus enclin à subir des pandémies et risques sanitaires. L'industrie pharmaceutique n'est pas en reste puisque certains laboratoires tels que Sanofi, AstraZeneca ou Moderna auraient été infiltrés par les services de renseignement pour en savoir davantage sur les vaccins mis sur le marché, utilisant ainsi les mêmes outils techniques que les cyber criminels, preuve encore de la vulnérabilité technologique de ces industries.[25]

B) Groupes cyber criminels principaux & modes opératoires

Les groupes APT (*Advanced Persistant Threat*) œuvrent la plupart du temps pour des acteurs étatiques (agences de renseignement, composantes militaires) et sont caractérisés par leur haut niveau de planification, coordination, moyens et dangerosité. Dans le cadre de l'identification des menaces cyber actuelles, les principales APT sont donc ici détaillées avec leur origine présumée, les différents modes opératoires utilisés par le groupe ainsi que leurs cibles. Principalement, les groupes du tableau établi ci-dessous proviennent de Chine et sont spécialisés dans le vol de données et de propriété intellectuelle principalement. Plus de 150 APT existent et ont été identifiées notamment par Mandiant dès 2013. Ces investigations cyber s'inscrivant dans la CTI ont permis de dresser un état des lieux des groupes actifs dans le cyberespace et de pouvoir ainsi agir en conséquence avec la mise en place d'outils d'investigation et de détections avancés.

Groupe	Origine probable	Mode opératoire & Cible
APT39	Iran	Dimension internationale, mais ses activités restent concentrées au MoyenOrient. Vol généralisé de données personnelles en utilisant les backdoors Seaweed, Cachemoney & Powbat Cible : secteur des télécommunications, industrie touristique, secteur technologique *Malwares* associés : Seaweed, Cachemoney, Powbat

APT38	Corée du Nord	Cyber espionnage, intelligence économique, partages de *malwares* avec Lazarus Group Utilisation de backdoors, DataMiners, *malwares*, etc. Ciblage précis des cibles, principalement financières : collecte d'informations, compromis, reconnaissance, pivot vers les serveurs SWIFT, transfert de fonds et destructions des preuves *Malwares* associés : Backdoors, Dataminers, etc.
APT37 **Scarcruft** **Group123**	Corée du Nord	Accès aux vulnérabilités 0-day, *malwares* Ingénierie sociale Cibles géographiques : Corée du Sud, Japon, Vietnam, Moyen-Orient Industries visées : industrie chimique, automobile, aérospatiale
APT35 (Newscaster Team)	Iran	Moyens complexes en termes d'ingénierie sociale Utilisation de spearphishing et *malwares* Cibles géographiques : ÉtatsUnis & Europe occidentale Le groupe vise le personnel militaire, diplomatique, les industries de l'énergie et la défense *Malwares* associés : Aspxshellsv, Brokeyolk, Pupyrat, Tunna,

		Mangopunch, Drubot, Houseblend
APT34 (OilRig)	Iran	Cyber espionnage, Malwares, Concentré sur les pays du Moyen-Orient Industries cibles : Télécommunications, énergie, chimique, finance *Malwares* associés : Powbat, Powruner, Bondupdater
APT33	Iran	Spearfishing, ingénierie sociale Cibles géographiques : ÉtatsUnis, Corée du Sud, Arabie Saoudite Industries cibles : aérospatial & énergie *Malwares* associés : Shapeshift, Dropshot, Turnedup, Nanocore, Netwire, Alfa She ll
APT32 Group) (Ocean Lotus	Vietnam	Cyber espionnage, espionnage industriel, Ingénierie sociale Cibles : entreprises étrangères implantées au Vietnam *Malwares* associés : Komprogo, Beacon, Phoreal, Soundbite, Windshield
APT41	Chine	Cyber espionnage parrainé par l'État chinois, spearfishing, malwares, compromission de systèmes Motivation financière

		14 pays ciblés depuis 2012 Industries cibles : haute technologie, télécommunications, vol de propriété intellectuelle, monnaies virtuelles, jeux vidéo *Malwares* associés : 46 familles de codes et outils différents
APT40	Chine	Cyber espionnage, spearfishing, malwares Cible principalement les pays impliqués dans la Nouvelle Route de la Soie Industries cibles : aviation, produits chimiques, Gouvernements, technologique *Malwares* associés : 51 Familles de codes différents
APT31	Chine	Cyber espionnage, renseignement stratégique politique, économique et militaire Exploitation de vulnérabilités Industries cibles : gouvernements, financier, défense, technologie, ingénierie, télécommunications, médias *Malwares* associés : Sogu, Luckybird, Slowgyro, Duckfat
APT30	Chine	Cyber espionnage

		Enregistrement de domaines DNS pour activités CnC malveillantes Existant depuis 2005 Cibles géographiques : membres de l'Association des nations de l'Asie du SudEst (ASEAN) *Malware* associés : Shipshape, Spaceship, Flashfood
APT28 (Tsar Team, Fancy Bear, Sofacy Group, Pawn Storm)	Gouvernement russe Lien probable avec le GRU	Cyber espionnage, renseignement stratégique Backdoors, malwares Cibles : OTAN, Maison Blanche, TV5Monde, pays de l'Europe de l'Est, Géorgie, Caucase et organisations de défense européennes *Malwares* associés : Chopstick, Eviltoss Sourface,
APT27	Chine	Vol de propriété intellectuelle, spearphishing, hameçonnage, exploitation de vulnérabilités Cibles géographiques : Amérique du Nord et Sud, Europe, Moyen-Orient Industries cibles : haute technologie, aérospatiale, transports *Malwares* associés : Pandora, Sogu, Zxshell, Ghost, Wideberth, Quickpulse, Flowerpot

APT26	Chine	Vol de propriété intellectuelle, malware, backdoors Industries cibles : aérospatiale, défense, énergie *Malwares* associés : Sogu, Htran, Postsize, Twochains, Beacon
APT25 (Uncool, Vixen Panda, Ke3chang, Sushi Roll, Tor)	Chine	Vol de données, spearphishing Industries cibles : défense, médias, finance et transport. Cibles géographiques : ÉtatsUnis et Europe. *Malwares* associés : Lingbo, Playwork, Madwofl, Mirage, Toughrow, Toysnake, Sabertooth
APT24 (PittyTiger)	Chine	Vol de données à caractère politique, hameçonnage, vol de propriété intellectuelle Industries cibles : gouvernements, santé, ingénierie, mins, ONG, télécommunications Cibles géographiques : ÉtatsUnis, Taïwan *Malwares* associés : Pittytiger, Enfal, Taidoor

APT23	Chine	Vol de données à caractère politique et militaire, phishing Cibles : gouvernements et médias aux États-Unis et Philippines

		Malwares associés : Nongmin
APT22 (Barista)	Chine	Intrusions, malwares, exploitation de vulnérabilités sur serveurs web Cibles : entités politiques, militaires et économiques. Cibles géographiques : Asie de l'Est, Europe, États-Unis *Malwares* associés : Pisces, Sogu, Flatnote, Angrybell, Baseless, Seawolf, Logjam
APT21 (Zhenbao)	Chine	Ingénierie sociale en langue russe, informations stratégiques en ce qui concerne la sécurité de l'État en Russie, malwares, spearfishing, backdoors. Cible : gouvernements, groupes dissidents. *Malwares* associés : Sogu, Tempfun, Gh0st, Travelnet, Homeunix, Zerotwo

APT20 (Twivy)	Chine	Vol de données, vol de propriété intellectuelle Surveillance des personnes avec intérêts politiques ciblés (abordant les sujets de démocratie, liberté de la presse, minorités ethniques, etc.) Industries cibles : santé, ONG, défense, production chimique *Malwares* associés : Qiac, Sogu, Gh0st, Zxshell, Poison
		Ivy, Beacon, Homeunix, Stew
APT19 (Codoso Team)	Chine	Cyber espionnage, phishing, exploitation de la vulnérabilité Microsoft Windows 2017-0199 Industries cibles : investissement et juridique *Malwares* associés : Beacon, Cobaltstrike
APT18 (Wekby)	Chine	Exploitation vulnérabilité CVE-2015-5119, cyber espionnage Industries cibles : aérospatiale, ingénierie, éducation, santé, haute technologie, télécommunications, transports *Malwares* associés : Gh0st RAT

APT17 (Tailgator Team, Deputy Dog)	Chine	Cyber espionnage, intrusions reseaux Industries cibles : gouvernement américain, cabinets d'avocats internationaux, technologique Cible géographique : États-Unis *Malwares* associés : Blackcoffee, CnC
APT16	Chine	Cyber espionnage, spearphishing, ingénierie sociale
		Industries cibles : organisations japonaises et taïwanaises, hautes technologies *Malwares* associés : Ironhalo, Elmer
APT15	Chine	Cyber espionnage, spearphishing Industries cibles : commerce, finance, énergie *Malwares* associés : Enfal, Baldeagle, Noisemaker, Mirage
APT14	Chine	Vol de données à caractère militaire & maritime Industries cibles : télécommunications, gouvernements, ingénierie *Malwares* associés : Gh0st, Poisonivy, Clubseat, Groovy

APT12 (Calc Team)	Chine	Cyber espionnage en lien supposé avec l'Armée populaire de libération chinoise, ingénierie sociale, hameçonnage Cibles : journalistes, gouvernements, défense *Malwares* associés : Riptide, Hightide, Threbyte, Waterspout,
APT10 (Menupass Team)	Chine	Cyber espionnage, renseignement militaire, vol de données commerciales confidentielles, spearphishing, intrusions

		Industries cibles : construction, ingénierie, aérospatiale, télécommunications, gouvernements Cibles géographiques : ÉtatsUnis, Europe, Japon *Malwares* associés : Haymaker, Snugride, Bugjuice, Quasarrat
APT9	Potentiellement Chine	Vol de données, spearphishing Industries cibles : pharmaceutique, biotechnologique, aérospatiale, défense *Malwares* associés : Sogu, Homeunix, Photo, Funrun, Gh0st, Zxshel

APT8	Chine	Vol de propriété intellectuelle, spearphishing Cibles géographiques : États-Unis, Europe, Inde, Japon *Malwares* associés : Hash, Flyzap, Golfpro, Safeputt
APT7	Chine	Vol de propriété intellectuelle Industries cibles : construction, ingénierie, aérospatiale, défense Cibles géographiques : ÉtatsUnis, Royaume-Uni *Malwares* associés : Digdug, Tracks

APT6	Chine	Vol de données, backdoors Industries cibles : construction, ingénierie, télécommunications Cibles géographiques : ÉtatsUnis, Royaume-Uni *Malwares* associés : Beluga, Exchain, Puptent

APT5	Chine	Vol de données à caractère militaire Composé de sous-groupes avec modes opératoires parfois distincts Industries cibles : télécommunications, technologique *Malwares* associés : Brightcrest, Sweetcola, Spiritbox, Palejab, Widerim, Winvault, Happysad, Birdworld, Farcy, Cyfree, Fullsilo, Hellotheworld, Hazelnut, Gif89a, Screenbind, Shinyfur, Truckbed, Leouncia, Frees
APT4 (Maverick Panda, Sykipot Group, Wisp)	Chine	Intrusions, hameçonnage en lien avec les thèmes du gouvernement américain Industries cibles : aérospatiale, défense, automobile, gouvernements, télécommunications, transports *Malwares* associés : Getkys, Lifesaver, Cchip, Shylilt, Sweettooth, Photo, Sogo

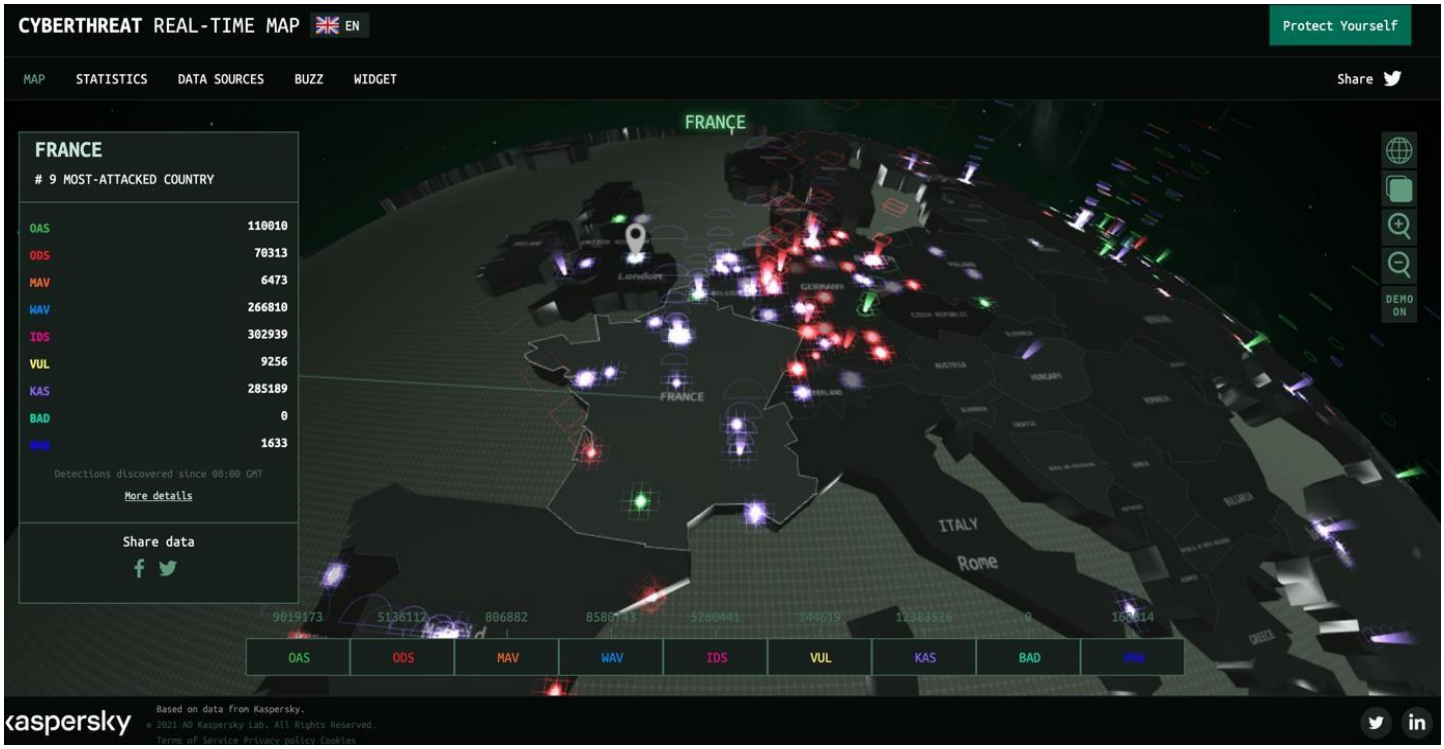
APT3 (UPS Team)	Chine	Cyber espionnage, exploitation de vulnérabilités 0-day, hameçonnage Industries cibles : aérospatiale, construction, télécommunications, transports *Malwares* associés : Shotput, Sogu, Cookiecutter
APT2	Chine	Vol de propriété intellectuelle, spearfishing Industries cibles : militaire et aérospatial *Malwares* associés : Moose, Warp
APT1 (Unité Comment 61398, Crew)	Chine	Attribué au 3ème département du département d'état-major de l'Armée populaire de libération de la Chine Vol de données, compromission d'organisations, spearphishing, ingénierie sociale, faux profils Industries cibles : défense, télécommunications, satellites, énergie, transport, construction, navigation, produits chimiques, santé, éducation, etc. *Malwares* associés : backdoors, Dalbot, Barkiofork, Trojan Ecltys, Revird, Badname, Wualess
Lazarus Group	Corée du Nord	Cyber espionnage, cryptolocker, infiltration, attaque Wannacry, etc.

		Cible : institutions financières

Typologie réalisée grâces aux sources suivantes : Mandiant[38] et le magazine Diplomatie[39]

C) Cartographie des cyberattaques en temps réel

Différents outils en sources ouvertes permettent aux investigateurs de suivre en temps réel les nombreuses attaques cyber. On compte notamment la carte interactive du cabinet russe Kaspersky. Celle-ci fournit des statistiques détaillées sur différentes données, à savoir : OAS (On-Access Scan), ODS (On-Demand Scan), MAV (Mail Anti-Virus), WAV (Web Anti-Virus), IDS (Intrusive Detection Scan), KAS (Kaspersky Anti-Spam), VUL (Vulnerability Scan), RMW (Ransomware), BAD (Botnet Activity.Detection).



40

[38] Mandiant. *Advanced persistent threats (apts) | threat actors & ; groups*.

[39] Berthier, T. (2019). Cybercriminalité : Le choix des armes. *Diplomatie - Les grands dossiers*, (52), 72.

[40] *MAP | kaspersky cyberthreat real-time map*. MAP | Kaspersky Cyberthreat real-time map. Il existe également une carte dédiée à la menace liée aux botnets avec les pays les plus touchés et les entreprises, développée par le Spamhaus Project.

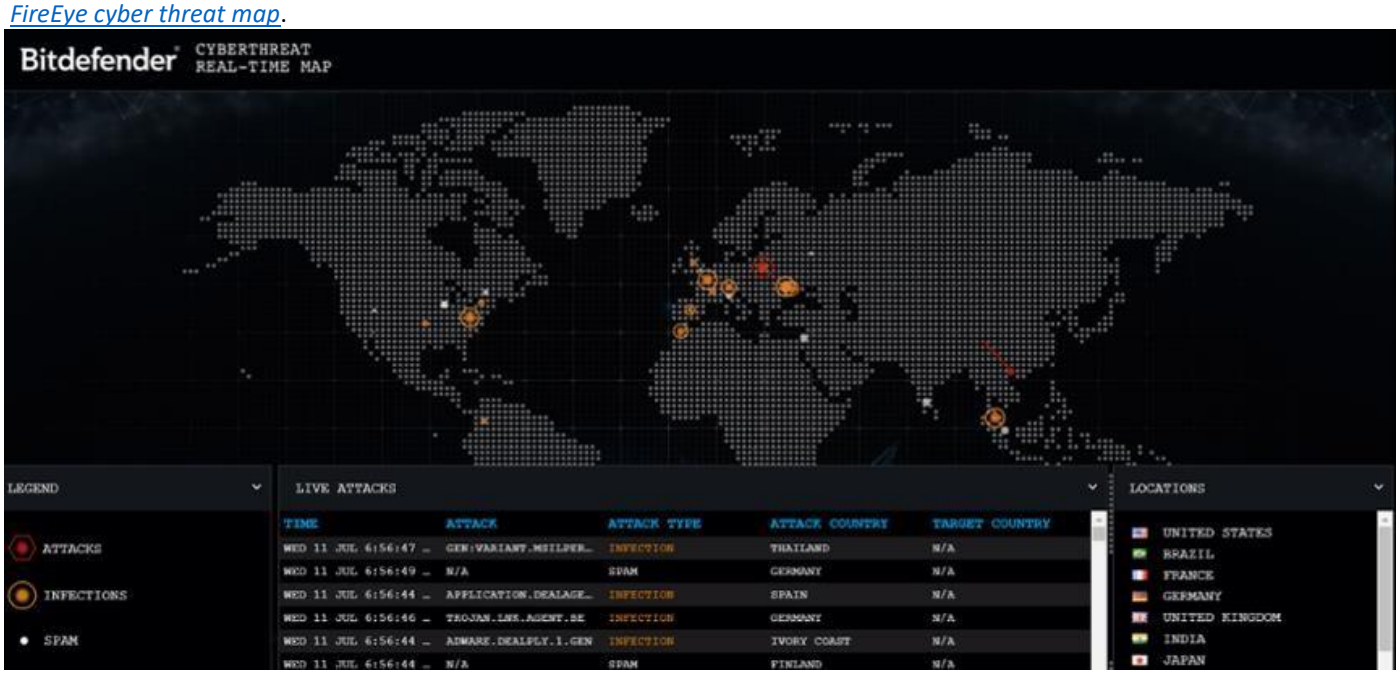
41

Par ailleurs, on peut aussi relever d'autres outils de cartographie en temps réel fournis par FireEye, BitDefender, SonicWall ou encore Threatbutt :

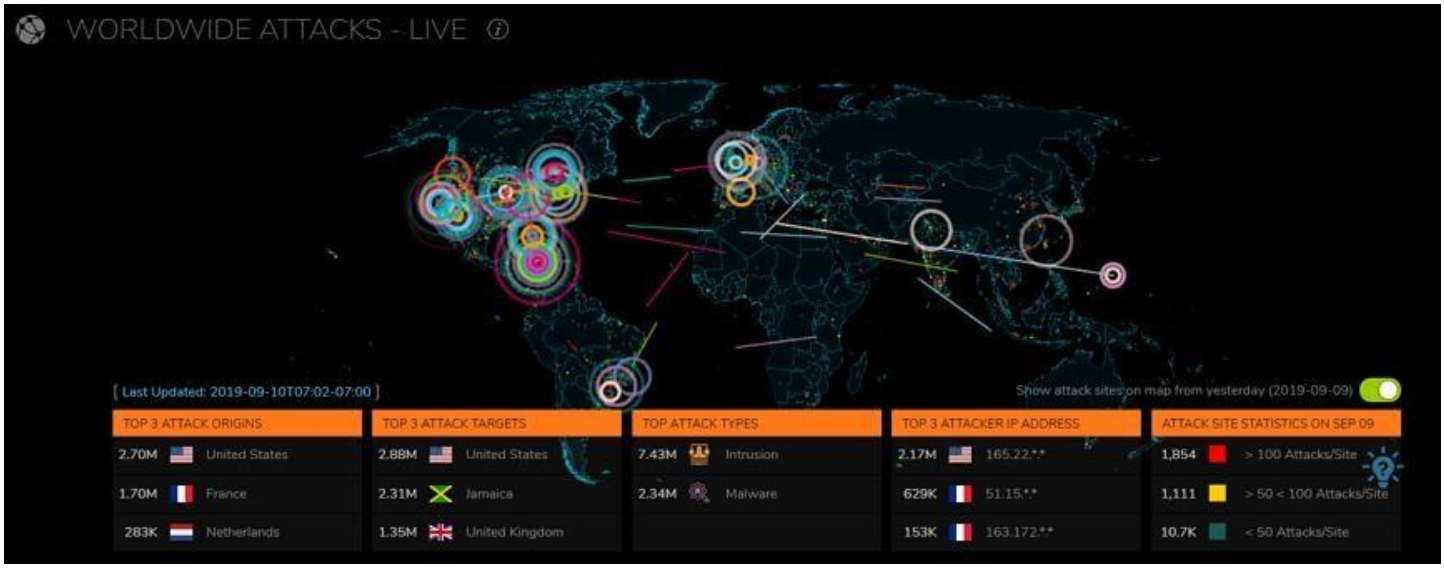
42

[41] *Live threat map*. (s. d.). Deteque.

[42] *FireEye cyber threat map*.



[43]



[43] *Threat map*. BitDefender.

[44] *Worlwide attacks map*. SonicWall Security Center.

[45] *Threatbutt internet hacking attack attribution map*. Threatbutt, comprehensive internet hacking protections.

28

45

Ainsi, ces cartographies un réel atout et un apport sur les investigations cyber aujourd'hui. Il est bien plus évident d'attribuer, de connaître et de se défense contre les groupes APT évoqués précédemment. On note notamment sur la carte de Kaspersky, que la Russie est en première ligne et numéro 1 dans leur classement des pays les plus touchés par les cyberattaques aujourd'hui. Nul doute que la situation actuelle n'accentue ce phénomène qui peut être étudié au travers de divers outils au service de l'enquêteur.

Partie 2 : Le cyberespace et l'investigation : outil multi-domaine au service de l'enquêteur

I. Une approche sémantique & méthodologique : l'apport pratique du cyber en investigation

A. L'investigation cyber : un domaine fragmenté corrélé aux couches de l'espace cyber

Le cyberespace représente une nouvelle source de capitalisation de la connaissance au sein des différentes institutions publiques[26] et journalistiques. Cependant, il est important d'identifier et de bien différencier les méthodes existantes d'enquête dans ce domaine. Les décompositions possibles sont plurielles et aucune nomenclature homogène officielle ne fait pour l'heure loi. Il est cependant possible de diviser les méthodes d'enquêtes en deux grandes catégories qui comprennent, elles-mêmes, plusieurs corps de métiers : le renseignement d'origine cyber (ROC), le renseignement d'intérêt cyber (RIC). Chaque méthode est spécialisée sur une couche précise du cyberespace. En effet, le cyberespace est défini par l'ANSSI comme
« *l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérisées »*[27]. Comme vu précédemment, cet espace est caractérisé par un système décomposé en trois couches[28] :

- La couche informationnelle correspond aux données qui transitent dans le cyberespace[49].
- La couche logicielle représente l'ensemble des programmes qui permettent la mise en place et la continuité du cyberespace[29].
- La couche physique représente l'ensemble des infrastructures physiques nécessaires à la mise en place et l'exploitation des données sur le cyberespace (serveur, ordinateur, DNS, fibre…)[30].

C'est en réalité réducteur d'affirmer que chaque couche cyber possède sa forme d'investigation à part entière. La frontière entre chaque couche peut être poreuse, et ce, plus particulièrement pour la couche informationnelle et logicielle.
Il est important de comprendre, avant de détailler le fonctionnement opérationnel des différents types d'investigation, que les informations liées aux pratiques réalisées par les administrations françaises sont floues. S'il est possible que certaines entités publiques exploitent des données non libres d'accès, il est impossible pour le moment de confirmer cette hypothèse. Le développement sera donc focalisé sur ce qui est nommé Renseignement d'Origine Source Ouverte (ROSO). Le ROSO, ou *Open Source Intelligence* (OSINT), est lui-même sujet à plusieurs définitions. Celle donnée par Jérôme Poirot représente un bon

[26] Renseignements (DRSD, DRPP, DRM, DGSI, DGSE…) et de maintien de l'ordre (gendarmerie, police).

[27] Gagner les cyberconflits. Au-delà du technique - François-Bernard Huyghe, Olivier Kempf, Nicolas Mazzucchi. Decitre.fr.septembre 2015.

[28] Vers un « Runet souverain » ? Perspectives et limites de la stratég... OpenEdition Journals [en ligne]. 25 juin 2021 [consulté le 4 juin 2022]. Disponible sur : https://journals.openedition.org/echogeo/21804#bibliography [49]Plus précisément, Frédérick Douzet défini la couche informationnelle comme « *celle des utilisateurs, des discussions et des échanges en temps réel à travers le monde, la plus difficile à appréhender et représenter d'un point de vue géographique.* » - DOUZET, Frédérick. « *La géopolitique pour comprendre le cyberespace* », *Hérodote*, vol. 152-153, no. 1-2, 2014, pp. 3-21.

[29] Plus précisément, Frédérick Douzet défini la couche logicielle comme l'ensemble des « *programmes informatiques conviviaux permettant à tout un chacun d'utiliser l'Internet sans rien connaître à la programmation informatique (Web, e-mail, réseaux sociaux, moteurs de recherche, etc.)* » - DOUZET, Frédérick. « La géopolitique pour comprendre le cyberespace », *Hérodote*, vol. 152-153, no. 1-2, 2014, pp. 3-21.

[30] Plus précisément, Frédérick Douzet défini la couche physique comme un *« ensemble de matériels installés sur le territoire, soumis aux contraintes de la géographie physique et politique, que l'on peut construire, modifier ou détruire, connecter ou déconnecter du réseau.* ». Douzet, Frédérick. « *La géopolitique pour comprendre le cyberespace* », *Hérodote*, vol. 152-153, no. 1-2, 2014, pp. 3-21.

compromis : « le *ROSO désigne le renseignement d'origine sources ouvertes, OSINT en anglais, pour Open Sources Intelligence. Le renseignement de source ouverte est celui qui est accessible, gratuitement ou non, parce que la personne ou l'institution qui le détient le met à disposition du public* »[31].

Dans ce cadre, le renseignement d'origine cyber s'attache à exploiter les données accessibles en source ouverte afin de créer de la connaissance. Il peut aussi bien être utilisé dans le cadre d'une enquête criminelle que dans celui d'une note de renseignement, l'une n'étant pas forcément exclusive de l'autre. L'intégration du ROC dans la méthodologie de l'enquête commence dès les années 1990, mais est réellement intégrée au renseignement après 2007[32]. Ce sont les États-Unis qui s'emparent de la question en premier avec la publication du *Congressional Research Service* en 2007[53]. Ce rapport pose la question de la place du ROC dans l'architecture du renseignement américain alors que l'on observe une densification rapide des données accessibles sur internet. Aujourd'hui, en France ce type de renseignement est aussi bien présent au sein des services de renseignement[54] que dans les services de forces de l'ordre comme la gendarmerie[55].

On distingue trois types de renseignements d'origine cyber s'appuyant sur les données accessibles en source ouverte :

- La *Due diligence* : elle consiste à étudier l'ensemble des activités d'une entreprise[33] afin d'y déceler de potentielles irrégularités. Cette pratique est issue du monde financier et est principalement réalisée avant une fusion/acquisition. Cependant, on constate depuis quelques années une démocratisation de cette méthode qui peut aujourd'hui venir aider l'enquêteur ou l'officier de recherche. De nombreuses données concernant les entreprises sont en libre accès sur internet, et ce, du nom des propriétaires jusqu'au nombre d'employés ou le niveau d'endettement. Lors d'une enquête, ces informations peuvent se révéler précieuses et permettent d'illustrer des anomalies ou identifier des entreprises stratégiques. La *Due Dilligence* en ROC s'est révélée particulièrement efficace lors de l'enquête menée par les journalistes d'investigation de *Rise.md*. Les journalistes d'investigation ont pu identifier des liens entre Igor Dogon, ex-président moldave et la Fédération de Russie grâce à l'étude des flux financiers des entreprises de Télécoms entourant l'ex-président et le Partie des Socialistes de la République moldave (PSRM)[34].

- L'empreinte numérique : Kaspersky définit l'empreinte numérique comme « *les données que vous laissez derrière vous quand vous utilisez Internet. Ces données comprennent les sites Web visités, les emails que vous envoyez et les informations que*
- *vous soumettez en ligne. Une empreinte numérique peut être utilisée pour suivre les activités en ligne et les appareils d'une personne.* »[35]. On distingue en réalité l'empreinte numérique active et l'empreinte numérique passive. o La première comprend les informations diffusées

[31] Jérôme Poirot, « ROSO ». dans *: Hugues Moutouh éd., Dictionnaire du renseignement*. Paris, Perrin, « Hors collection », 2018.

[32] Annual Report of The Congressional Research Service 2007.

[54] Voir partie I.1. [55] Ibid.

[33] L'étude peut se faire sur plusieurs indicateurs : le capital, le conseil d'administration, les employés, les emprunts, les relations de l'entreprise, les missions réalisées…

[34] Igor Dodon. *Rise Moldova*.

[35] Qu'est-ce qu'une empreinte numérique et comment la protéger des hackers ? www.kaspersky.

délibérément par une personne (photos, messages, réactions, liste d'amis…) o La seconde comprend les données nécessaires à une activité sur internet (adresse IP, identifiant réseaux sociaux, points entrés wifi…).
Ce type d'enquête est particulièrement intéressante pour les institutions. Elles permettent de suivre l'activité réelle grâce au numérique d'individus d'intérêt. Il est ainsi possible d'identifier la localisation, les liens amicaux ou les activités réalisées par une personne. L'empreinte numérique peut aussi se destiner à une emprise géographique. Elle peut prendre la forme d'une entreprise, d'une base militaire… Elle permet d'identifier les limites des emprises géographiques, les infrastructures ou encore les personnes qui sont liées à ces emprises.

- La SOCMINT[36] (Social Media Intelligence) ou opérations d'identification de réseaux d'influence : La multiplication des canaux de communication a été accentuée par la création de réseaux sociaux. Cette multiplication des canaux est corrélée à une utilisation grandissante des journaux en ligne ou des réseaux sociaux à des fins d'influence. Le rôle de l'enquêteur est de décomposer les différents narratifs[37] existant en ligne afin d'identifier l'origine du narratif, l'organisme qui se trouve derrière celuici et le public visé. Cela permet de caractériser l'objectif du narratif en fonction du demandeur. Cette analyse peut se faire par une étude des réseaux sociaux combinées à l'étude de *pure players*[38]. Il faut corréler ces canaux avec l'étude des éléments techniques[39] tels que les noms de domaines[40] et les serveurs[41]. Ainsi, il a été possible pour l'association *Open Facto* de relier le journal en ligne *Inforos* dépendant du GRU russe à environ 1300 sites d'informations en place sur le territoire russe[42]. L'étude n'a pas été réalisée, mais en observant sur quel médias sociaux les articles d'*Inforos* sont diffusés, il serait possible de recréer la sphère d'influence visée par le GRU.

Si on distingue trois opérations d'enquête possible en renseignement d'origine cyber, cela ne signifie pas que chaque opération est indépendante l'une de l'autre. Une *Due Diligence* peut déboucher sur l'empreinte numérique d'un membre du conseil d'administration de l'entreprise et inversement.

À contre-pied, le renseignement d'intérêt cyber, ou *cyber threat intelligence*[43], s'intéresse à l'espace cyber pour les informations qu'il peut mobiliser. L'objectif du RIC est de réaliser une investigation sur les systèmes numériques. Il existe aujourd'hui trois grandes branches de la CTI :

- Le premier axe de la CTI s'attelle à connaître les matériels numériques existants utilisés.

[36] Omand, David, Jamie Bartlett et Carl Miller. Introducing Social Media Intelligence (SOCMINT). Intelligence and National Security, 2012.
[37] D'après le Robert, un narratif est défini comme suit : « *qui relève de la* narration*, du récit* ». Dans le cadre de l'influence, un narratif est une idée transmise dans le cadre d'une stratégie d'influence. Un exemple type : « *les français sont une force d'occupation au Mali* ».
[38] Un *pure player* est un commerçant proposant un service exclusivement en ligne. Dans ce contexte précis, cela désigne les journaux exclusivement en ligne.
[39] Les éléments techniques sont les éléments non physiques reliées à une personne (numéro de téléphone, adresse mail, adresse IP…).
[40] Le nom de domaine correspond à l'URL d'un site web.
[41] Les serveurs sont des dispositifs informatiques qui offrent des services : stockage, accès aux informations du web, base de données.
[42] Rapport – La galaxie des sites russophones du GRU | OpenFacto. *OpenFacto | Association francophone Spécialisée Enquêtes en Sources Ouvertes,* 19 janvier 2022.
[43] Cyber Threat Intelligence. Thales Group.

- L'objectif est de déterminer, selon le type de matériel quelles sont les failles existantes. Cela peut se faire de deux manières différentes. Il est possible de rechercher les défauts et pannes liées à l'appareil en lançant de manière non ciblée des tests afin d'identifier les points de faiblesse existants ou alors rechercher des vulnérabilités au travers de failles. L'objectif est d'identifier des indicateurs de compromission (IoC)[44] avec pour objectif de capitaliser les failles existantes sur un panorama de matériels.
- Le second axe nommé *cyber forensic*[45] consiste à étudier les *malwares*. Il s'agit donc de récupérer et d'étudier les supports numériques corrompus afin d'analyser la donnée et de déterminer quelle faille exploite un *malware.* Il existe deux approches de la *cyber forensic* :
    - L'analyse à froid (*dead forensic*)[46] consiste à créer une réplique du système corrompu en copiant le disque dur sur un support externe. Cela permet d'analyser un *malware* en profondeur sans risquer de corrompre de nouvelles données.
    - L'analyse à chaud (*live forensic*)[70] consiste à analyser un système qui est toujours en cours de fonctionnement. Cette méthode comporte des risques pour le système puisque la poursuite du fonctionnement du système permet au virus de continuer à corrompre des données. Cependant, elle représente aussi un avantage certain. Éteindre le système pour mettre en place une analyse à froid entraîne la suppression des données volatiles qui étaient en cours de fonctionnement. Ces données peuvent représenter des failles invisibles pour l'analyse si la *dead forensic* est privilégiée.

- Le dernier axe d'enquête possible en RIC est la rétro-ingénierie (*reverse engineering*).
- L'objectif est ici de décortiquer les systèmes afin d'en comprendre leurs fonctionnements. Il existe deux types de rétro-ingénierie :
    - L'étude de la couche logicielle. Elle permet de comprendre le fonctionnement d'un programme. Cette étude peut aussi viser un virus afin de comprendre comment celui-ci fonctionne. L'objectif est de comprendre le fonctionnement du système pour que lors d'une enquête après une attaque cyber, le traitant puisse définir quel système est touché et ainsi comprendre quelle faille a pu être utilisée par l'assaillant.
    - L'étude de la couche physique du cyber est, elle aussi, particulièrement intéressante pour l'enquêteur. Le Comcyber de la gendarmerie constatait lors de la conférence « *Le rôle de la R&D et ses méthodes dans une investigation* »[47] que les criminelles avaient tendance à détruire leurs matériels numériques avant leurs arrestations. L'objectif de la rétro-ingénierie physique est de comprendre le fonctionnement de chaque objet et d'en déterminer la valeur. Cela peut permettre de reproduire l'objet de l'étude (par exemple une carte mémoire) voir de la reconstituer en cas de détérioration. Ainsi, certaines informations peuvent être recouvertes et apporter des éléments à une investigation, du moins partiellement.

[44] Indicateurs de compromission (IOC). IS Decisions, 2019.
[45] Définition de l'Analyse forensique. Assurance Cyber-risques - Protégez votre informatique contre les cyberattaques [en ligne].
[46] Live Vs Dead Computer Forensic Image Acquisition. International Journal of computer science and information technologies.
[47] Le rôle de la R&D et ses méthodes dans une investigation [conférence]. 2022.

Le rôle de la CTI est donc de capitaliser de la connaissance sur les systèmes, de comprendre quel groupe de hackers se trouve derrière quel *malware*. Comme vu précédemment dans la partie 1, un grand nombre d'APT existe et il est souvent difficile d'attribuer l'attaque cyber à un acteur criminel ou étatique. L'objectif du RIC est donc, d'abord et avant tout, d'étudier les *malwares* et les *patterns* d'attaque référencés. Les analystes en RIC s'appuient régulièrement sur des bases de données. Les bases de données en CTI sont prépondérantes puisqu'au vu de la densification des systèmes et des données dans l'espace cyber, il devient très compliqué pour une institution ou une entreprise d'avoir une connaissance exhaustive sur l'ensemble des systèmes, des *malwares* et des acteurs du monde cyber. On pourra citer la base de données MITRE ATT&CK[48] ou OpenCTI[73]. Elles référencent les types de tactiques, techniques et procédures (TTP)[49] mises en place par les assaillants référencés. Cela peut permettre, d'une part de comprendre pourquoi un indicateur de compromission a été privilégié au détriment d'un autre, mais aussi d'identifier un *pattern* pouvant permettre d'attribuer l'attaque à un acteur.

Si le renseignement d'origine cyber et le renseignement d'intérêt cyber permettent de capitaliser un nombre important de connaissances, il faut bien comprendre qu'ils ne peuvent représenter à eux seuls une source suffisante pour valider une information. Le RIC et le ROC sont des capteurs[50] qui doivent permettre de croiser une information avec un autre panel de sources d'informations. Dans ce contexte, et afin que l'information soit la plus juste possible, une méthodologie stricte doit être observée lors d'enquête RIC et ROC afin d'éviter de déformer ou de rendre impossible la judiciarisation de l'enquête.

B. La méthodologie de l'enquête numérique et le choix des outils

La méthodologie de l'investigations dans le domaine cyber est homogène et doit suivre un certain nombre d'étapes bien définies. Cependant, il est important de comprendre que si beaucoup de choses sont faisables en enquêtes d'intérêt ou d'origine cyber, il y a un cadre légal contraignant qui est incontournable. Lors d'une enquête, l'investigateur ne peut faire ce qu'il veut.

Les renseignements d'origine cyber et d'intérêt cyber sont soumis au *« Règlement général sur la Protection des Données* » (RGPD) qui « *encadre le traitement des données personnelles sur le territoire de l'Union européenne.* »[51]. L'objectif du RGPD n'est pas de rendre impossible l'exploitation des données personnelles, mais de rendre compatible cette utilisation et le droit à la vie privée. Lorsqu'une enquête est réalisée, il faut une base juridique définie par l'article 6 du RGPD[52] :

A. La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques.

[48] Centre cyber d'excellence. Référentiel cyber V6. Février 2021 [consulté le 30 mai 2022]. Disponible sur : https://www.pole-excellence-cyber.org/wp-content/uploads/2021/06/Brochure-Referentiel-V6.pdf. [73] OpenCTI - Plateforme ouverte d'analyse de la cybermenace. *OpenCTI - Plateforme ouverte d'analyse de la cybermenace* [en ligne]. 2019 [consulté le 30 mai 2022]. Disponible sur : https://www.opencti.io/fr/.

[49] Centre cyber d'excellence. Référentiel cyber V6. Février 2021 [consulté le 30 mai 2022]. Disponible sur : https://www.pole-excellence-cyber.org/wp-content/uploads/2021/06/Brochure-Referentiel-V6.pdf.

[50] « *Un capteur technique est un dispositif monté sur un vecteur, celui-ci étant défini comme une plate-forme capable de l'emporter. L'élément pertinent pour la recherche associe, en fait, le couple capteur et vecteur, qui détermine la capacité et l'efficacité du recueil de renseignement.* » - BRUN Olivier, « Capteur », dans : Hugues Moutouh éd., *Dictionnaire du renseignement.* Paris, Perrin, « Hors collection », 2018, p. 132-134. DOI : 10.3917/perri.mouto.2018.01.0132. URL :

[51] RGPD : de quoi parle-t-on ? | CNIL. *CNIL,* 8 juillet 2021.

[52] Chapitre II - Principes, *CNIL,* 2016.

B. Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.
C. Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.
D. Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.
E. Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.
F. Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. De plus, l'objectif de l'enquête en RIC et ROC doit être bien défini et les limites exposées. Il est en théorie illégal de dépasser le cadre choisi. Par ailleurs, les informations utilisées pour une enquête ne peuvent pas être réutilisées ultérieurement. Il faut également impérativement limiter le prélèvement de données privées et se limiter aux informations nécessaires à l'enquête en cours.

Le RGPD stipule entre autres que les données doivent être stockées sur une durée limitée et seulement durant le temps de l'enquête. Il y a par ailleurs un devoir d'intégrité et de diffusion de la donnée. S'il est impossible pour l'enquêteur d'assurer que la donnée ne sera pas corrompue ou diffuser sans autorisation, il lui est interdit de la conserver.
Enfin, d'après l'article 13 et 14, il est obligatoire de prévenir la personne lorsque des données personnelles sont prélevées en source ouverte. Cependant, l'article 23 du RGPD permet une exemption de l'article 13 et 14 si les critères suivants sont observés durant l'enquête :

A. La sécurité nationale.
B. La défense nationale ;
C. La prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.
D. D'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale.
E. La protection de l'indépendance de la justice et des procédures judiciaires.
F. La prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière.
G. Une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique.
H. La protection de la personne concernée ou des droits et libertés d'autrui.
I. L'exécution des demandes de droit civil.
On constate que l'exemption de l'article 13 et 14 du RGPD se fait essentiellement dans un cadre étatique.

Pour respecter au mieux le cadre légal tout en conservant la donnée non déformée, l'enquêteur cyber doit respecter une méthodologie de recherche stricte et identique pour l'ensemble des procédures.

Celle-ci est calquée sur ce que l'on nomme le cycle du renseignement qui a su s'adapter au monde cyber[53] :

- L'orientation : elle vise à identifier les besoins en fonction du contexte. Elle permet de lancer le cycle du renseignement et est choisie par le décideur ;

- La collecte : Cette phase, qui arrive en second, doit permettre de concaténer un certain nombre de données brutes qui vont permettre de mener une enquête. Ce sont des éléments destinés à l'analyste qui sont collectés par les différents capteurs. Ces données peuvent être récupérées de deux manières différentes. Soit par la mise en place d'une veille continue, soit par la collecte active réalisée directement par un chercheur. Comme le soulève TRACIP, il est primordial de conserver l'intégrité de la donnée obtenue afin que l'enquêteur puisse avoir une traçabilité sur l'ensemble de l'enquête. Lors de la récupération de données, il faut indiquer les éléments permettant d'assurer cette traçabilité (type de document, heure, date, lieu…) .
- Le traitement de la donnée : une fois la collecte réalisée, il faut traiter les informations obtenues afin de les trier et de les rendre intelligibles. Cela passe par trois étapes. D'une part, il faut normaliser l'ensemble des données afin de leur donner un format homogène. Ensuite, il faut qualifier la collecte selon deux critères : l'intérêt qu'elle comporte, mais aussi son degré de fiabilité. Enfin, il est possible d'enrichir la collecte en croisant les informations obtenues avec des analyses ou des recherches antérieures déjà produites.
- L'analyse : c'est la phase de mise en valeur des données collectées. C'est l'aboutissement d'une enquête qui doit permettre d'apporter une connaissance mise en perspective avec l'orientation choisie par le décideur.

Enfin, une fois le cadre légal et la méthodologie intégrée, la dernière étape est de bien sélectionner ses outils de recherche. Des outils destinés à la réalisation d'une empreinte numérique ne seront pas adaptés à la réalisation d'une enquête basée sur la rétro-ingénierie physique.
De même, une enquête réalisée sur la Russie ne demandera pas les mêmes outils qu'un travail ayant un *focus* sur la Belgique. Il existe un certain nombre d'outils en ligne disponible en source ouverte. On distingue trois types d'outils :

- Les bases de données : ces bases de données, vérifiées et sûres permettent d'obtenir un certain nombre d'informations. On distingue deux types : les bases de données publiques publiées directement par les États et les bases de données participatives.
- Une majorité de pays possèdent des bases de données publiques et les laissent en accès libre. Elle représente une source de choix pour la collecte de données.
- Il existe aussi des bases de données participatives. Elles sont particulièrement utiles en *cyber threat intelligence* puisqu'elles laissent à disposition un grand nombre d'informations issues d'analyses réalisées au préalable.
- Les outils déjà intégrés à une interface html. Il suffit de posséder l'URL de l'outil pour pouvoir l'utiliser. On pourra citer par exemple EPIOS[54] qui permet d'étudier une adresse mail.
- Les outils à intégrer à une commande d'ordinateur. Ces outils sont créés par la communauté OSINT et ont pour la plupart été vérifiés par les utilisateurs grâce à leur code en source ouverte. Ils permettent souvent plus de flexibilité que les outils intégrés, mais ne sont pas

[53] Sekoia Team, Threat Intel 101 — Le cycle du renseignement appliqué à la (Cyber) Threat Intelligence. *medium* [en ligne]. 8 novembre 2018 [consulté le 30 mai 2022]. Disponible sur : .
[54] Epieos, the ultimate OSINT tool. *Epieos*.

toujours nécessaires et peuvent être plus compliqués d'utilisation. Il faut adapter l'outil à son utilisation.

Aujourd'hui, ces méthodes d'investigation sont bien intégrées dans l'ensemble de la sphère d'investigation. Si, ceux sont les milieux du renseignement et de la contre-criminalité qui se sont emparée de ce domaine en premier, le secteur de l'investigation journalistique a su tirer profit des apports du cyber. L'exploitation du cyberespace est plurielle allant de méthode simple à de l'investigation utilisant des outils plus pointus et plus poussée.

II. Cyber Threat Intelligence & OSINT

Il est donc notamment nécessaire d'avoir une vision efficace de la surface d'exposition d'une organisation ou d'une société à travers les techniques, car aujourd'hui, il ne suffit plus de savoir d'où vient la menace et de connaître l'attaquant, mais il faut aussi connaître son environnement. L'open source intelligence permet de s'appuyer sur des informations qui sont accessibles à toutes et tous, si tenté qu'on sache évidemment où et comment bien trouver l'information afin de compléter le tableau. En somme, ce que l'on comprend bien c'est que l'OSINT et le CTI sont deux démarches qui se regroupent.

Aujourd'hui, il existe plusieurs formes d'OSINT. En effet, ce n'est pas forcément la dimension purement technique, mais ce sont aussi des sous-catégories.

La dimension SOCMINT (Social media-intelligence), comme évoquée précédemment, se rapporte à la présence à travers les réseaux sociaux. Le SOCMINT permet de trouver un certain nombre de faisceaux d'indices via les réseaux sociaux ; à travers des commentaires, des « likes » de proche, des identifications ou bien même des hashtags, des forums spécialisés, etc.

Dans le cadre de ce type d'investigations, une organisation se démarque du lot : Bellingcat. Connu pour ses nombreux rapports sur des sujets tels que l'utilisation d'armes pendant la guerre civile Syrienne, la guerre dans le Donbass (y compris la destruction du vol 17 de Malaysia Airlines), le raid d'El Junquito, la guerre civile yéménite, l'empoisonnement de Skripal et le meurtre de civils par les forces armées camerounaises, Bellingcat a totalement redéfini les règles de l'investigation. Dans le cadre de l'affaire Skripal notamment, [55] le site d'information avait évoqué le nom des deux agents russes ayant empoisonné l'ex-agent du GRU, Sergei

Skripal, à l'époque protégé par les services anglais du M-16 et c'est au travers de l'OSINT que Bellingcat a réussi à identifier les auteurs, entre autres grâce à des photos de mariage et des échanges avec différents intermédiaires de l'ambassade russe de Londres, des postions GPS et des caméras en libre-service.

En somme, l'aspect humain est non dissociable de l'OSINT du fait de l'analyse qui découle de ces investigations techniques. En effet, il faut être en mesure de déceler l'auteur de l'attaque, le mode opératoire, et de pouvoir mettre en place et coordonner une protection pérenne. Cette protection se révèle essentielle notamment dans le secteur de la santé, car comme évoqué précédemment, les conséquences peuvent être rapidement fatales pour les patients. Ce fut le cas en 2020 lors de l'attaque de l'hôpital universitaire de Brno en République Tchèque. Cette attaque a mené au transfert en urgence de patients ainsi qu'à la fermeture de leur réseau informatique[56]. L'hôpital a été forcé de fermer tout son réseau informatique pendant l'incident, Et dans ce cas précis L'OSINT a été indispensable pour

[55] Pommiers, Eléa. Que sait-on sur l'empoisonnement de l'ex-agent double russe au Royaume-Uni ? *Le Monde.fr,*19 mars 2018.

[56] Blog, Article du Janvier 2021 « Le monde de la santé face aux cyber-attaques».

contextualiser les menaces, détecter les fuites d’informations, établir et alimenter les tableaux de bord et plateformes de visualisation.

A) Étude de cas : Focus sur les plans de guerre de Poutine en Ukraine, dévoilés grâce à l'OSINT

La guerre en cours en Ukraine a mis en évidence une nouvelle dimension de l'importance des réseaux sociaux et de la disponibilité gratuite et publique de l'information. Le renseignement redéfinit donc les règles de la guerre moderne. En utilisant diverses sources accessibles au public, telles que des journaux, des images satellites, des vidéos sur Twitter et Telegram. Les conflits sont devenus totalement transparents.

1. Les fondamentaux : Archivage et documentation pour se prémunir des atrocités

Pour exemple, *La Voix de l'Allemagne (Deutsche Welle) a* déclaré le 24 mars 2022 que « *les chercheurs s'appuient sur le mécanisme de source ouverte qu'ils ont utilisé précédemment pour découvrir des crimes présumés en Syrie, pour documenter les violations et les éventuels crimes de guerre en Ukraine à la suite de l'invasion russe de ce pays* [57]». Ainsi, grâce au travail d'archivage et de documentation issu de la guerre en Syrie et des techniques apprissent à l'époque de ce conflit, le cyberespace peut permettre de retracer des crimes qui aurait été commis sur un théâtre d'opération, de manière documentée avec dans certain cas une chronologie et une traçabilité des faits déconcertante grâce à l'IA comme RBK-250 [58].

Dans un rapport du journal allemand Der Spiegel intitulé *Les leçons des enquêteurs en ligne en Syrie aident l'Ukraine*, [59] Il a été ajouté que le conflit en Syrie est similaire à la guerre actuelle en Ukraine, notamment en termes d'implication de la Russie dans la guerre dans les deux pays, et de tactiques de guerre. *« La Russie a utilisé des bombes dans les deux pays pour cibler des infrastructures civiles, des écoles, des maisons d'enfants, des hôpitaux et des marchés, dans des actions qui équivalent à des crimes de guerre en vertu du droit humanitaire et international* », a indiqué le rapport.

Dans les guerres syrienne et ukrainienne, les chercheurs utilisent des sources ouvertes pour découvrir les crimes commis, notamment des informations librement accessibles en ligne et sur les réseaux sociaux, d'où l'appellation de renseignement de source ouverte, selon le rapport. Il est mentionné que « *les chercheurs recueillent et vérifient des preuves à grande échelle, notamment l'identité et la concentration des forces attaquantes, le nombre de victimes et l'étendue des dommages causés aux infrastructures, ainsi que des informations sur les équipements militaires et les armes utilisées lors des attaques* ». De ce fait, avec le début de l'invasion russe de l'Ukraine, les enquêteurs ont utilisé des vidéos sur les médias et réseaux sociaux montrant l'utilisation d'attaques de missiles, et ont compté les chars qui ont été détruits et les noms des soldats en exercices et/ou décédés.

« *L'équipe d'enquête open source dans la guerre ukrainienne est divisée entre ceux qui travaillent à l'intérieur du territoire ukrainien et d'autres dans d'autres pays, répétant le même mécanisme utilisé en Syrie* », indique le rapport. Les pays occidentaux accusent l'armée russe de bombarder des civils dans le cadre des opérations militaires qu'elle mène depuis le 24 février en Ukraine.[60] Le 17 mars, les ministres des Affaires étrangères des pays du G7[61] ont averti, par le biais d'une déclaration commune, que les auteurs de crimes de guerre en Ukraine devront répondre de leurs actes devant la justice internationale, se déclarant satisfaits des enquêtes et des opérations de collecte de preuves menées en Ukraine.

[57] "Moscou emploie en Ukraine les mêmes méthodes qu'en Syrie.

[58] Intelligence artificielle. Prouver les crimes de guerre en Syrie à l'aide d'images synthétiques. *Courrier international.*

[59] Les dernières nouvelles de l'invasion de l'Ukraine. *Le Devoir*, 3 juin 2022.

[60] Guerre en Ukraine : chronologie des événements, Touteleurope.eu.

[61] Ukraine : les pays du G7 préviennent que les auteurs de crimes de guerre "devront rendre des comptes".

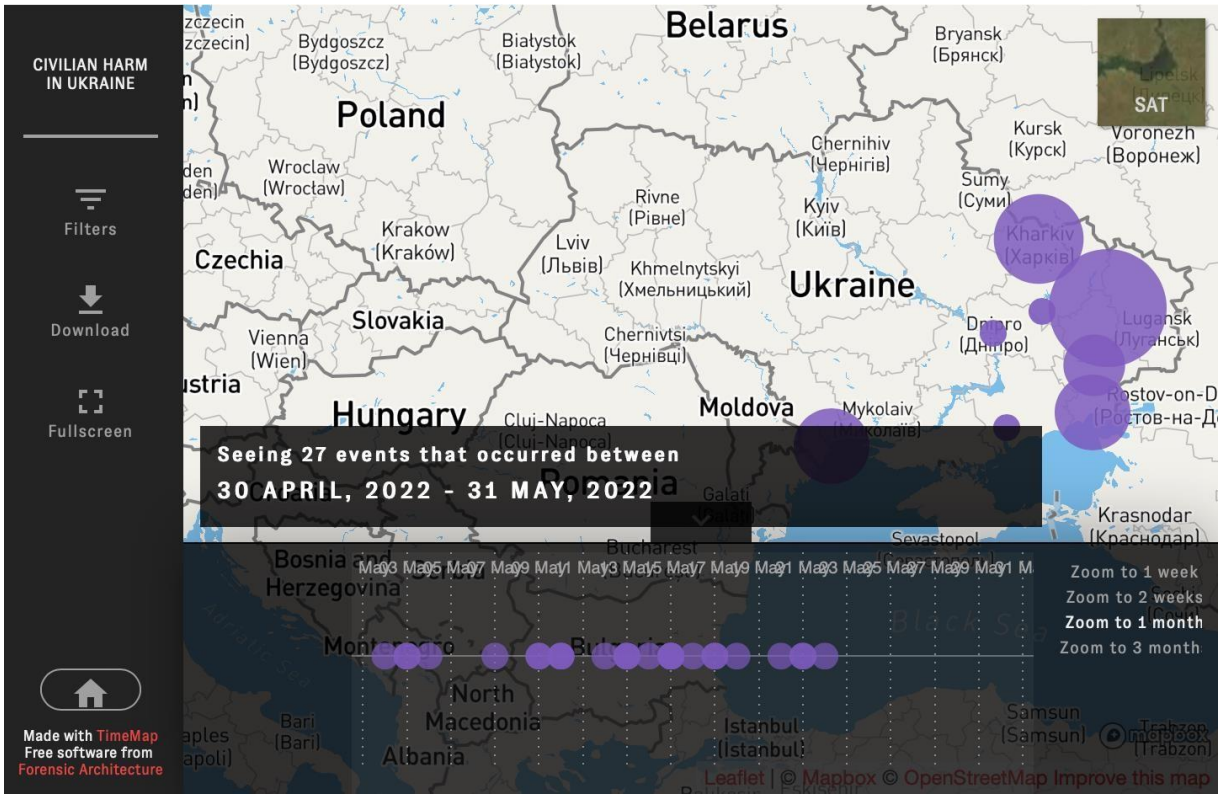


Illustration réalisée avec le logiciel TimeMap Free de Forensic Architecture sur le site Bellincat – référencement des attaques sur les sites civils bombardé par l'armée russe.

L'organisation à but non lucratif Mnemonic[62] basée à Berlin a également joué un rôle clé dans les efforts visant à enquêter sur les crimes commis lors de conflits dans des pays tels que la Syrie, le Yémen et le Soudan. Elle a formé une archive pour chacun de ces pays afin de préserver les preuves numériques des violations des droits de l'Homme.

Dans un entretien exclusif avec l'auteur du rapport de la DW ((*Deutsche Welle)),* M. al-Khatib de Mnemonic a déclaré : « *Il n'a fallu que quelques jours pour que nous soyons en mesure de créer les archives ukrainiennes. Nous avons les connaissances et l'expérience nécessaires pour créer de telles archives, car nous savons que certaines normes et certains protocoles doivent être mis en place pour préserver ce matériel.* » et « *Nous avons tout appris au cours de notre travail sur la Syrie. Nous avons réalisé l'utilisation des armes à sous-munitions en Ukraine dès que nous les avons vues. Nous savons comment elles peuvent être utilisées, et les différentes petites explosions qui en résultent se produisent en même temps au hasard* », Il estime que certains indicateurs permettent de conclure que le fait de cibler une maternité à Marioupol, en Ukraine, avec un missile, n'était pas une erreur. Car il est prouvé qu'il y a une intention délibérée avec un système d'action clair dans ce cadre, car un certain nombre de villes comme Marioupol et Kharkiv ont été exposés est identique à ce qui s'est passé dans la ville d'Alep en 2016.

2. L'importance de la crédibilité et de la fiabilité

La Russie a dû à plusieurs reprises supprimer des clips et des photos de plusieurs reportages télévisés après leur publication, car ils constituent un démenti direct aux allégations russes dans le contexte des guerres de Poutine en Syrie et en Ukraine.[90] Par exemple, grâce à des clips diffusés par des éléments

[62] Removing the guesswork from cybersecurity. *Mnemonic.*

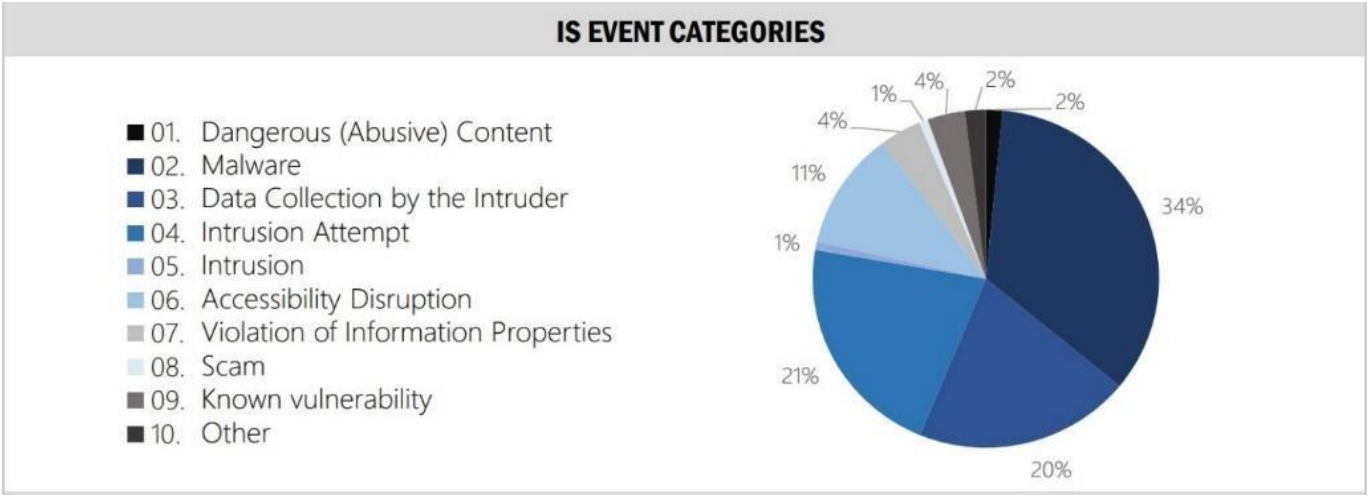
russes sur les réseaux sociaux, le journal russe Novaya Gazeta a publié en octobre 2019 une enquête sur les crimes commis en Syrie[91], où l'identité des auteurs, leurs noms et le parti auquel ils appartiennent, la milice Wagner, étaient connus. Les investigations du journal n'ont pas dépendu d'une source au sein de la milice russe, mais plutôt de renseignements de source ouverte et y ont trouvé crédibilité et fiabilité, menant à la publication de l'enquête.

Novaya Gazeta[92] n'est pas le premier journal à adopter les enquêtes en source ouverte. Il a été précédé par de nombreux grands journaux internationaux, dont le Washington Post, le
Guardian, Bild et le New York Times[93], ainsi que par des agences de presse internationales.
Des organisations de défense des droits de l'Homme telles que Human Rights Watch et les Nations unies se sont également appuyées sur ces enquêtes[94]. Aujourd'hui, Novaya Gazeta est fermé sur décision des autorités russes depuis fin avril.

3. Le CTI au cœur de la guerre en Ukraine

Depuis le début du conflit, l'Ukraine a observé près de 14 millions de cyber-incidents au premier trimestre 2022[95]. La majorité des incidents ont donné lieu à des tentatives de distribution de logiciels malveillants, d'hameçonnage et d'intrusion et cela trois mois après le début de l'invasion en cours de l'Ukraine par la Russie, le pays fait le point sur les turbulences auxquelles la nation a été confrontée dans sa cybersphère au cours du T1 2022, et envisage la voie à suivre.

L'équipe de réponse rapide du *State Cyber Defense Center* (SCPC)[96] de l'Ukraine, qui dépend du Service national des communications spéciales et de la protection de l'information de l'Ukraine, a transmis un rapport à l'Information Security Media Group[97].
Parmi ceux-ci, 78 000 ont été traités comme critiques, indique le SCPC à l'ISMG. Le rapport ajoute que 63 % des événements suspects ont été détectés au sein de ministères et d'organisations, tandis que 35 % ont affecté les administrations régionales.



[90] Guerre en Ukraine : parcourez les infox et les fausses images qui circulent depuis le début de l'offensive russe. *Le Monde.fr*,4 mars .
[91] Wagner en Syrie : Une cour russe pérennise l'impunité pour les responsables d'un meurtre violent. *Fédération internationale pour les droits humains*.
[92] Présentation
[93] Wise, Jeff. The DIY Intelligence Analysts Feasting on Ukraine. *Intelligencer* , 4 mars.

[94] Ukraine : une enquête des droits de l'homme de l'ONU met en lumière la détresse des civils. *ONU Info.*

Collecte d'informations

Les statistiques ont été recueillies par le centre d'opérations de sécurité du SCPC qui surveille et détecte les activités malveillantes ainsi que les anomalies des systèmes et des réseaux dans plusieurs installations de cyberdéfense en Ukraine. Il analyse les données obtenues à partir de dispositifs de réseau [tels que des capteurs actifs, des pare-feux, des scanners de vulnérabilité], de postes de travail et de serveurs, de systèmes d'autorisation et de sources de données internes et externes sur les cybermenaces, afin d'identifier les menaces, indique le SCPC.

Près d'un quart de ces sources de données proviennent de sources de données internes (9 %) et externes (15 %) sur les cybermenaces et une majorité écrasante de 35 % provient de scanners de vulnérabilité et de systèmes de détection des intrusions, indique le rapport.

Le SCPC a divisé ces incidents de sécurité de l'information ou de cybersécurité en plusieurs catégories et types afin de mieux comprendre les motivations des adversaires de l'Ukraine. Cette catégorisation a permis de constater que la diffusion de logiciels malveillants, l'hameçonnage ou la collecte de données par intrusion, et les tentatives d'intrusion dans des systèmes critiques sont les principales motivations et méthodes utilisées par les adversaires de l'Ukraine.

La majorité des attaques proviennent, sans surprise, de la Russie, mais le SCPC indique que d'autres pays importants à partir desquels la source de ces attaques a été retracée incluent la Chine, la Corée du Sud, les États-Unis, l'Inde et le Bangladesh, entre autres. Le SCPC précise toutefois que cela ne signifie pas nécessairement que les cyberattaques ont été attribuées à ces pays. « *Le suivi a été effectué sur la base du nombre de positifs ciblant les régions ukrainiennes à partir d'adresses IP d'autres pays et la localisation IP n'est que le nom de la délégation d'un pays.* » N'importe qui peut utiliser un réseau privé virtuel ou d'autres ressources pour diriger via l'adresse IP d'un autre pays, indique le SCPC.[98]

---

[95] L'Ukraine, victime d'une attaque informatique comme arme de guerre. *la revue européenne des médias et du numérique - Home Slider - La revue européenne des médias et du numérique* [en ligne]. [sans date] [consulté le 4 juin 2022]. Disponible sur : https://la-rem.eu/2022/05/lukraine-victime-dune-attaque-informatique-comme-arme de-guerre.

[96] Ukraine Observed Nearly 14M Cyber Incidents in Q1 2022. *Bank information security news, training, education - BankInfoSecurity* .

[97] Chuck. Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know. *Forbes* [en ligne].

[98] Rapport du SCPC, Ukraine (2022).

En ce qui concerne les régions d'Ukraine qui ont été ciblées lors de ces événements de cybersécurité, le SCPC indique que Kharkiv, Kyiv, Dnipro et Lviv sont en tête de liste, et sans surprises ces villes sont au cœur de la stratégie russe de conquête du territoire Ukrainien.

Partie 3 : Perspectives : évolutions et anticipations des nouvelles menaces

I. Les menaces cyber : une menace exponentielle et omniprésente dans le futur

A) La géopolitique, génératrice de nouvelles menaces

À l'avenir, les relations internationales vont être un facteur de plus en plus important dans les menaces cyber. En effet, les deux super puissances, que sont la Chine et les États-Unis, se partagent aujourd'hui le monopole des technologies, des équipements et des matériaux servant à la fabrication, et l'utilisation des systèmes d'information vont conserver leur avance technologique tant que personne ne se positionne sur ces secteurs. Le monopole de ces technologies ne serait rien sans les données. Encore plus qu'aujourd'hui, leurs collectes et analyses deviendront des actifs stratégiques aux services des Puissances. L'utilisation des données sera utilisée pour affiner les stratégies et connaissances sur les faiblesses des adversaires. Les attaques dépendent toujours de la géopolitique. En effet, certaines des menaces les plus sophistiquées dans le cyberespace proviennent d'autres États qui cherchent à mener des activités d'espionnage dans le but de compromettre les actifs gouvernementaux, militaires, industriels et économiques, ainsi que de surveiller les opposants à leur propre régime. Le cyberespace est déjà utilisé par les terroristes pour diffuser leur propagande, radicaliser leurs partisans potentiels, collecter des fonds, communiquer et planifier.

Ainsi, d'après Lehto[63], les cibles des menaces pour l'avenir seront plus que jamais liées aux infrastructures vitales : énergie, eau, production alimentaire, chaînes d'approvisionnement. Cependant, ces menaces ne sont pas encore considérées par tous les pays comme un sujet essentiel. En effet, la criticité des infrastructures vitales n'est mentionnée que dans les rapports de Stratégies de cybersécurité de la République tchèque, de l'Estonie et des États-Unis sur les neufs étudiés. L'exemple de la cyberattaque contre l'US Colonial Pipeline en est une bonne illustration, en effet en s'attaquant à une infrastructure critique cela a mené à la création de pénuries[64] : station-service et production d'énergie au fioul.

De la même manière, d'autres cyberattaques ont visé les infrastructures pétrolières et gazières de pays européens ces derniers mois : Allemagne, Belgique, et Pays-Bas[65]. Dans ces cas, les menaces ont visé des infrastructures critiques de l'énergie : les distributeurs, les fournisseurs et les installations de stockage d'hydrocarbures. D'après la classification de Lehto[66] des menaces à 5 niveaux basés sur des facteurs de motivation : cyberactivisme, cybercriminalité, cyberespionnage, cyberterrorisme et cyberguerre ; le 4e niveau, celui du cyberterrorisme semble être en augmentation, car il utilise les réseaux pour attaquer des systèmes CTI critiques. L'objectif de ces attaques est de causer des dommages, de susciter la peur parmi le grand public et de forcer les dirigeants politiques à céder aux exigences des terroristes[67].

[63] Lehto, Martti. The cyberspace threats and cyber security objectives in the cyber security strategies. *International Journal of Cyber Warfare and Terrorism,* 2013.

[64] Segal, Edward. 1 Year Later : Actions Taken, Lessons Learned Since The Colonial Pipeline Cyberattack.

[65] Vitard, Alice. Visés par une cyberattaque, des sites portuaires européens sont au ralenti. *usine-digitale.fr* [en ligne]. 7 février 2022.

[66] Lehto, Martti. The cyberspace threats and cyber security objectives in the cyber security strategies. *International Journal of Cyber Warfare and Terrorism,* 2013.

[67] Beggs, Christopher. Proposed risk minimization measures for cyber-terrorism and SCADA networks in Australia. *Proceedings of the 5th european conference on information warfare and security*. 2006, 9–18.

B) Le Dark Web développement d'un marché de menaces au service des cyberattaquants

Pour prévenir et se protéger des cyberattaques, il est capital de mener une veille des menaces au sein du monde cyber. Cette tâche est très complexe, notamment dû au fait de la constante évolution des technologies employées. Les cybermenaces sont intrinsèquement liées aux structures d'internet existantes, et que l'on trouve notamment dans le Dark Web. Il faut différencier les notions de Deep Web et Dark Web qui désignent le contenu du World Wide Web qui n'est pas indexé par les moteurs de recherche standard. Les couches les plus profondes du Deep Web, un segment connu sous le nom de Dark Web, contiennent du contenu qui a été intentionnellement dissimulé, notamment des informations illégales et antisociales[68].

Le Deep Web et Dark Web sont sujets aux spéculations et rumeurs en raison du peu de connaissance de l'opinion publique sur la réalité de ces cyberespaces. Bien qu'il ne s'agisse pas d'un espace illégal, le Dark Web est présenté comme un « *royaume sans loi* » utilisé par les cyberpuissances et hackers seuls en groupe pour mener des activités illégales[69]. Dans cet espace d'Internet où l'on peut trouver de nombreux moyens de nuire à autrui en passant par les virus, les vers, les chevaux de Troie, les logiciels malveillants, les rançongiciels et une pléthore d'autres codes malveillants à louer.
Les logiciels et services vendus ou loués sont très puissants, comme le montre l'exemple récent lorsque Cloudflare a déjoué un botnet visant une entreprise de cryptomonnaie. L'attaque a culminé à plus de 15,3 millions de requêtes par seconde se basant sur 6000 bots provenant de
112 pays différents.[70] En effet, les botnets ou réseaux d'ordinateurs manipulés par un virus, peuvent être loués pour quelques centaines de dollars ou moins.

Weimann[71] souligne le recours croissant au Dark Web par les cyberterroristes afin d'accéder à des logiciels aux capacités de plus en plus poussées. La surveillance de ce cyberespace est capital pour les services de renseignements, mais ces derniers font face à l'utilisation de plus en plus régulière d'outils d'invisibilisation. D'après Ablon, Libicki et Golay[108] à l'avenir la protection des communications, grâce au chiffrement, et des transactions, grâce aux VPN, devront faire l'objet d'une attention accrue par les services de renseignements des États afin d'anticiper les futures menaces. Pour cela il sera inévitable d'augmenter les ressources technologiques et humaines des services de surveillance étatiques.

D'après les recherches de Weimann[109], 57% des contenus que l'on trouve sur le Dark Web sont des contenus illégaux, allant de la pornographie à la drogue, au trafic d'armes, à la fausse monnaie, aux communications terroristes, etc. Dans leurs travaux Ablon, Libicki et Golay[110] illustrent ces craintes quant à l'utilisation de plus en plus précoce par les jeunes générations en déclarant que « *le piratage est devenu une petite ligue : tout le monde commence tôt et passe beaucoup de temps à le faire* ».
Le fait que TOR, désormais associé et largement utilisé par des criminels, des pirates informatiques et des groupes terroristes, ait été créé à l'origine par une entité gouvernementale américaine est surprenant. En effet, TOR est créé initialement par un laboratoire de recherche de l'US Navy, le but de cet outil étant de communiquer de manière anonyme. Aujourd'hui, le Dark Web et les passerelles qui y mènent ont évolués, continuant de croître et d'évoluer, mais reste sous l'influence du gouvernement

[68] Weimann, Gabriel. Terrorist Migration to the Dark Web. *Perspectives on Terrorism*. 2016, **10**(3), 40–44.
[69] Ibid.
[70] Cheminat, Jacques. Cloudflare déjoue une gigantesque attaque DDoS par HTTPS - Le Monde Informatique. *LeMondeInformatique*, 22 avril 2022.
[71] Weimann, Gabriel. Terrorist Migration to the Dark Web. *Perspectives on Terrorism*. 2016, **10**(3), 40–44.
[108] Lillian Ablon, Martin Libicki et Andrea Golay. Projections and predictions for the black market. *Markets for Cybercrime Tools and Stolen Data Book Subtitle : Hackers' Bazaar*. 2016, **10**(3), 40–44.
[109] Weimann, Gabriel. Terrorist Migration to the Dark Web. *Perspectives on Terrorism*. 2016.

américain, car ce dernier finance le projet et met à disposition des serveurs d'hébergement[72]. Cela s'est accentué ces dernières années avec l'apparition et le développement de technologies telles que l'Intelligence artificielle (IA), le Machine Learning (ML), l'informatique quantique et les nanotechnologies.

C) Nouveau *modus operandi* des cyberattaquants : Intelligence Artificielle et Machine Learning au service de nouveaux usages

Une des cybermenaces majeures dans les années à venir est due à la combinaison des maliciels basés sur l'Intelligence Artificielle (IA) et le Machine Learning (ML). Les pirates ont de plus en plus recours à des logiciels malveillants dont la particularité est de pouvoir conduire à l'autoréplication, voir l'évolution, du code. Les environnements informationnels offrent à ces cybermenaces un espace riche en données dans lequel elles peuvent proliférer, s'adapter, croître et se reproduire à volonté. Un tel système utilisant l'IA pour écrire du code a été mis au point par des chercheurs de l'université de Rice et appelé BAYOU[73]. Le système utilise l'apprentissage neuronal (ML) pour générer de nouveaux programmes. D'après les travaux de Murali[74], « *les expériences indiquent que le système peut souvent générer des corps de méthode complexes à partir de quelques tokens seulement, et que l'apprentissage au niveau des esquisses est essentiel pour effectuer une telle génération efficacement* ». Ces systèmes sont ce qu'on appelle des « *systèmes empoisonnés* », où les logiciels malveillants infectent et modifient les parties les plus importantes du système.

Ainsi, ces « *systèmes empoisonnés* » sont décrits par Stevens et Biller[75], dans un rapport pour l'OTAN, comme se distinguant des virus informatiques, car ils permettent au code malveillant de se transférer vers d'autres systèmes lorsqu'il remplit diverses conditions. L'exemple le plus emblématique de ce maliciel est Stuxnet. Ce ver extrêmement sophistiqué s'est fait connaître en détruisant des centaines de centrifugeuses d'enrichissement de l'uranium utilisées dans l'installation nucléaire iranienne de Natanz[76]. La caractéristique principale de Stuxnet est qu'il a été codé avec la capacité de s'adapter pour muter. Cette capacité a fait que la sécurité informatique n'a découvert le ver que lorsqu'il a commencé à faire apparaître des écrans bleus et à redémarrer les systèmes Windows[77].

Aujourd'hui, les logiciels malveillants développés sont repérables par les antivirus, et peuvent ensuite être ajoutés aux bases de données pour prévenir les infections d'autres ordinateurs ou objets connectés[78]. Cependant, les maliciels comme l'a observé un analyste du secteur, cité par Downes[79], les analystes informatiques sont incapables, pour l'heure, de suivre le rythme de l'augmentation du nombre de maliciels. En passant par les ransomwares aux botnets visant les PC, les ordinateurs portables, les smartphones ou les appareils mobiles, il y a des milliards d'appareils insuffisamment protégés. Face à cette perspective de terrain de jeu grandissant, de grands nombres de hackers proposent leurs services à la location et vendent leurs *malwares* afin de mener des cyberattaques de plus en plus sophistiquées contre des entreprises, des gouvernements et autres institutions internationales.

---

[72] Tor. The Tor Project | Privacy & ; Freedom Online. *Tor Project | Anonymity Online*, 2022.

[73] Murali, Vijayaraghavan et al. Neural Sketch Learning for Conditional Program Generation. *Conference Paper ICLR 2018*. 2018, 1–17.

[74] Ibid.

[75] Ertan, Amy et al. Cyber Threats and NATO 2030: Horizon Scanning and Analysis. *CCDCOE*. 2020.

[76] Ibid.

[77] Jabbour, Kamal et Erich Devendorf, Cyber Threat Characterizatoin. *The Cyber Defense Review*. 2022.

[78] Klipstein, Michael. Seeing is Believing : Quantifying and Visualizing Offensive Cyber Operations Risk. *The Cyber Defense Review*. 2019, **4**(1), 85–106.

[79] Downes, Cathy. Strategic Blind–Spots on Cyber Threats, Vectors and Campaigns. *The Cyber Defense Review*. 2018.

Avec l'avancement continu de l'IA et du ML, les capacités associées aux logiciels malveillants avancés sont inquiétantes, mais aussi fascinantes à la lumière de leur capacité à changer, à croître et à se reproduire, ce qui ajoute une autre couche de complexité. Comme avancé par Bort[80], les nouveaux produits de sécurité intégrant le ML et l'IA ajoutent facilement des cycles de test. Ainsi, le logiciel malveillant s'auto-évalue par rapport à la matrice de test, permettant de s'assurer qu'aucun produit testé ne peut être détecté et signalé par les antivirus.

Pour le moment, l'atout de cette méthode d'auto-évaluation du maliciel est qu'il n'est pas optimal, et possède des failles réduisant son potentiel de nuisance. Ainsi, comme présenté par Mason[81], bien que les environnements de développement avancés générant du code automatiquement fonctionnent, ce n'est pas le cas en toutes circonstances. Dès lors, « *il convient d'observer que l'utilisation croissante des systèmes ML complique cette question, car le code logiciel reçoit l'instruction de prendre d'autres décisions lors de son exécution, ce qui augmente la complexité. En outre, la véracité des systèmes ML comme les réseaux neuronaux ne peut pas être facilement comprise ou vérifiée* »[82]. À mesure que ces types de systèmes prennent de l'importance et deviennent de plus en plus fiables, nous pouvons nous attendre à une croissance potentiellement exponentielle de la prolifération des codes et des logiciels malveillants, ce qui entraînera la nécessité de se pencher sur l'environnement informationnel dans lequel le « *code vivant* » existera et se reproduira.

II. Les scénarios d'anticipation à l'horizon 2030

Si l'on se penche sur le cas de la France et des menaces à venir notamment ceux de l'horizon 2030, il est important de poser différentes tendances afin d'anticiper les menaces probables. C'est notamment ce qu'a fait Cyber Campus[83] qui a publié un rapport de prospectives sur les menaces du futur. Parmi celles-ci, les plus pertinentes sont celles relevant de l'ultra connectivité, du cloisonnement des réseaux et de la réglementation.

A) Les dangers de l'ultra connectivité : l'accélération des échanges et des menaces

L'ultra connectivité de la société entraîne de nombreux défis. Avec l'augmentation de la vitesse de connexion, les produits et services connectés vont augmenter, ce qui va mener à de nouveaux usages et augmenter les surfaces d'attaques pour les cyberattaquants. Ces surfaces d'attaques se verront principalement :

- Dans les entreprises : L'augmentation de la connectivité va entraîner un développement accru des chaînes d'approvisionnement qui seront davantage automatisées, notamment grâce aux robots, que ce soit dans la production ou la livraison des produits. Le numérique va permettre une croissance de la productivité des entreprises grâce à l'automatisation des tâches et la plus place plus importante de l'IA dans des tâches effectuées auparavant par des humains.
- Au quotidien : L'utilisation de plus en plus poussée des capteurs que ce soit dans les villes (*smart cities*), les transports (*smart mobility*), lieux publics (*smart education*, *smart health*) et les habitations (*smart homes*) vont entraîner une augmentation des données. Le risque étant de voir ces dernières récupérées, modifiées, analysées à différents desseins (terrorismes, pécuniers). Les pratiques citoyennes comme les démarches administratives vont évoluer vers

[80] Bort, Bryson. There IS No Cyber Defense. *The Cyber Defense Review*. 2018, **3**(1), 41–46.

[81] Mason, Stephen. The Presumption That Computers Are 'Reliable'. *Electronic Evidence*. 2017, 101–192.

[82] Ibid.

[83] Horizon Cyber 2030, Campus Cyber, 2022.

plus d'inclusivité et de simplicité grâce aux progrès technologiques et à l'interconnectivité des services.

- Cette hyperconnectivité des systèmes va offrir aux cyberattaquants un large éventail de cibles (ex. : arrêt de la chaîne d'approvisionnement, perturbation des usines, des magasins ; accès aux bases de données ; contrôle des objets domestiques ou professionnels). La rapidité des technologies va permettre d'étendre rapidement et largement leurs attaques. Notamment grâce à l'essor de la plateformisation des usages supporte le développement économique des filières criminelles qui utilisent ces plateformes pour vendre leurs compétences et s'organiser (notamment via les places de marché du Deep Web où sont vendus de nombreux maliciels), tel que :
- Piégeage à grande échelle des chaînes d'approvisionnement physiques (e.g., perturbation des usines, des magasins...) ;
- Utilisation large des systèmes numériques à des fins criminelles (e.g., réseaux de robot pour lancer des attaques) ;
- Instantanéité de propagation de logiciels malveillants (e.g., type NotPetya), instrumentalisée dans le cadre d'attaque sur les services essentiels ;
- Création de faux frais et de services numériques peu onéreux pour piéger les victimes (e.g., faux services de protection, faux accès premium à des services gratuits) ;
- Diffusion de fausses informations (fake news) dans tous les secteurs (e.g., sur la finance en impactant plus facilement les cours de bourse en raison de la forte automatisation).

B) Le cloisonnement des réseaux internet : l'émergence et la consolidation des réseaux internet nationaux

L'ultra-cloisonnement est poussé par l'exacerbation des méfiances géopolitique et des craintes face aux dépendances entre écosystèmes numériques. En effet, l'heure actuelle est à une politisation des réseaux d'informations et la souveraineté numérique, se fait ainsi tant du point de vue des infrastructures réseaux que sur la production de maliciels. En effet, avec la
Chine et sa grande muraille d'Internet, les États ont tendance à créer de plus en plus de frontières numériques. Que ce soit en Afrique ou au Moyen-Orient, la grande majorité des États censurent internet. Nous constatons la mise en place de plus en plus de frontières numériques comme la
Russie avec le Runet.[84] D'après l'étude d'anticipation de Campus Cyber, l'horizon 2030 sera marqué par un cloisonnement accru d'Internet, notamment par une isolation technologique comme avec les processeurs, les fabricants de microprocesseurs et le clou dans l'appui à la défense nationale. L'exacerbation des tensions internationales entraîne une volonté de contrôle des flux internet, comme on peut le constater actuellement dans la guerre que la Russie a déclarée à l'Ukraine.[85]

L'affirmation des intérêts économiques nationaux ajouter aux tensions géopolitiques, vont entraîner une augmentation des attaques cyber et accentuer les pratiques d'espionnage entre États. Ces tensions risquent de pousser les États à augmenter leur contrôle sur les populations. Les menaces terroristes et la défense des intérêts nationaux vont entraîner une augmentation de la captation des données dans une volonté d'anticiper les menaces. De plus en plus surveillés, les individus ne pourront plus échanger de l'information librement et de manière anonyme. Si les États arrivent à lutter contre le chiffrement

[84] Corot, Léna, *La guerre en Ukraine peut-elle précipiter la fragmentation de l'Internet ?* usine-digitale.fr, 1 mars 2022.
[85] Lausson, Julien. La Russie tente d'asseoir sa domination dans l'Ukraine occupée en détournant Internet. *Numerama*, 31 mai 2022.

de bout en bout, comme le montrent[86] les nombreuses tentatives au niveau européen et mondial, cela entraînera *de facto* une réduction de la sécurité des échanges sur internet.
D'un point de vue économique, les entreprises internationales se verraient obliger de cloisonner leurs systèmes d'informations afin de réduire leurs failles, impactant négativement leurs ressources et leurs expertises dans chaque zone souveraine.

Pour les cyberattaquants, ces faiblesses les pousseraient à opérer de plus nombreuses attaques sur les systèmes d'information des États, ces derniers possédant de plus en plus d'informations sensibles sur les entreprises et les citoyens. Le maintien d'un marché international de vulnérabilités, comme vu précédemment avec le Dark Web, favorisera l'essor économique d'organisations cybercriminelles. Ces dernières détiennent l'expertise et les ressources nécessaires pour les exploiter de manière encore plus rapide et efficace. Le cloisonnement régional des écosystèmes simplifiera la détection des cibles pour les attaquants, mais réduira le risque de dégâts collatéraux. La proximité entre États et cybercriminels va aussi permettre aux groupes d'être dotés de meilleures capacités offensives, tout en bénéficiant d'impunité et de protection dans leur propre espace souverain. Ainsi, les attaques mêleront informationnels, cognitifs et cyber. Ainsi, l'espionnage numérique sortira renforcé avec la multiplication de hackers soustraitants, proposant leurs services aux États. Ces derniers pourront mener des attaques sous « *faux drapeau* », ce qui consiste à laisser des traces lors d'une attaque afin de faire croire qu'il s'agit d'un autre groupe ou État qui a mené l'attaque. Surtout, une menace systémique redoutée est celle visant la destruction physique de certains câbles sous-marins.

C) La réglementation du monde numérique : les défis du renforcement réglementaire pour s'adapter aux menaces futures

Le secteur numérique va faire face à une augmentation réglementaire afin de renforcer la sécurité et la confiance dans les usages numériques. Dans le futur, il est possible que les réglementations se multiplient et les différentes autorités renforcent leurs capacités de contrôle.
Dans cette perspective, deux visions s'opposent : celle en faveur d'une monétisation des données contrôlées par l'utilisateur, comme souvent présenté par le philosophe Gaspard Koenig[87] et celle percevant ces dernières comme une extension de la vie personnelle et nécessitant une protection. Chaque grande zone de puissance met en place ses propres réglementations (États-Unis, Europe, Chine, Russie) donnant plus ou moins de contrôle et d'obligations aux utilisateurs et offreurs de services numériques.

Ainsi, dans les zones où le citoyen détient ses données personnelles la possibilité de contrôler et de valoriser leurs « *traces numériques* », comme aux États-Unis avec les assurances permettant de diminuer les cotisations mensuelles en échange d'un accès aux données personnelles[88]. Dans d'autres zones, le modèle d'extension de vie personnelle protège les individus contre la collecte insidieuse de données personnelles par des acteurs privés. Bien qu'il soit considéré comme un frein au développement de l'économie numérique, ce modèle est majoritairement défendu par la population.

[86] Bazoge, Mickaël. Le gouvernement britannique prépare une action choc contre le chiffrement de bout en bout. *iGeneration*, 17 janvier 2022.

[87] Koenig, Gaspard: « Chaque citoyen doit pouvoir vendre ses données personnelles ». Les Echos.

[88] Lausson, Julien. Un assureur américain baisse ses prix si le client accepte d'utiliser un bracelet de santé, 20 septembre 2018

En conséquence, la prolifération des organes de régulations et des agences étatiques sur le numérique dans tous les pays entraîne une absence de clarté sur les règles à respecter, devenant un champ de bataille de *soft power* et d'influence économique. Les régulations restent sujettes à interprétation, notamment en Europe où de nouvelles directives sont créées, mais implémentées de façon hétérogène. Finalement, le modèle économique de grands acteurs numériques est mis à mal dans plusieurs zones géographiques.

Certains services ferment, d'autres basculent vers des modèles payants. De nouvelles logiques de valorisation des données émergent, et deviennent sujettes à de nombreux débats éthiques et technologiques. Finalement, seuls les grands groupes internationaux parviennent à se mettre en conformité face aux nombreuses régulations, acceptant souvent le plus souvent de payer les amendes. Face à ce flou dues à la multiplicité des régulations, les cyberattaquants en profitent pour lancer des attaques d'un nouveau type, non plus basé sur la détention et la menace de suppression ou de revente des données, mais sur la dénonciation possible aux régulateurs pour non-conformité. Ces pratiques d'extorsion redoutablement efficaces font que le nombre de victimes et le gain des cyberattaques s'envolent, favorisant le développement économique des filières criminelles. Les attaques deviendront ainsi plus faciles, ciblées et discrètes.

Finalement, dans les années à venir, notamment à l'horizon 2030, les attaques vont se multiplier, se complexifier dans la technologie utilisée et dans les modes d'actions employés. Les impacts seront plus dévastateurs encore dans une société qui se transforme numériquement et voit les systèmes informationnels et technologiques devenir de plus en plus connectés. Dans ce contexte, le décalage entre la rapidité d'action des cybercriminels et les temps de détection va devoir progresser au risque de voir les cyberattaquants rester impunis.
Il va falloir accroître le renforcement de la solidarité entre les acteurs et normalement la multiplication des ressources humaines ne suffira pas à réduire l'écart dans la durée. De nouvelles techniques éprouvées permettent déjà d'automatiser un certain nombre de processus comme l'utilisation d'Intelligence Artificielle couplé à du Machine Learning.

III. Anticipations et moyens de défense contre les nouvelles menaces cyber

Dans un contexte où la transformation numérique ne cesse de s'accélérer, le campus Cyber, projet initié par le président de République, rassemblant les principaux acteurs nationaux et internationaux du domaine de la cybersécurité, prospecte l'avenir du numérique et explique qu'à horizon 2035 : "*deux facteurs majeurs vont déterminer l'évolution de la problématique de la cybersécurité : le degré d'accélération de la transformation digitale et l'évolution de l'environnement extérieur au cyberespace (coopération entre États, respect de l'État de droit, conjoncture économique et sociale, stratégies gouvernementales mises en œuvre, etc.)*"[89].

La numérisation accélérée liée à la pandémie de COVID-19 a considérablement influencé le développement d'un certain nombre de cybermenaces, selon la nouvelle édition de l'évaluation de la menace de la criminalité organisée sur le site Internet d'Europol[90]. À l'avenir, face à la menace croissante, le maintien et le renforcement d'une méthodologie stratégique de défense et d'anticipation seront nécessaires pour tous les acteurs, public et privé, faisant l'objet de : cyberactivisme,

[89] Construisons ensemble une société numérique de confiance. *Campus.*
[90] *The International Criminal Police Organization. Interpol.*

cybercriminalité, cyberespionnage, cyberterrorisme et cyberguerre. L'identification des nouvelles vulnérabilités nécessite un plan d'orientation stratégique à adapter à son activité[91] :

- **Rechercher :** adopter une stratégie d'acquisition de données brutes par les moyens d'outils suivants ; la veille, l'OSINT, le BLACKINT/DARKINT et le SOCMINT.
- **Exploiter :** contextualiser les données brutes par l'intelligence humaine et en dégager des renseignements utiles.
- **Diffuser :** dresser des recommandations stratégiques pour les décideurs, partager le retour d'expérience.

A) Le renforcement des moyens de défense traditionnels face aux nouvelles menaces

Les principaux agents de menace dans le cyberespace sont les entreprises, les cybercriminels, les employés, les hacktivistes, les États-nations et les terroristes[92]. Un renforcement et une vigilance de la CTI sont indispensables pour lutter contre les menaces, l'OSINT, bien que nécessaire s'en retrouve juridiquement limité.

1. Les défis de la Cyber Threat Intelligence : une capacité de défense renforcée

La raison d'être du renseignement sur les cybermenaces (CTI) est de fournir des connaissances significatives sur les menaces pour la cybersécurité. Cybersécurité et renseignement sont intimement liés : l'augmentation considérable des données et la diversité des canaux de partage impliquent une étroite collaboration entre ces deux sphères. Des renseignements sur les menaces inexacts, incomplets ou obsolètes constituent un problème majeur, seule une CTI de haute qualité peut être utile pour détecter les cyberattaques et s'en défendre. À l'avenir, la nécessité d'une meilleure collaboration peut être réalisée par le biais d'une base de données. Un partage des menaces, sera essentielle pour (1) signaler toute nouvelle vulnérabilité (2) augmenter l'efficacité du travail d'identification et de désamorçage de la menace. Le nombre, mais aussi la complexité des attaques a augmenté depuis 2010, ce qui se traduit par des intrusions réussies avec des formes plus graves de violations de la sécurité. Pour les organisations individuelles, il est presque impossible de détecter ces attaques complexes et décentralisées.[93]

Illustration de défense européenne contre les menaces : le cas polonais :

L'évaluation des risques en temps réel est très importante, compte tenu de la nature des menaces évolutives que représentent les attaquants et les groupes criminels électroniques. En 2019, l'étude de Janiszewski, Marek, Anna Felkner, and Piotr Lewandowski. « *A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Intelligence.* » développent une plateforme nationale polonaise de cybersécurité en utilisant la CTI[94]. L'outil évalue le risque numérique en temps réel, et produit une analyse globale sur l'ensemble des cybermenaces destinées à la Pologne. La plate-forme à plusieurs objectifs : la surveillance de l'espace de cybersécurité, la détection précoce des menaces et la préparation des mesures contre les dangers à l'avance. La Pologne est le premier pays européen qui utilise les menaces intelligentes.

[91] Le renseignement sur les cybermenaces ou Cyber Threat Intelligence, activité indispensable aux décideurs, dans une logique d'anticipation défensive et proactive. *Cyber-day.info - Journée de conférences et d'échanges. Cyber-sécurité - Cyber-crises*.

[92] ENISA. Aperçu du renseignement sur la cybermenace.

[93] Schlette, Daniel et al. Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, 2020.

[94] Janiszewski, Marek. A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Intelligence. 2019.

À titre d'exemple en criminalistique :
La cybercriminalité recouvre une dimension importante eue égard à la diversité des actes illicites commis, à son caractère internationalisé, aux dommages causés aux États, aux entreprises et aux personnes[95]. Le Rapport d'information 2020 du Sénat : « *Cybercriminalité : un défi à relever au niveau national et européen* » affirme qu'il est « *difficile* » de quantifier « l'*ensemble des infractions* ». L'évaluation du produit de la cybercriminalité fait l'objet d'« *une grande incertitude* »[96]. La Threat Intelligence permet de croiser un grand nombre de données pour dresser une typologie criminelle, faciliter la prévention des menaces et à défaut l'appréhension des auteurs. Chaque niveau de la Cyber Threat Intelligence (stratégique, technique et opérationnel) contribue à une meilleure anticipation des cyber risques. En partageant leurs analyses sur les comportements des cybercriminels et des modes opératoires, les analystes en Cyber Threat Intelligence améliorent leurs connaissances des cybermenaces pour : renforcer leurs capacités de détection, anticiper les nouveaux risques et lutter ensemble contre les cyberattaques.

2. L'OSINT : moyens de défense juridiquement limités contre les nouvelles menaces
L'utilisation de l'OSINT est une démarche fondamentale pour toute entité qui protège son système d'information contre les menaces émergentes. Nico Dutch affirme que l'OSINT a "*amorcé sa transformation depuis 2018 et l'avènement du RGPD*". Avec le règlement européen s'accompagnent des impératifs juridiques qui limitent fortement la mise en application de l'OSINT et de la CTI. La mise en application du RGPD pose un véritable problème de posture et de mise en conformité pour les professionnels et les entreprises opérant dans ce milieu. " *l'avenir de l'OSINT fait face au cloisonnement de l'information*" soumis à certains principes énoncés dans le II ci-dessus[97].

Le comportement de pratiquants qui collectent et stockent des données sans reconnaître de responsabilité vis-à-vis de ces mêmes données limite la portée et le moyen d'action de l'OSINT. Pourtant, le propre de la démarche est de rendre ce dernier conforme avec la réglementation en vigueur. Face à l'évolution des menaces, le cadre législatif se confronte à une contradiction, il restreint aussi bien, la cyberdéfense des entités publiques et privées qu'ils les protègent.

B) Les infrastructures numériques et l'Union européenne, garants d'une cyberdéfense effective
Les cybermenaces et les cyberattaques ont désormais évolué. Ces dernières nécessitent une nouvelle approche renforcée de défense et de sécurité (1) développé par l'Union européenne
(2).

1. Le renforcement des infrastructures pour assurer une cyberdéfense performante
Le renseignement issu de la CTI permet de comparer l'émergence de nouvelles menaces aux mesures que l'on peut mettre en place afin de les détecter et de les contrer. Cependant, l'apparition d'une nouvelle technique d'attaque limite dans le temps, le moyen de défense utilisé. En cause, le système dans sa configuration actuelle n'est pas en mesure de détecter ou de contrer la cybermenace. Afin d'assurer un niveau constant de sécurité des données, l'infrastructure doit être anticipée et renforcée pour évoluer.

[95] Pereira, Brigitte. La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité. *Revue internationale de droit économique* [en ligne]. 2016.
[96] Cybercriminalité : un défi à relever aux niveaux national et européen. *Accueil – Sénat*.
[97] Threat Intelligence - Renseignement & ; Cybersécurité,. *Devoteam France*.

L'Agence européenne pour la cybersécurité (ENISA), agence de l'Union européenne qui vise à garantir un niveau élevé commun de cybersécurité dans toute l'Europe utilise un modèle de paysage des cybermenaces, composé de scénarios de menaces. Ces scénarios comprennent des méthodes et techniques d'attaque, des logiciels malveillants et des menaces physiques[98].

La défense se fera de manière cyber, mais aussi au niveau des infrastructures physiques. De cette manière, les attaques contre les infrastructures critiques et les infrastructures TIC d'un pays sont considérées comme les menaces les plus importantes. Les États étant de plus en plus dépendant de structures en réseau, ces cibles sont considérées comme vitales pour le fonctionnement de la société. Les systèmes de contrôle numérique (Supervisory Control and Data Acquisition, SCADA) qui gèrent le réseau électrique et l'approvisionnement en eau sont les systèmes clé des fonctions critiques de la société. Lorsque leurs commandes ont été remplacées par des systèmes modernes en réseau, leur vulnérabilité a augmenté. Par conséquent, la menace d'une attaque s'en est trouvée accrue.

2. Le rôle de l'Union européenne dans le renforcement de la cyberdéfense face aux nouvelles menaces

> "*Prévenir et combattre la cybercriminalité, de même que renforcer la cybersécurité, constituent des priorités d'action de la stratégie de sécurité intérieure renouvelée pour l'Union européenne 2015-2020, adoptée en juin 2015*", le Rapport d'information 2020 du Sénat : "Cybercriminalité : un défi à relever aux niveaux national et européen" rappel les ambitions européennes en matière de cyberdéfense face à la hausse des menaces : "*Cet axe est abordé dans cette stratégie sous deux angles : d'une part, l'attention particulière portée à la promotion de technologies de l'information et de communication sûres et sécurisées afin de renforcer la cybersécurité25(*) au sein de l'Union, et, d'autre part, sur un plan opérationnel, le rappel du rôle de premier plan que doit jouer le cycle politique de l'Union européenne26(*) pour lutter contre la criminalité organisée*"[99].

La Commission européenne a dévoilé ses objectifs en termes de cybersécurité pour les prochaines années. En revenant sur sa capacité de résilience du COVID-19, elle affirme que "*les institutions et les États membres de l'UE ont réagi à l'augmentation des risques liés à la cybersécurité découlant de la crise en intensifiant l'échange d'informations et en améliorant le niveau de préparation à une crise informatique potentielle*". Différentes actions ont été mises en œuvre[100]:

- Coopération de l'UE renforcée dans les institutions concernées (groupe de coopération SRI et réseau des centres de réponse aux incidents de sécurité informatique (CSIRT).
- Simulation Blue OLEx («*Blueprint Operational Level Exercise*») 2020, organisé, dans le cadre du réseau CyCLONe (« *Cyber Crisis Liaison Organisation Network* ») (plan de réaction rapide d'urgence en cas de cyberincidents ou de crises transfrontières).
- Adoption des premières sanctions de l'UE le 30 juillet 2020 par le Conseil. A la suite à des cyberattaques à l'encontre de l'OIAC Organisation pour l'interdiction des armes chimiques (OIAC) et de celles de « *WannaCry* », « *NotPetya* » et « *Operation Cloud Hopper* ».

Juhan Lepassaar, directeur général de l'Agence européenne chargée de la sécurité des réseaux et de l'information, estime que l'approche de l'Union européenne en matière de sécurité de l'information « *peut encore être largement améliorée* ». Il ajoute que « *les institutions européennes dépensent*

[98] ENISA. Aperçu du renseignement sur la cybermenace.

[99] Cybercriminalité : un défi à relever aux niveaux national et européen. *Accueil – Sénat*.

[100] *EUR-Lex — Access to European Union law — choose your language*.

actuellement en moyenne 41 % de moins en sécurité de l'information que leurs homologues américaines ». Les entreprises européennes seraient moins informées sur les menaces et leurs conséquences liées à l'étendue des volumes de données personnelles sensibles liées à l'identité de leurs employés qui sont accessibles au public ou en vente sur le dark web[101].

L'ENISA utilise un modèle de cybermenace composé de menaces. Elles comprennent différentes formes d'attaques et de techniques, ainsi que des logiciels malveillants et des menaces physiques. Dans son modèle, « *un agent de menace est toute personne ou chose qui agit (ou a le pouvoir d'agir) pour provoquer, porter, transmettre ou soutenir une menace* »[142] :

- Renforcement du CTI en tenant compte des évolutions observées dans les États membres, la Commission européenne et d'autres organismes européens, les fournisseurs et les utilisateurs finaux du CTI.
- Le renforcement de la coopération des activités du CTI à l'échelle de l'UE entre les États membres.
- Le développement d'un modèle de maturité pour le CTI.
- La consolidation et la diffusion du contenu CTI multifonctionnel et utile, tel que la hiérarchie des menaces utilisable dans d'autres domaines (par ex., la certification, la gestion des risques, les paysages sectoriels, etc.).

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) en 2019 a entrepris des travaux stratégiques et collaboratifs : ANSSI10+ : L'agence dévoile sa stratégie sur 3 piliers pour anticiper les menaces[102] :

- Un rôle d'éclaireur des transformations numériques.
- Renforcement de l'efficacité opérationnelle face à des menaces "*profondément changeantes, notamment face à la recrudescence des menaces de masse*" et "et inventer les moyens de la cybersécurité de demain".
- Renforcement de la connaissance informatique et de ses vulnérabilités par la formation initiale.

Cas pratique : L'avenir de la cybersécurité : 3 scénarios à envisager selon la société PWC.
"*Quel avenir en matière de cybersécurité ? La question est légitime au vu de l'explosion de la cybercriminalité dans le monde*".

[101] ENISA. Aperçu du renseignement sur la cybermenace
[142] Ibid.
[102] Notre stratégie. *ANSSI*.

PWC affirme que "*deux facteurs majeurs vont déterminer l'évolution de la problématique de la cybersécurité au cours des dix prochaines années : le degré d'accélération de la transformation digitale et l'évolution de l'environnement extérieur au cyberespace (coopération entre États, respect de l'État de droit, conjoncture économique et sociale, stratégies gouvernementales mises en œuvre, etc.)*". Ces scénarios développent des compétences nécessaires à la connaissance des nouvelles menaces et à la mise en place d'une cyberdéfense efficiente[103].

C) L'avenir du facteur humain : « *Exploiter le renseignement sur la menace cyber pour sensibiliser et former à la sécurité* »

Le rapport du Forum Économique Mondial a publié en janvier 2022, relatif aux risques mondiaux, informe que « *95 % des failles de cybersécurité sont dues à des erreurs humaines* »[104]. La société IBM, rapporte que « *s'il était possible de soustraire l'erreur humaine de l'équation, 19 failles de sécurité sur 20 ne se produiraient pas* »[105]. Les erreurs commises par les administrateurs réseau et les utilisateurs ; incapacité à corriger les vulnérabilités dans les systèmes anciens, mauvaise configuration des paramètres, non-respect des procédures standards ouvrent la porte à l'immense majorité des attaques réussies (1) [106]. Face à l'insuffisance des technologies numériques, des

[103] L'avenir de la cybersécurité : 3 scénarios à envisager. *PwC* .

[104] Le tournant cognitif de la cybersécurité : changement de paradigme et prolégomènes à la cybersécurité cognitive. *European Scientist* .

[105] Cost of a Data Breach Report 2021. *IBM - Deutschland | IBM*.

[106] Chauvin, Sandrine. Facteur humain et cybersécurité : les leçons du Pentagone. 14 janvier 2016.

infrastructures et de la législation, les entités publiques et privées s'attachent à créer une culture de la sensibilisation à la cybersécurité (2).

1. La multiplication du risque humain : cible privilégiée des cybercriminels
Si l'élément humain représente la première ligne de défense, il constitue également le maillon le plus faible de la chaîne de protection des données. Vulnérabilité bien comprise des cybercriminels, ils vont chercher à exploiter simultanément les failles systèmes et le facteur humain en multipliant les stratégies d'attaques personnalisées : collecte de l'information, identification des interlocuteurs grâce aux informations disponibles sur le web et les réseaux sociaux.

La peur et le stress sont créés et déclenchés artificiellement par les cyberattaquants auprès de leur cible, avec un impératif de rapidité afin de ne pas laisser le temps aux équipes informatiques ou à l'utilisateur pour réagir. Les approches psychologiques utilisées rendent les victimes démunies face à la sophistication des attaques. Désormais, admettre ce caractère faillible de l'Humain est « *primordial* »[107].
Illustration de risques dus au facteur humain :

- **Le non-respect des procédures** : en 2008, un membre du commandement militaire américain basé au Moyen-Orient a inséré dans un ordinateur sécurisé une clé USB contenant un logiciel malveillant. En 2016, l'article « *Facteur humain et cybersécurité : les leçons du Pentagone. Facteur humain et cybersécurité : les leçons du Pentagone* » qualifiait cette attaque comme « *la plus grave d'un réseau classifié* ».
- **La responsabilité du fait des informaticiens** : en 2014, l'envoi d'un courriel d'hameçonnage a compromis les données de vérification de plusieurs administrateurs système. Au total, ce sont 80 millions clients de l'assureur Anthem qui ont été victimes de vol des données personnelles.
- **Le manquement à une procédure de mise à jour** : en 2015, un compte Twitter personnel au sein du commandement militaire américain a « *brièvement* » été contrôlé par l'organisation État islamique. En l'absence de mise à jour, le compte ne disposait donc pas de l'authentification à deux facteurs : la confirmation de l'utilisateur du compte par mot de passe et la « *génération de nombres aléatoires ou d'une puce encryptée* »[108].

2. La sensibilisation sur les formes de cybercriminalité : moyen d'anticipation contre l'erreur humaine
Michel Gérard Président Directeur Général de la société Olsféo, affirme que la sensibilisation à la sécurité des risques cyber « *marche* ». Il explique qu'à ce jour, « *70 à 95 % des infections sont liées à des défauts de comportement des utilisateurs. Une étude menée par Aberdeen Group expliquait même que sensibiliser pouvait réduire les incidents liés à la sécurité de l'ordre de 60 % ! »,* ainsi, à l'avenir, *« l'objectif, c'est de faire de l'humain un maillon fort, car la sécurité ce ne sont plus seulement des process, des normes et de la technologie ».* Il assure enfin que *« si l'on avait mis autant d'énergie et d'argent sur la sensibilisation des personnes que pour les infrastructures, il y aurait bien moins d'attaques réussies aujourd'hui*. » [109]. Les organisations privées et publiques seront amenées à développer une meilleure culture de la sécurité pour faire changer les comportements, améliorer la protection globale de l'entité et créer de nouveaux réflexes de méfiance. Le groupe Orange Cyberdéfense dans son étude sur « *la*

[107] Failles de cybersécurité : la nécessité de reconnaître le facteur humain. *Orange Cyberdefense : Region and language selection page*.
[108] Ibid.
[109] *Inforisque, Risques professionnels et prévention SST*.

nécessité de reconnaître le facteur humain » de 2022, relève deux niveaux de renforcement du facteur humain[110]:

- **La sensibilisation** sur toutes les formes de cybercriminalité (phishing, ingénierie sociale, désinformation, etc.). Elle inclut une communication autour des répercussions (financiers ou de réputation) d'une cyberattaque ainsi qu'une formation des collaborateurs.
- **Le recrutement** : « *Le paysage des menaces évolue et les profils attendus aussi* ». Les nouveaux profils seront évalués sur leurs capacités d'adaptation et de gestion liées aux nouvelles menaces et aux nouvelles vulnérabilités.

Illustration sur la prévention du comportement en entreprise :

- **La gestion des mots de passe** : la quasi-totalité des chartes informatiques exige désormais des mots de passe « compliqués » avec des majuscules, minuscules, chiffres voire caractères spéciaux… La société Olféo affirme que les utilisateurs n'ayant pas connaissance de cette exigence de sécurité font usage de mots de passe : « Password1 », « P@ssword1 » ou « Nomdel'entreprise01 ». Ainsi, l'entreprise doit accompagner le facteur humain et le faire évoluer afin qu'il devienne un « *maillon plus fort de la chaîne de sécurité* »[111].

  Protéger les utilisateurs et les organisations s'appliquera de la manière suivante :
  - **La récurrence** : développement d'une stratégie de communication continue.
  - **Adapter le message de sensibilisation à chaque niveau d'interlocuteur** : rendre régulières et accessibles des informations complexes.
  - **Mise en application concrète des moyens de prévention dans le temps** : pédagogie, jeux de rôle ou encore prospective[112].

Illustration sur la prévention du facteur humain : en France :

Au niveau étatique, l'évoluent et la prise en compte du facteur humain se développe progressivement. Les pouvoirs publics ont créé Cybermalveillance, la plateforme a pour mission d'« *assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance* »[113]. Des campagnes de sensibilisation régulière et la mise en place d'outils de sécurité adaptés ont été mises en place[114]. Franck Gicquel, Responsable des partenariats au sein de Cybermalveillance, explique, au sujet des utilisateurs, qu'« *il faut revenir aux fondamentaux en leur parlant d'abord des usages dans leur vie personnelle si l'on veut réussir à les impliquer davantage puis à les rapprocher avec les enjeux de sécurité business. C'est pour cela que Cybermalveillance. gouv.fr met à disposition son kit de sensibilisation des collaborateurs composé autour d'outils ludiques…* ».

Illustration sur la lutte contre le facteur humain : le cas des États-Unis :

Afin de lutter contre les risques liés au facteur humain en cybersécurité, trois auteurs,
Sandy Winnefeld, Christopher Kirchhoff et David M. Upton, ont présenté dans leur recueil de 2021 « *Facteur humain et cybersécurité : les leçons du Pentagone. Facteur humain et cybersécurité : les leçons du Pentagone* », une méthodologie issue du cybercommandement américain, développer par l'amiral

[110] Failles de cybersécurité : la nécessité de reconnaître le facteur humain. *Orange Cyberdefense : Region and language selection page*.
[111] *Inforisque, Risques professionnels et prévention SST*.
[112] *Ibid.*
[113] Dispositif d'assistance aux victimes d'actes de cybermalveillance.
[114] *Inforisque, Risques professionnels et prévention SST*.

Hyman Rickover, « *père de la marine nucléaire* », spécialisé en sûreté nucléaire en 2009. Utilisé par le Pentagone, l'objectif est d'exporter la méthodologie aux dirigeants d'entreprise. La technique est la suivante : « *Des capteurs, des fonctions analytiques et des « piles de sécurité » sophistiquées (ensembles de logiciels réalisant diverses fonctions, notamment l'analytique du big data)* » offrent aux administrateurs réseau une grille de lecture globale sur les menaces et un champ de modification des configurations réseau en conséquence en cas d'attaque.
L'analyse de l'amiral Mike Rogers, superviseur du cyber commandement américain, conclu de la manière suivante, à l'avenir : « *Nous devons aller au-delà du seul volet technique.*
C'est une question d'éthique. Une question de culture. [Il s'agit de savoir] comment on recrute, on forme et on arme son entreprise, comment on la structure, quels concepts opérationnels on y applique. »[115].

[115] CHAUVIN, Sandrine. Facteur humain et cybersécurité : les leçons du Pentagone. 14 janvier 2016.

Conclusion

Au travers de ce rapport, nous venons de voir que l'apport du cyber dans les techniques d'investigation actuelles et futures est essentiel.
Nous avons commencé par l'état des lieux de la cybercriminalité en France et vu de quelle manière l'État opère pour lutter. Ces dernières années, les cyberattaques ont visé plus directement des intérêts politiques et économiques, en opération des altérations ou des espionnages des réseaux de communication, avec une augmentation de 50% des attaques envers les collectivités publiques en 2020. La crise sanitaire a permis de s'en rendre compte avec les hôpitaux, victimes de phishing, d'attaques DDoS ou, comme à Angers, de ransomwares. Dans le secteur technologique, il va y avoir un vrai défi de sécurité avec les 35 milliards d'objets connectés (IoT), prévus d'ici à 2030.
Face à la professionnalisation croissante des réseaux de cybercriminels, nous avons vu que la politique de cybersécurité française s'est caractérisée par son volontarisme. Que ce soit dans le secteur public, avec une augmentation des recrutements et des budgets alloués à la cybersécurité, ou dans le secteur privé avec un chiffre d'affaires de la cybersécurité en croissance constante.
Le projet de Cyber Campus, représente l'élément le plus récent dans cette la vision de l'État. Permettant de mutualiser les activités de veille et d'analyse, de formation et d'innovation ainsi qu'une collaboration plus étroite entre secteurs publics et privés.

Nous avons poursuivi en nous focalisant sur les outils au service d'investigations au profit des cyber enquêteurs. En effet, avec pratiquement 5 milliards d'humains connectés à Internet, le nombre de données produites est un véritable défi d'analyse. Surtout que le renseignement d'origine cyber exploite les données accessibles en source ouverte (OSINT). Les renseignements cyber s'appuient sur des méthodes d'analyse différentes, la due diligence, l'empreinte numérique et le renseignement par réseaux sociaux ou SOCMINT. Ces opérations de récupération d'informations étant bien évidemment, plus efficaces combinées ensemble.
Le renseignement d'intérêt cyber, (CTI), s'intéresse lui à l'espace cyber pour récupérer les informations. Cela passe par la connaissance du matériel et ses failles, et se base pour cela sur trois méthodes d'analyse, la *forensic*, qui se focalise sur la récupération et l'étude des supports numériques corrompus, et la rétro-ingénierie.

La combinaison du CTI et de l'OSINT permet d'avoir une vision efficace de la surface d'exposition d'une organisation ou d'une société.
La géopolitique va voir les puissances internationales s'opposer bien plus dans le monde numérique. Mais aussi sur des enjeux de *hardware* technologiques, comme les semi-conducteurs, notamment avec ceux qui détiennent les chaînes d'approvisionnement ou les ressources.
Il a aussi été question de l'évolution et de l'anticipation des cyber menaces, avec une focale sur les menaces cyber en provenance du Dark Web et de l'utilisation accrue de l'intelligence artificielle et du Machine Learning dans les nouveaux maliciels. Au cœur des logiciels malveillants, une utilisation accrue de l'Intelligence Artificielle et du Machine Learning va complexifier le repérage et la lutte contre ces logiciels, car ils seront capables d'évoluer, compliquant le travail de ceux qui luttent contre les maliciels.
Nous avons aussi vu les scénarios d'anticipation avec ce que risquent probablement d'être les menaces dans le futur. En effet, l'ultra connectivité, le cloisonnement des réseaux et les multiples réglementations vont poser de nombreux défis dans la lutte contre les cyberattaquants dans le futur.
Ainsi, il sera important de prendre en compte le facteur humain, qui est capital dans la lutte cyber. En effet, nous avons vu que 95% des failles en cybersécurité sont dues à des erreurs humaines. Sans le facteur humain, 19 failles de sécurité sur 20 ne se produiraient pas. C'est sur ces failles humaines que

les cybers attaquants misent. C’est pourquoi la formation est très importante et que les cyberattaques pourraient être réduites de 60% en cas de formation des utilisateurs.

Sources :

PARTIE 1 - ÉTATS DES LIEUX DES MENACES & MESURES
Cybercriminalité, cyber attaques: une notion à géométrie variable
AMICELLE, Anthony et al. Criminology in the face of flows : reflections on contemporary policing and security. *Global Crime* [en ligne]. 2017, **18**(3), 165–175. ISSN 1744-0580
[consulté le 31 mai 2022]. Disponible sur : doi:10.1080/17440572.2017.1350427

CAULIER, Sophy. Comment les acteurs du cybercrime se professionnalisent. *Le Monde.fr* [en ligne]. 15 novembre 2020 [consulté le 31 mai 2022]. Disponible sur : https://www.lemonde.fr/economie/article/2020/11/15/comment-le-cybercrime-sehttps://www.lemonde.fr/economie/article/2020/11/15/comment-le-cybercrime-se-professionnalise-en-s-attaquant-aux-particuliers-et-aux-entreprises_6059830_3234.htmlprofessionnalise-en-s-attaquant-aux-particuliers-et-aux-entreprises_6059830_3234.html

Criminalité informatique : menaces, pratiques de sécurité. *WikiMemoires* [en ligne]. 1 février 2021 [consulté le 31 mai 2022]. Disponible sur : https://wikimemoires.net/2021/02/criminalitehttps://wikimemoires.net/2021/02/criminalite-informatique-menaces-pratiques-de-securite/ - stoc-la-criminalite-informatiqueinformatique-menaces-pratiques-de-securite/#stoc-la-criminalite-informatique

Cyber Crime [en ligne]. 8 avril 2020 [consulté le 31 mai 2022]. Disponible sur : https://cybercrime-fr.org/wp-content/uploads/2020/04/8.pdf

Cybercriminalité : mythe ou réalité ? *Centre international de criminologie comparée* [en ligne]. 2 février 2017 [consulté le 31 mai 2022]. Disponible sur : https://www.cicchttps://www.cicc-iccc.org/public/media/files/prod/banque_fichiers_events/499/FredericGaudreau.pdficcc.org/public/media/files/prod/banque_fichiers_events/499/FredericGaudreau.pdf

Cybersécurité : comment l'UE lutte contre les cybermenaces. *Home - Consilium* [en ligne]. 18 mai 2022 [consulté le 31 mai 2022]. Disponible sur : http://www.consilium.europa.eu/fr/policies/cybersecurity

Cybersécurité, faire face à la menace : la stratégie française. *ANSSI* [en ligne]. 1 février 2021 [consulté le 1 juin 2022]. Disponible sur : https://www.ssi.gouv.fr/actualite/cybersecurite-fairehttps://www.ssi.gouv.fr/actualite/cybersecurite-faire-face-a-la-menace-la-strategie-francaise/face-a-la-menace-la-strategie-francaise/

Cybersécurité : l'action du ministère en chiffres. *http://www.interieur.gouv.fr/Archives/Archives-des-actualites/2019-Actualites/Le-ministere*http://www.interieur.gouv.fr/Archives/Archives-des-actualites/2019-Actualites/Le-ministere-present-au-FIC-2019/Cybersecurite-l-action-du-ministere-en-chiffres*present-au-FIC-2019/Cybersecurite-l-action-du-ministere-en-chiffres* [en ligne]. 18 janvier 2019 [consulté le 31 mai 2022]. Disponible sur : https://www.interieur.gouv.fr/Archives/Archives-des-actualites/2019-Actualites/Le-ministerehttps://www.interieur.gouv.fr/Archives/Archives-des-actualites/2019-Actualites/Le-ministere-present-au-FIC-2019/Cybersecurite-l-action-du-ministere-en-chiffrespresent-au-FIC-2019/Cybersecurite-l-action-du-ministere-en-chiffres

Décret n°2000-405 du 15 mai 2000 portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. *Légifrance* [en ligne]. 15 mai 2000 [consulté le 31 mai 2022]. Disponible sur : http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000765391&categorie Lien=id

DEFNET 2021 | la chaîne de cyberdéfense : CALID, CASSI et CRPOC. *Ministère des Armées | Ministère des Armées* [en ligne]. 18 mai 2021 [consulté le 31 mai 2022]. Disponible sur : https://www.defense.gouv.fr/terre/actualites/defnet-2021-chaine-cyberdefense-calid-cassihttps://www.defense.gouv.fr/terre/actualites/defnet-2021-chaine-cyberdefense-calid-cassi-crpoccrpoc

En cas d'incident. *ANSSI* [en ligne]. [sans date] [consulté le 31 mai 2022]. Disponible sur : https://www.ssi.gouv.fr/en-cas-dincident

ESTANO, Nicolas. Nouvelles technologies et cyberharcèlement : l'exemple du swatting. *Criminologie* [en ligne]. 2019, **52**(2), 13. ISSN 1492-1367 [consulté le 31 mai 2022]. Disponible sur : doi:10.7202/1065854ar

FORTIN, Francis et Olivier DELÉMONT. La criminologie de l'information : état des lieux et perspectives. *Criminologie* [en ligne]. 2019, **52**(2), 5. ISSN 1492-1367 [consulté le 31 mai 2022]. Disponible sur : doi:10.7202/1065853ar

HASSID, Olivier et Christian AGHROUM. *Les entreprises et l'État face aux cybermenaces*. Paris : L'Harmattan, 2013. ISBN 9782343012339.

La criminologie de l'information : état des lieux et perspectives – Criminologie. *Érudit* [en ligne]. [sans date] [consulté le 31 mai 2022]. Disponible sur : doi:10.7202/1065853ar

Notre plateforme. *Assistance aux victimes de cybermalveillance* [en ligne]. 19 août 2019 [consulté le 31 mai 2022]. Disponible sur : https://www.cybermalveillance.gouv.fr/tous-noshttps://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/la-plateforme-cybermalveillance-gouv-frcontenus/a-propos/la-plateforme-cybermalveillance-gouv-fr

Panorama de la menace informatique 2021. *CERT-FR - Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques* [en ligne]. 1 janvier 2021 [consulté le 31 mai 2022]. Disponible sur : https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menacehttps://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdfANSSI.pdf

Policier investigateur en cybercriminalité. *Page d'accueil | Police nationale* [en ligne]. 1 février 2022 [consulté le 3 juin 2022]. Disponible sur : https://www.devenirpolicier.fr/metiers/enqueter/policier-investigateur-en-cybercriminalite

Policier investigateur en cybercriminalité. *Site du Ministère de l'Intérieur* [en ligne]. 1 janvier 2017 [consulté le 31 mai 2022]. Disponible sur : https://www.interieur.gouv.fr/content/download/69214/504609/file/Policier%20investigateur %20cybercriminalité.pdf

Sous-direction de lutte contre la cybercriminalité. *https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte*https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite*contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite* [en ligne]. 23 février 2022 [consulté le 3 juin 2022]. Disponible sur : https://www.policehttps://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalitenationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Luttehttps://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalitecontre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite

II. Typologie des groupes criminels & modes opératoires

Bancal, D. (2022, 10 janvier). *Le secteur industriel plus que jamais menacé – Data Security Breach*. Data Security Breach – L'actualité cybersécurité pour PME/PMI/TPE. https://www.datasecuritybreach.fr/secteur-industriel-plus-que-jamaishttps://www.datasecuritybreach.fr/secteur-industriel-plus-que-jamais-menace/menace/

Berthier, T. (2019). Cybercriminalité : Le choix des armes. *Diplomatie - Les grands dossiers*, (52), 72.

Bodnar, B. (s. d.). *La Russie est officiellement accusée d'une cyberattaque contre un satellite européen*. Numerama. https://www.numerama.com/cyberguerre/956787-la-russie-esthttps://www.numerama.com/cyberguerre/956787-la-

russie-est-officiellement-accusee-dune-cyberattaque-contre-un-satellite-europeen.htmlofficiellement-accusee-dune-cyberattaque-contre-un-satellite-europeen.html

Bohic, C. (2014, 10 juin). *Sécurité IT : Le poids économique de la cybercriminalité*. ITespresso.fr. https://www.itespresso.fr/securite-it-poids-economique-cybercriminalitehttps://www.itespresso.fr/securite-it-poids-economique-cybercriminalite-76206.html76206.html

Dubois, M. (2022, 17 février). *Une attaque informatique géante, ce cauchemar redouté par les banques du monde entier*. Ouest France. https://www.ouest-france.fr/leditiondusoir/2022-02-17/une-attaque-informatique-geante-ce-cauchemar-redoute-par-les-banques-du-monde-entierhttps://www.ouest-france.fr/leditiondusoir/2022-02-17/une-attaque-informatique-geante-ce-cauchemar-redoute-par-les-banques-du-monde-entier-537001b6-e09d-419e-97a6-8677eac58a74537001b6-e09d-419e-97a6-8677eac58a74

FireEye cyber threat map. (s. d.). FireEye. https://www.fireeye.com/cyber-map/threathttps://www.fireeye.com/cyber-map/threat-map.htmlmap.html

Franceinfo & Fayolle, M. (2021, 24 avril). *ENQUÊTE. La santé, nouveau terrain de jeu des pirates informatiques*. Franceinfo. https://www.francetvinfo.fr/internet/securite-surhttps://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/enquete-la-sante-nouveau-terrain-de-jeu-des-pirates-informatiques_4383561.htmlinternet/cyberattaques/enquete-la-sante-nouveau-terrain-de-jeu-des-pirateshttps://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/enquete-la-sante-nouveau-terrain-de-jeu-des-pirates-informatiques_4383561.htmlinformatiques_4383561.html

Francois, M. (2021, 18 mai). *Comment évoluer vers l'industrie 4.0 en se protégeant des cyberattaques*. JDN : E-business, FinTech, Big Data, IoT, tendances média, décideurs... https://www.journaldunet.com/solutions/dsi/1500987-comment-evoluer-vers-unehttps://www.journaldunet.com/solutions/dsi/1500987-comment-evoluer-vers-une-industrie-4-0-tout-en-se-protegeant-contre-l-augmentation-des-cyber-attaques/industrie-4-0-tout-en-se-protegeant-contre-l-augmentation-des-cyber-attaques/

Gendre, A. (2022, 12 mai). *[Tribune] Cyberattaques contre les administrations : Les Français font les frais d'une cyberdéfense défaillante*. Alliancy, le mag Numérique et Business. https://www.alliancy.fr/cyberattaques-administrations-cyberdefense-defaillante Gutman, Y. (2019, 18 novembre). *The education sector and the increasing threat from cybercrime*. SentinelOne. https://www.sentinelone.com/blog/the-education-sector-and-thehttps://www.sentinelone.com/blog/the-education-sector-and-the-increasing-threat-from-cybercrime/increasing-threat-from-cybercrime/

L'Entrepreneur. (s. d.). *Le secteur de l'éducation est le plus susceptible de payer la demande de ransomware, selon un rapport*. https://lentrepreneur.co/innovation/b2b/le-secteur-dehttps://lentrepreneur.co/innovation/b2b/le-secteur-de-leducation-est-le-plus-susceptible-de-payer-la-demande-de-ransomware-selon-un-rapport-14032022leducation-est-le-plus-susceptible-de-payer-la-demande-de-ransomware-selon-un-rapporthttps://lentrepreneur.co/innovation/b2b/le-secteur-de-leducation-est-le-plus-susceptible-de-payer-la-demande-de-ransomware-selon-un-rapport-1403202214032022

Live threat map. (s. d.). Deteque. https://www.deteque.com/live-threat-map/

Mandiant. (s. d.). *Advanced persistent threats (apts) | threat actors & ; groups*. https://www.mandiant.com/resources/apthttps://www.mandiant.com/resources/apt-groups?gclsrc=aw.ds&&utm_source=Google&utm_medium=cpc&utm_campaign=PROD|M-Trends|FR|EN|Performance&utm_content=all&utm_term=en&cid=us&gclid=Cj0KCQjwheyUBhD-ARIsAHJNM-NCRv7EMAQi43Kw5omOhMkvAVACacAtD3YcCGbwHK-GFOlY8-zINakaAssAEALw_wcBgroups?gclsrc=aw.ds&&utm_source=Google&utm_medium=cpc&utm_campaign=PROD|M-Trends|FR|EN|Performance&utm_content=all&utm_term=en&cid=us&gc lid=Cj0KCQjwheyUBhD-ARIsAHJNM-NCRv7EMAQi43Kw5omOhMkvAVACacAtD3YcCGbwHK-GFOlY8https://www.mandiant.com/resources/apt-groups?gclsrc=aw.ds&&utm_source=Google&utm_medium=cpc&utm_campaign=PROD|M-Trends|FR|EN|Performance&utm_content=all&utm_term=en&cid=us&gclid=Cj0KCQjwheyUBhD-ARIsAHJNM-NCRv7EMAQi43Kw5omOhMkvAVACacAtD3YcCGbwHK-GFOlY8-zINakaAssAEALw_wcBzINakaAssAEALw_wcB

MAP | kaspersky cyberthreat real-time map. (s. d.). MAP | Kaspersky Cyberthreat real-time map. https://cybermap.kaspersky.com/

Mercourt, L. (2022, 29 mars). *Les enjeux de la cybersécurité dans les banques et assurances*. Freelance.com. https://www.freelance.com/blog/bonnes-pratiques/cybersecurite-banqueshttps://www.freelance.com/blog/bonnes-pratiques/cybersecurite-banques-assurances/assurances/
Rioux, P. (2018, 6 février). *Internet des objets : 35 milliards d'appareils connectés en 2030 selon l'Institut Idate*. ladepeche.fr. https://www.ladepeche.fr/article/2018/02/06/2736948https://www.ladepeche.fr/article/2018/02/06/2736948-internet-objets-35-milliards-appareils-connectes-2030-selon-institut-idate.htmlinternet-objets-35-milliards-appareils-connectes-2030-selon-institut-idate.html

Tehtris. (2022, 5 avril). *Le monde de la santé face aux cyberattaques - TEHTRIS*. TEHTRIS. https://tehtris.com/fr/blog/le-monde-de-la-sante-face-aux-cyberattaques

Threatbutt internet hacking attack attribution map. (s. d.). Threatbutt - comprehensive internet hacking protections. https://threatbutt.com/map/

Threat map. (s. d.). BitDefender. https://threatmap.bitdefender.com/

Worlwide attacks map. (s. d.). SonicWall Security Center. https://securitycenter.sonicwall.com/m/page/worldwide-attacks

PARTIE 2 - LE CYBERESPACE & L'INVESTIGATION: OUTIL MULTI-DOMAINE AU SERVICE DEL'ENQUÊTEUR

I. Approche sémantique & méthodologique: l'apport pratique du cyber en investigation

GAUDIAUT, Tristan. Infographie : Combien y a-t-il d'internautes dans le monde ? *Statista Infographies* [en ligne]. 2021 [consulté le 30 mai 2022]. Disponible sur : https://fr.statista.com/infographie/26337/evolution-du-nombre-de-personnes-ayant-acces-ouhttps://fr.statista.com/infographie/26337/evolution-du-nombre-de-personnes-ayant-acces-ou-pas-a-internet-dans-le-monde/pas-a-internet-dans-le-monde/.

FRANÇOIS-BERNARD HUYGHE. Gagner les cyberconflits. Au-delà du technique - François-Bernard Huyghe,Olivier Kempf,Nicolas Mazzucchi. Decitre.fr : Livres, Ebooks, romans, BD, polars et mangas en ligne [en ligne]. 1 septembre 2015 [consulté le 30 mai 2022]. Disponible sur : https://www.decitre.fr/livres/gagner-les-cyberconflits-9782717868104.html.
Kevin Limonier, « Vers un « Runet souverain » ? Perspectives et limites de la stratégie russe de contrôle de l'Internet », *EchoGéo* [En ligne], 56 | 2021, mis en ligne le 25 juin 2021, consulté le 30 mai 2022. URL : http://journals.openedition.org/echogeo/21804 ; DOI : https://doi.org/10.4000/echogeo.21804.

POIROT Jérôme, « ROSO », dans : Hugues Moutouh éd., Dictionnaire du renseignement. Paris, Perrin, « Hors collection », 2018, p. 677-681. DOI : 10.3917/perri.mouto.2018.01.0677.
URL : https://www.cairn.info/--9782262070564-page-677.htm.

2007 Annual Report of The Congressional Research Service 2007 | PDF | Congressional Research Service | Administrative Law. Scribd [en ligne]. Février 2008 [consulté le 30 mai 2022]. Disponible sur : https://fr.scribd.com/doc/298019914/2007-Annual-Report-of-thehttps://fr.scribd.com/doc/298019914/2007-Annual-Report-of-the-Congressional-Research-Service-2007Congressional-Research-Service-2007.

OMAND, David, Jamie BARTLETT et Carl MILLER. Introducing Social Media Intelligence (SOCMINT). Intelligence and National Security [en ligne]. 2012, 27(6), 801–823. ISSN 17439019 [consulté le 30 mai 2022]. Disponible sur : doi:10.1080/02684527.2012.716965.

Rapport – La galaxie des sites russophones du GRU | OpenFacto. *OpenFacto | Association francophone Spécialisée Enquêtes en Sources Ouvertes* [en ligne]. 19 janvier 2022 [consulté le 30 mai 2022]. Disponible sur :

https://openfacto.fr/2022/01/18/rapport-la-galaxie-des-siteshttps://openfacto.fr/2022/01/18/rapport-la-galaxie-des-sites-russophones-du-gru/russophones-du-gru/.

Live Vs Dead Computer Forensic Image Acquisition. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGIES [en ligne]. 2017 [consulté le 30 mai 2022]. Disponible sur : https://ijcsit.com/docs/Volume%208/vol8issue3/ijcsit2017080331.pdf.

CENTRE CYBER D'EXCELLENCE. référentiel cyber V6. Février 2021 [consulté le 30 mai 2022]. Disponible sur : https://www.pole-excellence-cyber.org/wphttps://www.pole-excellence-cyber.org/wp-content/uploads/2021/06/Brochure-Referentiel-V6.pdfcontent/uploads/2021/06/Brochure-Referentiel-V6.pdf.

II. Cyber Threat Intelligence & OSIN

BROOKS, Chuck. Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know. Forbes [en ligne]. 3 juin 2022 [consulté le 4 juin 2022]. Disponible sur : https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-midyear-2022-that-you-need-to-know/

ÐÐ¾Ð²Ð°Ñ Ð³Ð°Ð·ÐµÑ‚Ð°. ÐÐ¾Ð²Ð°Ñ Ð³Ð°Ð·ÐµÑ‚Ð° [en ligne]. [sans date] [consulté le 4 juin 2022]. Disponible sur : https://novayagazeta.ru

DEVOIR, Le. Les dernières nouvelles de l'invasion de l'Ukraine. Le Devoir [en ligne]. 3 juin 2022 [consulté le 4 juin 2022]. Disponible sur : https://www.ledevoir.com/monde/europe/678927/blogue-en-direct-dernieres-nouvelleshttps://www.ledevoir.com/monde/europe/678927/blogue-en-direct-dernieres-nouvelles-conflit-ukraine-russieconflit-ukraine-russie

GEOFFROY, Romain et al. Guerre en Ukraine : parcourez les infox et les fausses images qui circulent depuis le début de l'offensive russe. Le Monde.fr [en ligne]. 4 mars 2022 [consulté le 4 juin 2022]. Disponible sur : https://www.lemonde.fr/les-decodeurs/article/2022/03/04/guerreen-ukraine-notre-guide-pour-detecter-les-infox-et-les-fausses-images_6116197_4355770.html

Guerre en Ukraine : chronologie des événements - Touteleurope.eu. Touteleurope.eu [en ligne]. [sans date] [consulté le 4 juin 2022]. Disponible sur : https://www.touteleurope.eu/l-ue-danshttps://www.touteleurope.eu/l-ue-dans-le-monde/guerre-en-ukraine-chronologie-des-evenements/le-monde/guerre-en-ukraine-chronologie-des-evenements/

Intelligence artificielle. Prouver les crimes de guerre en Syrie à l'aide d'images synthétiques. Courrier international [en ligne]. [sans date] [consulté le 4 juin 2022]. Disponible sur : https://www.courrierinternational.com/article/intelligence-artificielle-prouver-les-crimes-dehttps://www.courrierinternational.com/article/intelligence-artificielle-prouver-les-crimes-de-guerre-en-syrie-laide-dimages-synthetiquesguerre-en-syrie-laide-dimages-synthetiques

L'Ukraine, victime d'une attaque informatique comme arme de guerre. la revue européenne des médias et du numérique - Home Slider - La revue européenne des médias et du numérique [en ligne]. [sans date] [consulté le 4 juin 2022]. Disponible sur : https://la-rem.eu/2022/05/lukrainehttps://la-rem.eu/2022/05/lukraine-victime-dune-attaque-informatique-comme-arme-de-guerre/victime-dune-attaque-informatique-comme-arme-de-guerre/

"Moscou emploie en Ukraine les mêmes méthodes qu'en Syrie" | DW | 07.04.2022. DW.COM [en ligne]. [sans date] [consulté le 4 juin 2022]. Disponible sur : https://www.dw.com/fr/russiehttps://www.dw.com/fr/russie-ukraine-syrie-fabrice-balanche/a-61399848ukraine-syrie-fabrice-balanche/a-61399848

POMMIERS, Eléa. Que sait-on sur l'empoisonnement de l'ex-agent double russe au RoyaumeUni ? Le Monde.fr [en ligne]. 19 mars 2018 [consulté le 4 juin 2022]. Disponible sur : https://www.lemonde.fr/international/article/2018/03/19/que-sait-on-sur-l-empoisonnementhttps://www.lemonde.fr/international/article/2018/03/19/que-sait-on-sur-l-empoisonnement-de-serguei-skripal-l-ex-agent-double-russe-au-royaume-uni_5273209_3210.htmlde-serguei-skripal-l-ex-agent-double-russe-au-royaume-uni_5273209_3210.html

Removing the guesswork from cybersecurity. Mnemonic [en ligne]. [sans date] [consulté le 4 juin 2022]. Disponible sur : https://www.mnemonic.io

Ukraine : les pays du G7 préviennent que les auteurs de crimes de guerre "devront rendre des comptes". BFMTV [en ligne]. [sans date] [consulté le 4 juin 2022]. Disponible sur : https://www.bfmtv.com/international/ukraine-les-pays-du-g7-previennent-que-les-auteurs-dehttps://www.bfmtv.com/international/ukraine-les-pays-du-g7-previennent-que-les-auteurs-de-crimes-de-guerre-devront-rendre-des-comptes_AD-202203170612.htmlcrimes-de-guerre-devront-rendre-des-comptes_AD-202203170612.html

Ukraine Observed Nearly 14M Cyber Incidents in Q1 2022. Bank information security news, training, education - BankInfoSecurity [en ligne]. [sans date] [consulté le 4 juin 2022]. Disponible sur : https://www.bankinfosecurity.com/ukraine-observed-nearly-14m-cyberhttps://www.bankinfosecurity.com/ukraine-observed-nearly-14m-cyber-incidents-in-q1-2022-a-19175incidents-in-q1-2022-a-19175

Ukraine : une enquête des droits de l'homme de l'ONU met en lumière la détresse des civils. ONU Info [en ligne]. [sans date] [consulté le 4 juin 2022]. Disponible sur : https://news.un.org/fr/story/2022/05/1119742

Wagner en Syrie : Une cour russe pérennise l'impunité pour les responsables d'un meurtre violent. Fédération internationale pour les droits humains [en ligne]. [sans date] [consulté le 4 juin 2022]. Disponible sur : https://www.fidh.org/fr/regions/europe-asie-centrale/russie/wagner-en-syrie-la-decision-d-une-cour-russe-perennise-l-impunite

WISE, Jeff. The DIY Intelligence Analysts Feasting on Ukraine. Intelligencer [en ligne]. 4 mars 2022 [consulté le 4 juin 2022]. Disponible sur : https://nymag.com/intelligencer/2022/03/theosint-analysts-feasting-on-ukraine.html?regwall-newsletter-signup=true

PARTIE 3 - PERSPECTIVES: ÉVOLUTIONS & ANTICIPATION DES NOUVELLES MENACE

I. Les menaces cyber: une menace exponentielle & omniprésente dans le futur

ABOMHARA, Mohamed et Geir M. KØIEN. Cyber Security and the Internet of Things : Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility* [en ligne]. 2015, 4(1), 65–88. ISSN 2245-1439 [consulté le 1 juin 2022]. Disponible sur : doi:10.13052/jcsm2245-1439.414

ALJUHAMI, Amira M. et Doaa M. BAMASOUD. Cyber threat intelligence in risk management. *International Journal of Advanced Computer Science and Applications* [en ligne]. 2021, **12**(10). ISSN 2156-5570 [consulté le 1 juin 2022]. Disponible sur : doi:10.14569/ijacsa.2021.0121018

BEGGS, Christopher. Proposed risk minimization measures for cyber-terrorism and SCADA networks in Australia. *Proceedings of the 5th european conference on information warfare and security*. 2006, 9–18.

BAZOGE, Mickaël. Le gouvernement britannique prépare une action choc contre le chiffrement de bout en bout. *iGeneration* [en ligne]. 17 janvier 2022 [consulté le 4 juin 2022]. Disponible sur : https://www.igen.fr/ailleurs/2022/01/le-gouvernement-britannique-preparehttps://www.igen.fr/ailleurs/2022/01/le-gouvernement-britannique-prepare-une-action-choc-contre-le-chiffrement-de-bout-en-bout-127681une-action-choc-contre-le-chiffrement-de-bout-en-bout-127681

BORT, Bryson. There IS No Cyber Defense. *The Cyber Defense Review*. 2018, **3**(1), 41–46. CAMPUS CYBER. *Horizon Cyber 2030*. Paris : Campus Cyber, 2022. Disponible sur : https://campuscyber.fr/wp-content/uploads/2022/02/LIVRET-INTERACTIF.pdf

COROT, Léna. La guerre en Ukraine peut-elle précipiter la fragmentation de l'Internet ? *usinedigitale.fr* [en ligne]. 1 mars 2022 [consulté le 1 juin 2022]. Disponible sur : https://www.usinehttps://www.usine-digitale.fr/article/la-guerre-en-ukraine-peut-elle-precipiter-la-fragmentation-de-l-internet.N1789762digitale.fr/article/la-guerre-en-ukraine-peut-elle-precipiter-la-fragmentation-de-lhttps://www.usine-digitale.fr/article/la-guerre-en-ukraine-peut-elle-precipiter-la-fragmentation-de-l-internet.N1789762internet.N1789762

DOWNES, Cathy. Strategic Blind–Spots on Cyber Threats, Vectors and Campaigns. *The Cyber Defense Review*. 2018, **3**(1), 79–104.

ERTAN, Amy et al. Cyber Threats and NATO 2030: Horizon Scanning and Analysis. *CCDCOE*. 2020, **1**(1).

FIREEYE. L'importance du contexte : une Threat Intelligence complète pour unesécurité efficace. *FireEye* [en ligne]. [sans date] [consulté le 1 juin 2022]. Disponible sur : https://www.fireeye.com/blog/fr-executive-perspective/2020/07/using-cyber-threathttps://www.fireeye.com/blog/fr-executive-perspective/2020/07/using-cyber-threat-intelligence-to-increase-security-effectiveness.html - :~:text=vue%20des%20dirigeants-,L'importance%20du%20contexte%20:%20une%20Threat%20Intelligence,compl%C3%A8te%20pour%20une%20s%C3%A9curit%C3%A9%20efficace&text=Pour%20r%C3%A9%C3%A9quilibrer%20le%20rapport%20de,de%20leur%20programme%20de%20s%C3%A9curit%C3%A9.intelligence-to-increase-security-effectiveness.html#:~:text=vue%20des%20dirigeants-,L'importance%20du%20contexte%20:%20une%20Threat%20Intelligence,complète%20pour%20une%20sécurité%20efficace&text=Pour%20rééquilibrer%20le%20rapport%20de,de%20leur%20programme%20de%20sécurité.

FIREEYE. Rapports de veille des menaces | FireEye. *FireEye* [en ligne]. 2022 [consulté le 1 juin 2022]. Disponible sur : https://www.fireeye.fr/current-threats/threat-intelligencehttps://www.fireeye.fr/current-threats/threat-intelligence-reports.htmlreports.html

JABBOUR, Kamal et Erich DEVENDORF. Cyber Threat Characterizatoin. *The Cyber Defense Review*. 2022, **2**(3), 79-94.

KILPSTEIN, Michael. Seeing is Believing: Quantifying and Visualizing Offensive Cyber Operations Risk. *The Cyber Defense Review*. 2019, **4**(1), 85–106.

KOENIG, Gaspard. Gaspard Koenig : « Chaque citoyen doit pouvoir vendre ses données personnelles ». Les Echos [en ligne]. 7 janvier 2018 [consulté le 13 avril 2022]. Disponible sur : https://www.lesechos.fr/2018/01/gaspard-koenig-chaque-citoyen-doit-pouvoir-vendre-seshttps://www.lesechos.fr/2018/01/gaspard-koenig-chaque-citoyen-doit-pouvoir-vendre-ses-donnees-personnelles-981229donnees-personnelles-981229

LAUSSON, Julien. Un assureur américain baisse ses prix si le client accepte d'utiliser un bracelet de santé. *Numerama* [en ligne]. 20 septembre 2018 [consulté le 4 juin 2022]. Disponible sur : https://www.numerama.com/business/419453-un-assureur-americain-baissehttps://www.numerama.com/business/419453-un-assureur-americain-baisse-ses-prix-si-un-bracelet-de-sante-connecte-est-utilise.htmlses-prix-si-un-bracelet-de-sante-connecte-est-utilise.html

LAUSSON, Julien. La Russie tente d'asseoir sa domination dans l'Ukraine occupée en détournant Internet. *Numerama* [en ligne]. 31 mai 2022 [consulté le 1 juin 2022]. Disponible sur : https://www.numerama.com/tech/982185-la-russie-tente-dasseoir-sa-domination-danshttps://www.numerama.com/tech/982185-la-russie-tente-dasseoir-sa-domination-dans-lukraine-occupee-en-detournant-internet.htmllukraine-occupee-en-detournant-internet.html

LEHTO, Martti. The cyberspace threats and cyber security objectives in the cyber security strategies. *International Journal of Cyber Warfare and Terrorism* [en ligne]. 2013, 3(3), 1–18. ISSN 1947-3443 [consulté le 1 juin 2022]. Disponible sur : doi:10.4018/ijcwt.2013070101

LILLIAN Ablon, Martin LIBICKI et Andrea GOLAY. Projections and predictions for the black market. *Markets for Cybercrime Tools and Stolen Data Book Subtitle : Hackers' Bazaar*.
2016, **10**(3), 40–44.
MASON, Stephen. The Presumption That Computers Are 'Reliable'. *Electronic Evidence*.
2017, 101–192.

MURALI, Vijayaraghavan et al. Neural Sketch Learning For Conditional Program Generation. *Conference Paper ICLR 2018*. 2018, 1–17.

NATO. CCDCOE. *CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.* [en ligne]. [sans date] [consulté le 1 juin 2022]. Disponible sur : https://ccdcoe.org/library/publications/cyber-threatshttps://ccdcoe.org/library/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis/and-nato-2030-horizon-scanning-and-analysis/

REY, Marion. Le renseignement sur les cybermenaces ou Cyber Threat Intelligence, activité indispensable aux décideurs, dans une logique d'anticipation défensive et proactive. *Cyberday.info - Journée de conférences et d'échanges. Cyber-sécurité - Cyber-crises* [en ligne]. 14 février 2021 [consulté le 1 juin 2022]. Disponible sur : https://www.cyber-day.info/Lehttps://www.cyber-day.info/Le-renseignement-sur-les-cybermenaces-ou-Cyber-Threat-Intelligence-activite-indispensable-aux-decideurs-dans-une_a339.htmlrenseignement-sur-les-cybermenaces-ou-Cyber-Threat-Intelligence-activite-indispensablehttps://www.cyber-day.info/Le-renseignement-sur-les-cybermenaces-ou-Cyber-Threat-Intelligence-activite-indispensable-aux-decideurs-dans-une_a339.htmlaux-decideurs-dans-une_a339.html

SCHLETTE, Daniel et al. Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security* [en ligne]. 2020. ISSN 1615-5270
[consulté le 1 juin 2022]. Disponible sur : doi:10.1007/s10207-020-00490-y

SEGAL, Edward. 1 Year Later : Actions Taken, Lessons Learned Since The Colonial Pipeline Cyberattack. *Forbes* [en ligne]. 7 mai 2022 [consulté le 20 mai 2022]. Disponible sur : https://www.forbes.com/sites/edwardsegal/2022/05/07/1-year-later-actions-takenhttps://www.forbes.com/sites/edwardsegal/2022/05/07/1-year-later-actions-taken-lessons-learned-since-the-colonial-pipeline-cyberattack/lessons-learned-since-the-colonial-pipeline-cyberattack/

TOR. The Tor Project | Privacy & ; Freedom Online. *Tor Project | Anonymity Online* [en ligne].
2022 [consulté le 4 mai 2022]. Disponible sur : https://www.torproject.org/about/sponsors/
VITARD, Alice. Visés par une cyberattaque, des sites portuaires européens sont au ralenti. *usine-digitale.fr* [en ligne]. 7 février 2022 [consulté le 3 juin 2022]. Disponible sur : https://www.usine-digitale.fr/article/vises-par-une-cyberattaque-des-sites-portuaireshttps://www.usine-digitale.fr/article/vises-par-une-cyberattaque-des-sites-portuaires-europeens-sont-au-ralenti.N1781402europeens-sont-au-ralenti.N1781402
WEIMANN, Gabriel. Terrorist Migration to the Dark Web. *Perspectives on Terrorism*.
2016, **10**(3), 40–44.

II. Anticipations et moyens de défense contre les nouvelles menaces cyber

Campus Cyber – Construisons ensemble une société numérique de confiance. *Campus Cyber – Construisons ensemble une société numérique de confiance* [en ligne]. [sans date] [consulté le 28 mai 2022]. Disponible sur : https://campuscyber.fr/

CHAUVIN, Sandrine. Facteur humain et cybersécurité : les leçons du Pentagone. 14 janvier 2016 [consulté le 28 mai 2022]. Disponible sur : https://www.hbrfrance.fr/magazine/2016/01/9365-facteur-humain-ethttps://www.hbrfrance.fr/magazine/2016/01/9365-facteur-humain-et-cybersecurite-les-lecons-du-pentagone/cybersecurite-les-lecons-du-pentagone/

Cost of a Data Breach Report 2021. *IBM - Deutschland | IBM* [en ligne]. [sans date] [consulté le 28 mai 2022]. Disponible sur : https://www.ibm.com/security/data-breach

Cybercriminalité. *INTERPOL | The International Criminal Police Organization* [en ligne].
[sans date] [consulté le 28 mai 2022].
Disponible sur : https://www.interpol.int/fr/Infractions/Cybercriminalite

Cybercriminalité : un défi à relever aux niveaux national et européen. *Accueil - Sénat* [en ligne].
[sans date] [consulté le 28 mai 2022]. Disponible sur : http://www.senat.fr/rap/r19-613/r19http://www.senat.fr/rap/r19-613/r19-613_mono.html613_mono.html

Cybercriminalité : un défi à relever aux niveaux national et européen. *Accueil - Sénat* [en ligne].
[sans date] [consulté le 28 mai 2022]. Disponible sur : http://www.senat.fr/rap/r19-613/r19http://www.senat.fr/rap/r19-613/r19-613_mono.html - toc256613_mono.html#toc256

Dispositif d'assistance aux victimes d'actes de cybermalveillance.
CYBERMALVEILLANCE.GOUV.FR [en ligne]. [sans date] [consulté le 28 mai 2022].
Disponible sur : https://www.cybermalveillance.gouv.fr/

ENISA. Aperçu du renseignement sur la cybermenace. [en ligne]. [sans date] [consulté le 28 mai 2022]. Disponible sur : https://www.enisa.europa.eu/publications/report-files/ETL-translations/fr/etl2020-ctihttps://www.enisa.europa.eu/publications/report-files/ETL-translations/fr/etl2020-cti-overview-ebook-en-fr.pdfoverview-ebook-en-fr.pdf

EUR-Lex — Access to European Union law — choose your language [en ligne]. [sans date] [consulté le 28 mai 2022]. Disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52020DC0797&from=ES

INFORISQUE | Risques professionnels et prévention SST [en ligne]. [sans date] [consulté le 28 mai 2022]. Disponible sur : https://www.inforisque.info/actualite-du-risque/documents/7632-ebook-olfeo-facteur-humainhttps://www.inforisque.info/actualite-du-risque/documents/7632-ebook-olfeo-facteur-humain-prochain-maillon-fort-cybersecuriteprochain-maillon-fort-cybersecurite

JANISZEWSKI, Marek. A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Intelligence. 2019.

L'avenir de la cybersécurité : 3 scénarios à envisager. *PwC* [en ligne]. [sans date] [consulté le 28 mai 2022]. Disponible sur : https://www.pwc.fr/fr/decryptages/securite/avenir-de-lahttps://www.pwc.fr/fr/decryptages/securite/avenir-de-la-cybersecurite-3-scenarios-a-envisager.htmlcybersecurite-3-scenarios-a-envisager.html

Le renseignement sur les cybermenaces ou Cyber Threat Intelligence, activité indispensable aux décideurs, dans une logique d'anticipation défensive et proactive. *Cyber-day.info* -

Journée de conférences et d'échanges. Cyber-sécurité - Cyber-crises [en ligne]. [sans date] [consulté le 28 mai 2022]. Disponible sur : https://www.cyber-day.info/Le-renseignement-surhttps://www.cyber-day.info/Le-renseignement-sur-les-cybermenaces-ou-Cyber-Threat-Intelligence-activite-indispensable-aux-decideurs-dans-une_a339.htmlles-cybermenaces-ou-Cyber-Threat-Intelligence-activite-indispensable-aux-decideurs-danshttps://www.cyber-day.info/Le-renseignement-sur-les-cybermenaces-ou-Cyber-Threat-Intelligence-activite-indispensable-aux-decideurs-dans-une_a339.htmlune_a339.html

Le tournant cognitif de la cybersécurité : changement de paradigme et prolégomènes à la cybersécurité cognitive. *European Scientist* [en ligne]. [sans date] [consulté le 4 juin 2022].
Disponible sur : https://www.europeanscientist.com/fr/opinion/le-tournant-cognitif-de-lahttps://www.europeanscientist.com/fr/opinion/le-tournant-cognitif-de-la-cybersecurite-changement-de-paradigme-et-prolegomenes-a-la-cybersecurite-cognitive/cybersecurite-changement-de-paradigme-et-prolegomenes-a-la-cybersecurite-cognitive/

Notre stratégie. *ANSSI* [en ligne]. [sans date] [consulté le 28 mai 2022]. Disponible sur : https://www.ssi.gouv.fr/agence/missions/notre-strategie/#anssi-10

Orange Cyberdefense : Failles de cybersécurité : la nécessité de reconnaître le facteur humain.
Orange Cyberdefense : Region and language selection page [en ligne]. [sans date] [consulté le 28 mai 2022].
Disponible sur : https://www.orangecyberdefense.com/fr/insights/blog/cyberdefense/failleshttps://www.orangecyberdefense.com/fr/insights/blog/cyberdefense/failles-de-cybersecurite-la-necessite-de-reconnaitre-le-facteur-humainde-cybersecurite-la-necessite-de-reconnaitre-le-facteur-humain

PEREIRA, Brigitte. La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité. *Revue internationale de droit économique* [en ligne]. 2016, **XXX**(3), 387. ISSN
1782-1525 [consulté le 28 mai 2022]. Disponible sur : doi:10.3917/ride.303.0387

Threat Intelligence - Renseignement & ; Cybersécurité | Devoteam France. *Devoteam France* [en ligne]. [sans date] [consulté le 28 mai 2022].
Disponible sur : https://france.devoteam.com/livre-blanc/livre-blanc-la-threat-intelligence-ahttps://france.devoteam.com/livre-blanc/livre-blanc-la-threat-intelligence-a-la-croisee-du-renseignement-et-de-la-cybersecurite/la-croisee-du-renseignement-et-de-la-cybersecurite/