PREFACE

Qui tente de prévoir l'avenir, prend le risque de se tromper. Mais celui qui néglige l'analyse prospective adopte une attitude passive qui le place en situation de faiblesse face à la dictature des événements. Anticiper les évolutions de la société c'est afficher la volonté de ne pas subir.

Les pionniers d'Internet, parmi lesquels Paul Baran, récemment décédé, n'imaginaient pas sans doute que le réseau internet relierait un demi-siècle plus tard plus de deux milliards d'abonnés.

Qui l'aurait prédit ? L'essor des technologies numériques modifie fondamentalement notre société. Qui aurait imaginé leur impact sur les modes de télécommunication, les relations sociales, l'économie, les processus industriels, la domotique, la vie politique, etc. ?

Certains assimilent la révolution numérique à l'invention de l'imprimerie par Gutenberg. La rupture est sans doute d'une plus grande ampleur, car elle concerne l'ensemble des activités humaines. Chaque jour nous sommes les témoins d'une véritable reconfiguration touchant les individus, les entreprises, les institutions.

Le cyberespace est un espace de liberté, de créativité, de croissance qui offre des perspectives ***"exponentielles"***. C'est une chance pour l'humanité. Mais tout progrès a son revers. Les effets pervers se manifestent aussi car les prédateurs en exploitent immédiatement les failles, pour tirer des profits, détruire ou neutraliser tout ce qui gène le développement de leur entreprise criminelle.

Le cyberespace offre aujourd'hui des opportunités mais il est aussi un espace de puissance, de conflits. La guerre y est déclarée.

L'avenir peut être imaginé sur la base de certitudes. Le cyberespace va mettre en relation de plus en plus d'êtres humains, dans les pays développés mais surtout dans les pays émergents ; la Chine plus particulièrement. Cette expansion s'observe aussi dans les pays du tiers monde, qui peuvent désormais accéder aux nouvelles technologies en faisant un saut qualitatif qui gomme des écarts encore cuisants.

Les nouvelles technologies vont aussi irriguer la vie quotidienne jusque dans les moindres détails, c'est une autre certitude. La notion de puissance devra être examinée sous un nouveau jour, l'expression de la démocratie s'affranchira du calendrier des consultations électorales. Les institutions publiques ou privées devront s'adapter à ce nouveau comportement des citoyens, des consommateurs. Les modes d'organisation glisseront vers un système matriciel plus complexe.

Il appartient aux responsables d'identifier les continuités mais aussi de déceler les ruptures potentielles liées à une évolution des technologies. D'où l'importance de la veille scientifique.

L'avenir repose aussi sur des incertitudes. L'Etat, dont la légitimité repose d'abord sur la défense et la sécurité, pourra t-il conserver ce monopole face à des menaces ou à des attaques multiples et diffuses, non signées, quotidiennes ?

La coopération internationale sera-t-elle en mesure de maîtriser la contradiction entre une mondialisation inhérente à la constitution des réseaux et le maintien de frontières politiques, juridiques et militaires ?

La crise économique durable autorisera-t-elle le financement des indispensables mesures de défense et de sécurité qui ne se substituent pas mais s'ajoutent à celles encore nécessaires pour garantir la paix dans les espaces terrestres aériens et maritimes ? Les états ***"noirs"***, les mafias, les organisations criminelles, les mouvements terroristes ne vont-ils pas bénéficier

d'une liberté d'action et de moyens qui feront défaut à ceux qui veulent contrer le développement de leur empire?

Pour éviter le chaos, une prise de conscience est nécessaire. Les pouvoirs publics s'engagent aujourd'hui avec résolution. La création récente de l'agence nationale de la sécurité des systèmes d'information *(ANSSI)* est la partie visible et hautement symbolique d'une politique volontariste qui ne peut, discrétion oblige, afficher toutes ses composantes.

Les entreprises aussi se mobilisent progressivement, car elles savent que leur potentiel humain, matériel et immatériel peut être affecté ou anéanti faute de vigilance.

Mais la prise de conscience doit être aussi partagée par l'ensemble des citoyens. D'où la nécessité d'une formation à l'école ou à l'université qui soit au plus vite intégrée dans les programmes, car il faut semer aujourd'hui pour récolter demain.

Au delà, la question essentielle qui se pose au prévisionniste est celle de la place de l'homme dans le cyberespace. Ce qui est en jeu, c'est pour chacun la préservation de son identité, de son droit à l'image, de sa sphère d'intimité, de sa liberté d'opinion, de son accès à une information objective. L'homme doit rester maître du cyberespace et ne pas en devenir l'esclave, notamment par le caractère intrusif et la traçabilité des technologies numériques.

L'analyse prospective sur l'évolution de la cybercriminalité que nous livrent vingt-deux experts est le fruit de la convergence d'expériences différentes.

Elle a le grand mérite de mettre en évidence la dimension humaine des enjeux de la *"criminalité du XXIème siècle"*.

Ce travail fondateur apporte des réponses concrètes aux interrogations d'aujourd'hui sans lesquelles demain pourrait ne pas avoir d'avenir.

Général d'armée Marc WATIN-AUGOUARD
Inspecteur général des armées - Gendarmerie

AVANT-PROPOS

La cybercriminalité évolue à un rythme effréné suivant la même dynamique que la pénétration inéluctable des technologies de l'information et de la communication dans l'ensemble des activités humaines. Tandis que la société s'invente et évolue, parallèlement, les criminels déploient une remarquable capacité d'adaptation pour en tirer le plus grand profit. Afin de ne pas leur laisser l'initiative, il importe que les acteurs de la lutte contre la cybercriminalité tentent d'anticiper l'évolution des éléments sous-jacents au phénomène, tant sur le plan qualitatif que quantitatif, pour y adapter leurs moyens.

A l'issue de l'édition 2010 du forum international sur la cybercriminalité (FIC 2010), les organisateurs ont souscrit au projet présenté par Daniel GUINIER de réitérer un travail de prospective sur le phénomène cybercriminel mené par Philippe ROSÉ en 1991[1]. Le résultat de cette réflexion collective pour la prochaine décennie devait être présenté dans le cadre des travaux de l'édition 2011 du FIC, annulée depuis.

Cette étude prospective sur la prochaine décennie a réuni un panel d'experts issus des secteurs public et privé. La démarche retenue pour sa conduite se fonde sur un processus itératif de consultations par la méthode Delphi, sur la base d'un questionnaire établi par un comité scientifique, avec des synthèses intermédiaires rédigées par un comité *ad hoc*. La procédure de consultation dématérialisée a été efficace tout en permettant de conserver l'anonymat sur les réponses des participants, et donc leur indépendance en évitant l'effet de leadership. Les 22 experts ayant contribué à ces travaux ont bénéficié de trois tours de consultation individuelle pour s'exprimer et reformuler leurs réponses en les confrontant aux résultats des réflexions collectives. Sans exclure la possibilité d'une rupture technologique majeure, la combinaison de leurs analyses, étayées par leurs expériences professionnelles respectives, a permis de dégager les convergences d'opinions tout en préservant la richesse des apports des expertises individuelles, et d'indiquer les tendances d'un phénomène criminel typique du 21ème siècle. Le processus de maturation délicat aura pris une année[2] avant d'en présenter les résultats sous cette forme synthétique.

Le résultat de ce travail n'est pas une fin en soi mais un outil destiné à alimenter la réflexion des décideurs politiques, économiques et les représentants de la société civile sur les stratégies à mettre en œuvre pour être en mesure de mieux maîtriser un espace numérique sans frontière.

La publication de cette étude prospective[3] est ici la récompense pour les experts de leur contribution personnelle à l'élaboration d'une vision collective.

Le lecteur trouvera en annexe les détails de la méthode, la liste des participants à l'étude et le questionnaire qui leur a été soumis.

[1] Rosé P. (1992) : La criminalité informatique à l'horizon 2005 ; Guinier D. (1995) sur le développement d'une criminologie liée aux technologies de l'information.

[2] Depuis la présentation du projet aux organisateurs du FIC en avril 2010, jusqu'en mars 2011.

[3] **Avertissement relatif aux droits** : S'agissant d'une œuvre collective diffusée à l'initiative de la gendarmerie nationale, il est entendu que les lecteurs et acteurs de ce travail, -*membres des comités et experts consultés nommés*- sont autorisés à en faire bon usage, par des reprises partielles, sous condition de mentionner complètement la source : *"Analyse prospective sur l'évolution de la cybercriminalité de 2011 à 2020"*, © 2011 Gendarmerie nationale. En revanche, toute publication de ce travail est soumise à l'autorisation expresse de la gendarmerie nationale, bénéficiaire de l'ensemble des droits patrimoniaux, au même titre que le *"Guide pratique du chef d'entreprise face au risque numérique"*, dont la seconde version du 31 mars 2010 avait été présentée au FIC 2010 à Lille.

TABLE DES MATIERES

INTRODUCTION

Définition et orientations de la cybercriminalité

Il s'agit de présenter les résultats concernant la définition du terme "cybercriminalité" dans les différentes orientations perçues par les experts, au cours de la décennie 2011-2020[4].

Etymologiquement, la *"cybercriminalité"* associe le terme *"criminalité"* à la racine *"cyber"* du mot *"cybernétique"*, issu du Grec *"kubernân"* qui signifie piloter ou gouverner. L'environnement *"cyber"* inclut toutes formes d'activités numériques, conduites ou non au travers de réseaux et sans frontières. Ceci étend la précédente dénomination de *"criminalité informatique"*, pour englober les délits perpétrés en rapport avec l'Internet, l'ensemble des technologies numériques et les réseaux de télécommunications. Cette terminologie, plus récente, recouvre une large diversité de faits qui conduisent à des divergences d'approche selon la culture dominante des experts, pour la faire paraître tantôt réductrice, tantôt plus étendue, sous différentes orientations, face à des questions émergeantes qui relèvent aussi de sa diversification.

Orientation pénaliste de la cybercriminalité

Dans une orientation pénaliste, certains experts indiquent qu'il n'est pas besoin de changer ou de redéfinir ce terme mais seulement de préciser ce qu'il englobe, en reprenant **la convention sur la cybercriminalité** du Conseil de l'Europe[5]. Ils soulignent la coexistence d'infractions de droit commun du monde réel, avec d'autres, plus attachées au monde virtuel, ou encore spécifiques, *-telle l'usurpation d'identité en ligne-*. Les proportions des différents types d'infractions commis ou perçus en fonction des sensibilités du public concerné sont susceptibles d'évoluer. Les dix prochaines années verront certainement le développement de **la dimension financière**, *-avec le blanchiment, alors qu'Internet facilite le contournement du système bancaire classique-*, celui de **l'implication de groupes criminels organisés**, souvent internationaux, et l'importance de la sécurité des données personnelles.

D'autres préfèrent cependant ***"criminalité liée aux technologies numériques"*** qui regroupe les infractions et les actions judiciaires qui font intervenir des technologies numériques. D'autres encore indiquent que **le terme *"cybercriminalité"* est plutôt réducteur**, au vu de la répartition des atteintes, largement liées à des causes indépendantes de l'informatique, et de divers modes opératoires en cours d'évolution, dépassant largement l'Art. 323 du Code pénal, tandis que sont maintenant visés les contenus, les services et les infrastructures.

Orientation technologique de la cybercriminalité

Dans une orientation technologique, d'autres experts indiquent **la nécessité d'une prise en compte plus globale sous la dénomination *"criminalité électronique"*** ou ***"e-criminalité"***, du fait de la convergence des TIC[6] : *éléments mobiles et téléphonie, mémoires, systèmes de surveillance, etc.*, mais aussi des nanotechnologies et de la robotique qui sont à prendre en compte dès maintenant. Ces moyens électroniques représenteront des cibles de plus en plus convoitées mais également des supports pour masquer, commettre ou accompagner

[4] Selon la question posée Q01 : Comment pourrait-on redéfinir ou préciser les domaines d'activités illicites et redéfinir le terme *"cybercriminalité"* pour la prochaine décennie ?
[5] Dite : *"Convention de Budapest du 21 novembre 2001"*.
[6] Technologies de l'information et de la communication.

des crimes et délits. Seuls les actes positifs pour lesquels un ou plusieurs moyens ont été utilisés pour commettre un des éléments constitutifs de l'infraction peuvent être retenus[7].

Orientation anthropologique de la cybercriminalité

Dans une orientation anthropologique, la cyber-délinquance, issue de diverses populations, comporte des facteurs socio-éducatifs, socio-économiques, techno-idéologiques et leurs expressions, y compris pathologiques comme l'addiction. En effet, l'inadaptation du système éducatif peut participer au développement de nouvelles formes de cybercriminalité ou à des pratiques et des comportements déviants plus ou moins graves : *tricherie, atteintes à la réputation, etc.*, pouvant être liés à des frustrations et à la redéfinition des valeurs matérielles et citoyennes, et en tout cas non conformes à ce qui est attendu pour aborder ou mener une vie d'adulte. Les conditions socio-économiques difficiles concernent aussi l'Internet comme lieu d'expression de troubles psychologiques d'origine socio-économique : *vol, usurpation, pédopornographie, appels à la déstabilisation, à la violence et à la haine, etc.* Concernant les facteurs techno-idéologiques, il y a lieu de considérer les sites et réseaux de propagande, de déstabilisation et de manipulations psychologiques individuelles ou de masse, avec le recours à des méthodes de traitements numériques d'images, de vidéos, et audio.

Orientation stratégique de la cybercriminalité

Dans une orientation stratégique, la cybercriminalité est perçue en tant qu'atteinte à la cyber-sécurité, à savoir l'attaque des réseaux numériques visant à une prise de contrôle, une paralysie, voire une destruction des infrastructures vitales des États et des secteurs d'activité identifiés d'importance vitale.

Amplification et diversification de la cybercriminalité

Les experts s'accordent sur le fait que **les activités illicites ou criminelles sont et seront démultipliées**, les conditions de passage à l'acte et les processus de réalisation sont déjà et seront modifiés par l'usage des TIC dans divers domaines, usuels ou innovants : *transactions financières, vie privée, usurpation d'identité, atteintes à la réputation, atteintes aux systèmes critiques, terrorisme, etc.* **Les questions émergeantes** relèvent de la classification des infractions au regard des technologies nouvelles et à venir, mais aussi de la compréhension des motivations des auteurs et des commanditaires. Elles auront à prendre en compte les relais constitués par des **réseaux sociaux peu structurés mais instrumentés**, la présence d'**organisations très structurées**, plus ou moins discrètes, agissant au niveau international, et l'ampleur des conséquences, au vu du terrorisme, de la guerre de l'information et de la cyber-guerre qui toucherait les infrastructures et systèmes socio-économiques stratégiques, avec des risques de pannes de grande ampleur, entraînant l'indisponibilité de réseaux et de systèmes entiers.

Références :

CE (2001) : Convention sur la cybercriminalité (STE n° 181), Budapest, 23/11/01, Conseil de l'Europe.
Clusif (2010) : Menaces informatiques et pratiques de sécurité en France. Édition 2010.

[7] La seule utilisation de moyens de communication ou autre ne suffit pas à qualifier un fait délictueux. Par exemple, un message de hameçonnage *("phishing")* permettra de qualifier l'infraction de fait de cybercriminalité, car le message, en lui-même, contient la preuve de l'usage d'un faux nom ou d'une fausse qualité, nécessaire à la qualification d'escroquerie. En revanche, un rendez-vous fixé à partir d'un téléphone, fixe ou cellulaire, pour procéder à une vente illicite ne contient pas la preuve de commission d'infraction directe, mais seulement celle d'un rendez-vous au cours de laquelle une infraction pourrait être commise.

FIC2010 (2010) : Guide pratique du chef d'entreprise face au risque numérique version 2010 : risques identifiés et solutions proposées en 13 fiches, recommandations, 90 pages.
Filiol E., Richard P. (2006) Cybercriminalité. Enquête sur les mafias qui envahissent le Web, Dunod, 212 pages.
Guinier D. (1995) : Développement d'une criminalité spécifique liée aux technologies de l'information - *en rapport avec l'informatique, les réseaux et les autoroutes électroniques.* Proc. 7ème Symposium CITSS, Ottawa, pp. 21-45.
Krone, T., 2005. High Tech Crime Brief. Australian Institute of Criminology. Canberra, Australie. ISSN 1832-3413. 2005.
Quéméner M. (2008) : Cybermenaces, entreprises et internautes. Economica, 264 pages.
Quéméner M., Yves Charpenel (2010) : Cybercriminalité, droit pénal appliqué, Economica, 273 pages.
PWC, Coopers (2009) : IT Governance Global Status Report.
Rosé P. (1992) : La criminalité informatique à l'horizon 2005 - Analyse prospective, par l'IHESI et les éditions l'Harmattan, 165 pages.
Tisserand I. (2000) : Nouvelles populations, nouvelles addictions : l'exemple des hackers, Annales de médecine interne, Masson, vol. 151, pp. B49-B52
Tisserand I. (2002) : Hacking à cœur : les enfants du numérique, e-dite, Paris, 136 pages

http://blog.crimenumerique.fr/2008/10/30/faire-face-nouveaux-defis-delinquance-numerique
http://europa.eu/scadplus/leg/fr/lvb/114560.htm
http://ftp.jrc.es/EURdoc/JRC58484.pdf
http://lesrapports.ladocumentationfrancaise.fr/BRP/044000076/0000.pdf
http://re.jrc.ec.europa.eu/refsys/pdf/Snapshots_EUR_2010i.pdf
www.aucc.ca/publications/media/2010/banting_postdocs_07_06_f.html
www.ccl-cca.ca/CCL/Reports/LessonsInLearning/LinL20100707AcademicDishonesty-2.html
www.cio-online.com/contributions/lire-le-traitement-des-risques-humains-en-milieux-professionnels-strategiques-logique-ou-modernite-en-ssi-101.html
www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079if09pres_aseger_247cp.pdf
www.eea.europa.eu/publications/the-territorial-dimension-of-environmental-sustainability/at_download/file
www.enisa.europa.eu/about-enisa/activities/programmes-reports/general-report-2009
www.fedpol.admin.ch/content/dam/data/kriminalitaet/diverse_berichte/cybercrime_sab_200110f.pdf
www.huyghe.fr/dyndoc_actu/495a33359efe6.pdf
www.interieur.gouv.fr/sections/a_votre_service/votre_securite/internet/cybercriminalite
www.nap.edu/openbook.php?record_id=1581&page=283
www.operationspaix.net/sites/politiquessociales.net/IMG/pdf/CP_suivi_tableau_de_bord_pauvrete.pdf
www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved Report_16Oct2009.pdf
www.voltage.com/pdf/Voltage-Data-Breach-Incident-Analysis.pdf

Place de la cybercriminalité

Il s'agit de présenter les résultats concernant la place de la cybercriminalité et ses rapports avec d'autres formes de criminalité, au cours de la décennie 2011-2020[8].

Extension et croissance de la cybercriminalité

Si les technologies modernes ont radicalement modifié les modes de vie, les formes classiques de crimes et délits s'appuieront sur elles **en franchissant les frontières criminelles**. En effet, les réseaux numériques facilitent le passage à l'acte avec de nombreux avantages : *la discrétion, l'impression d'anonymat, la démultiplication des infractions, le caractère international, et la fugacité des preuves.*

[8] Selon la question posée Q02 : Quelle sera la place de la cybercriminalité et ses rapports avec les autres formes de crimes et délits : *contrefaçons, délinquance financière et économique, pédopornographie, trafics de stupéfiants et d'êtres humains, terrorisme, etc.* ?

La place de la cybercriminalité sera croissante du fait du développement exponentiel des connexions, de l'augmentation des connaissances en la matière, de la culture et de la présence de technologies et de l'électronique programmable embarquées, ce qui augmente le nombre de cibles potentielles. Par rapport aux autres formes de crimes et de délits, elle nécessite généralement moins d'investissements et peut être réalisée en divers lieux, sans contrainte géographique, en se jouant des frontières.

Prépondérance et liens de la cybercriminalité

Chacun s'accorde à penser que **la cybercriminalité occupera une place prépondérante et couvrira le spectre de la criminalité classique**. L'argumentation se fonde sur les points communs ou les liens entre la cybercriminalité et les formes classiques de criminalité, et sur des exemples qui montrent l'impact des possibilités offertes par les TIC et l'Internet. Du fait de la proximité, de l'apparence d'impunité, et de la potentialité, l'Internet et les TIC favorisent divers crimes et délits, par exemple : *contrefaçons, délinquance économique, blanchiment, pédopornographie, proxénétisme, trafic de stupéfiants et d'êtres humains, terrorisme, escroqueries, etc.* Ces formes, et notamment le crime organisé financier et économique et le blanchiment, seront sans doute de plus en plus intégrés à la *"cybercriminalité"*.

Le terrorisme pourrait aussi s'appuyer sur la fragilité de certains systèmes et infrastructures : *aéroports, contrôles aériens, transports, transactions financières, centrales et distribution d'énergie, centres de données et de surveillance, etc.,* en développant de nouvelles méthodes avec des impacts considérables. Il faut s'attendre à voir l'arrivée d'une génération d'individus imprégnés de technologie de l'information et de la communication désirant agir sur le monde tout en restant derrière leur écran. La possibilité d'opérer en partie ou totalement à distance en toute impunité sera une puissante incitation au passage à l'acte.

Des risques nouveaux apparaîtront, avec le développement de la bioinformatique et la pose d'implants bio-électroniques dans le corps humain, qui vont offrir un champ immense d'attaques possibles, notamment fondées sur la perturbation à distance[9]. Le développement de la domotique et celui des objets communicants favoriseront aussi les portes d'entrée pour les cybercriminels dans l'espace privatif.

Nuances apportées sur la cybercriminalité

Pour certains, **la cybercriminalité sera dominante**, du fait que la majeure partie des gains financiers criminels se réaliseront sur les réseaux, au travers de schémas de plus en plus complexes, de systèmes de blanchiment difficiles à démanteler, en profitant notamment de difficultés juridiques entre les États et du manque de moyens de lutte mis en œuvre. Des experts estiment même que la cybercriminalité est déjà prépondérante. Ainsi, aux Etats-Unis en 2009 pour la première fois, les transferts frauduleux de fonds immatériels ont dépassé les vols physiques dans les agences bancaires.

Pour d'autres, **la cybercriminalité restera en retrait** par rapport à la délinquance financière et économique sous toutes ses formes. Toutefois, l'impact économique de la cybercriminalité reste difficile à estimer et, encore plus, la comparaison avec la délinquance économique et le trafic de stupéfiants.

Références :

Guidère M. (2010) : Les nouveaux terroristes, Editions Autrement, 156 pages.

[9] Comme la modification des paramètres de gestion de *"pacemakers"* ou d'autres implants vitaux.

http://forms.cybersource.com/forms/FraudReport2010NAANETwww2010
http://krebsonsecurity.com/2010/03/page/3/
www.globalsecuritymag.fr/Vigil-nce-Pacemaker-multiples,20091109,13745.html
www.interieur.gouv.fr/sections/a_votre_service/statistiques/criminalite/2009
www.mcafee.com/us/local_content/white_papers/cybercrime_20100315_en.pdf

Impact global de la cybercriminalité

Il s'agit de présenter les résultats concernant l'impact global des évolutions et des ruptures technologiques sur la maîtrise ou, au contraire, sur la montée de la cybercriminalité, au cours de la décennie 2011-2020[10].

Perception de l'impact global de la cybercriminalité

L'impact global reste difficile à percevoir, alors qu'il existe une montée en puissance de la maîtrise des technologies de l'information et de l'exploitation des failles par les cybercriminels, un écart entre États de droit et pays corrompus, et un paradoxe lié aux évolutions et ruptures technologiques. Il est toujours utile de rappeler que la technologie est neutre. En revanche, l'usage qui en est fait sera qualifié de néfaste ou au contraire, de positif.

C'est en particulier le cas de la cryptographie qui permet de sécuriser les transactions et les échanges de données, mais aussi, d'assurer la confidentialité des communications couvrant des activités illégales et l'établissement de preuves. Les nouvelles technologies sont rarement maîtrisées et pas totalement abouties, et utilisées pour le bien et le mal, ce que montre l'histoire.

Les dix années à venir relèvent de la mobilité, avec des exigences de disponibilité, de communication en temps réel, de connectivité, et davantage de dépendance des équipements et de risque pour l'identité numérique. Cette décennie sera aussi celle des systèmes de supervision des automates et ouvrira de nouveaux risques.

Evolutions d'impact négatif au regard de la cybercriminalité

Les évolutions prévues, susceptibles d'avoir un impact négatif sur la cybercriminalité, sont l'effacement de la frontière entre les sphères professionnelle et privée, la difficulté de localiser les informations de l'entreprise et les applications Web avec le *"cloud computing"*, les codes malveillants furtifs ciblés, et plus généralement l'usage massif des nouvelles technologies, notamment mobiles et sans fil, et l'exposition sans précaution à l'ingénierie sociale, aux réseaux sociaux, aux téléchargements par des moyens mobiles moins sûrs, etc.

Le caractère volatile des données de preuve et les difficultés de remontée aux sources des infractions, sans moyens légaux offensifs, doivent être soulignés car les cybercriminels s'adaptent aussi aux nouvelles technologies.

D'une façon générale, l'anonymat sur l'Internet et l'étendue et la profondeur mondiale des réseaux favorisent l'impunité des délinquants, et le *"cloud computing"* rendront plus difficile la recherche et la saisie de preuves. Les groupes criminels ont aussi les moyens financiers de s'attacher des services de R&D pour développer des outils facilitant les attaques ou la commission des actes délictueux ou criminels, entraînant une forme de professionnalisation.

[10] Selon la question posée Q03 : Quel sera l'impact global des évolutions et ruptures technologiques : *informatique en nuages et virtualité, systèmes mobiles, cryptologie, stéganographie, codes malveillants, etc.*, sur la maîtrise ou au contraire la montée de ce phénomène ?

Evolutions d'impact positif au regard de la cybercriminalité

A l'opposé, **des mesures de sécurité fondées sur ces technologies pourraient avoir un impact positif**. La sécurité est au centre du problème et devra s'appuyer sur des politiques et la stricte application de mesures. Elle sera un défi majeur avec le *"cloud computing"*, du fait de la complexité des lieux de stockage des données et de leurs diverses juridictions, avec des risques majeurs liés à la gouvernance et à la territorialité. Le niveau de qualité effective de la sécurité sera un facteur-clé d'acceptation de ces nouveaux services.

Références :

Guinier D. (2010) : L'informatique dématérialisée en nuages - *Ontologie et sécurité du "cloud computing"*. *Expertises,* n° 351, octobre, pp. 335-344

www.gartner.com/it/page.jsp?id=1422314
www.klb-group.com/fr/upload/larticle_du_mois/liens/cost_killing__mai_2010.pdf

1. LES MENACES

1.1. Les menaces émergentes : cibles et formes attendues

Il s'agit de présenter les résultats de l'étude concernant les menaces émergentes et les nouvelles formes attendues, ainsi que leur niveau de sophistication, au cours de la décennie 2011-2020[11].

Concernant les cibles attendues

Les menaces émergentes porteront non seulement sur les transactions et les applications en ligne, -*avec maintenant les jeux et les paris d'argent*-, mais aussi sur les systèmes de commande industriels, robotiques, domotiques et embarqués, avec le développement de la connectivité à l'Internet et la dépendance de plus en plus forte à l'outil numérique. Les systèmes SCADA[12] de télésurveillance, de contrôle distant et de télégestion technique en temps réel, et les systèmes satellitaires pourraient être particulièrement ciblés. Les services à la demande du *"cloud computing"* favoriseront par ailleurs des programmes malveillants abusant les utilisateurs.

Il est probable que les nouvelles menaces visent des technologies pas forcément novatrices, mais en phase ou en attente de déploiement massif. Afin de diminuer l'impact financier, les délais d'installation sont diminués et donc le temps consacré à la sécurité réduit à sa plus simple expression. Dès lors des attaques auparavant envisageables mais non réalisées par manque d'intérêt financier, deviennent lucratives sinon significatives par leur effet de masse. Il est cité comme illustration les appels en nombre à des numéros surtaxés et la fraude aux centraux téléphoniques[13]. Cette exploitation n'est cependant sophistiquée que dans son montage, lequel nécessite la génération d'appels en nombre dans un ou plusieurs pays, et la création d'une structure adéquate dans un paradis fiscal pour disposer des sommes résultantes[14].

Il s'agira enfin d'attaques menées à l'encontre d'infrastructures critiques et de services stratégiques financiers, socio-économiques, etc., avec le recours à des relais vulnérables ou à des groupes actifs, pour désorganiser et paralyser des systèmes, visant le *black-out* des communications ou de la distribution d'énergie, en particulier en cas de conflits.

Concernant les formes attendues

Toute innovation technique apporte de nouvelles vulnérabilités, du fait que les produits comportent souvent des erreurs, de la conception à l'exploitation, **et la nouveauté entraîne**

[11] Selon la question posée Q11 : Quelles sont les menaces émergentes et les nouvelles formes attendues et leur niveau de sophistication ?
[12] Pour *Supervisory Control And Data Acquisition*. Il s'agit notamment de la télésurveillance et de la télégestion technique des bâtiments et des installations : *climatisation, chauffage, alarme, éclairage, accès, etc*.
[13] Par exemple, les centraux de type PABX : Cette technologie permet de créer autant de mini-standards que de postes configurés. Chacun dispose de la fonction de renvoi d'appels configurable à distance. Mais, par manque de temps, le mot de passe protégeant la configuration n'est que rarement changé. Des pirates font des essais sur des listes de numéros de téléphone et lorsqu'ils détectent une entreprise équipée, ils configurent un renvoi et génèrent des appels surtaxés en masse.
[14] Avec parfois l'intermédiaire de *"mules"* pour percevoir et retransmettre ces sommes, moyennant une promesse d'une rémunération.

souvent un détournement de finalité, qui devient à son tour une source de nouvelles potentialités de malveillance. L'évolution des réseaux sociaux, confortée par le goût croissant des utilisateurs pour la communication électronique, ne manquera donc pas de générer des menaces à l'encontre des personnes, mais aussi des entreprises, des organisations publiques et des États. Les possibilités de chantage et d'extorsion[15] envers les entreprises et les services des États pourraient utiliser notamment des réseaux de discréditation, *-notamment en combinant par exemple les potentialités de WikiLeaks et de Facebook-*. Se développeront indubitablement les escroqueries et les fraudes, avec usurpations et vols d'identité numérique et de coordonnées bancaires[16], l'utilisation frauduleuse de données personnelles, la violation de la vie privée, les attaques à base d'ingénierie sociale, etc. Le **risque bioinformatique**, avec la récupération de données personnelles d'ordre médical et surtout l'atteinte à leur intégrité dans un but criminel, est aussi à prendre en compte.

Concernant les causes et nuances associées

D'un côté, le niveau de complexité de la menace ne sera pas directement fonction du niveau de complexité de la technologie. **De l'autre**, il faut s'attendre à des innovations et à la sophistication des menaces, pour repérer et exploiter au mieux les failles nouvelles ou non corrigées : *réseaux non filaires, applications Web, etc.*, pour le vol massif de données, contrer les mesures en place, et tromper la vigilance. En outre, les méthodes d'ingénierie sociale seront plus subtiles, en ciblant les utilisateurs de façon personnalisée.

Pour certains experts, c'est l'augmentation du nombre d'occurrences des différentes menaces qui risque de poser un problème majeur, avec les outils et les territoires de non-droit, et la démultiplication d'infractions certaine mineures mais qui échappent aux moyens judiciaires. **Pour d'autres encore**, c'est le renforcement des menaces de détournement d'informations, dans un contexte de crise, voire de guerre économique, et l'exacerbation de la concurrence entre les entreprises, au niveau mondial mais aussi local.

Références :

Laïdi A. (2010) : Les États en guerre économique, Seuil.
Metzger M. (2010) : Letting the Air out of tire pressure monitoring systems, Conférence Defcon.
Rosé P., Loitier P., Guichardaz P. (1998) : L'infoguerre, stratégie de contre-intelligence économique pour les entreprises, Dunod.

http://blog.crimenumerique.fr/
http://laurentgentil.wordpress.com/
http://maghrebinfo.actu-monde.com/archives/article7622.html
www.enisa.europa.eu
www.forrester.com ; *The value of Corporate Secrets, Forrester Research, mars 2010.*
www.gao.gov/new.items/d07737.pdf
www.idtheft.gov/reports/IDTReport2008.pdf
www.infoguerre.fr
www.lemondeinformatique.fr/actualites/lire-motorola-poursuit-huawei-pour-espionnage-industriel-31269.html
www.mcafee.com/us/local_content/reports/7985rpt_labs_threat-predict_0110_fr_fnl_lores.pdf

[15] *"Racket"* ou *"taxage"*.
[16] Par tous moyens, notamment en exploitant les failles des techniques innovantes : *diverses cartes sans contact, RFID, etc.*

1.2. Les menaces envers les organismes

Il s'agit de présenter les résultats de l'étude concernant les menaces envers les organismes publics et privés, au cours de la décennie 2011-2020[17].

Pour cette question, il est présenté une synthèse qualitative des citations *; en précisant que les menaces dépendent du secteur d'activité de l'entreprise, du type de collectivité, et de la nature de l'administration, qui sont concernés.*

Concernant les menaces les plus graves

Les trois menaces les plus citées sont communes aux entreprises, **aux collectivités et aux administrations**. Il s'agit de :

- **l'indisponibilité** : *déni de service, sabotage, blocage, paralysie,*
- **l'atteinte aux données** : *stratégiques, personnelles, confidentielles, sensibles,*
- **l'atteinte à l'image** : *désinformation, diffamation, compromission.*

Du point de vue des sciences cognitives et sociales, **il est souligné les difficultés de gestion des crises pouvant entraîner la paralysie** partielle ou totale des réseaux et des systèmes d'information dont dépendent les activités critiques et les besoins majeurs, alors que **la dépendance envers ces systèmes est bien réelle**, **mais peu prise en compte.**

Les tableaux suivants présentent de façon décroissante le nombre de citations au regard des menaces correspondantes.

Nombre	Menaces les plus graves citées concernant les entreprises
9	Déni de service / blocage / paralysie / indisponibilité
8	Perte et vol de données stratégiques / concurrence déloyale
7	Désinformation / diffamation / atteinte à l'image
5	Intrusions / fraudes économiques / détournement de fonds
4	Cyber-extorsion / demande de rançon
3	Vol de données personnelles gérées par l'entreprise
2	Menaces sur les infrastructures vitales
2	Propagation de codes malicieux par réseaux sociaux / navigation Web
1	Abus ou détournement d'usage
1	Falsification de documents

Nombre	Menaces les plus graves citées concernant les collectivités
8	Perte et vol de données personnelles et confidentielles gérées
7	Désinformation / actions de nature politique / atteinte à l'image
6	Déni de service / blocage / paralysie / indisponibilité
3	Fraudes / détournement de fonds
3	Menaces sur les installations techniques / de sécurité / de surveillance
3	Cyber-extorsion / demande de rançon / chantage
2	Sabotage / menaces sur les infrastructures vitales
1	Propagation de codes malicieux par réseaux sociaux / navigation Web
1	Falsification de documents / atteinte intégrité d'informations nominatives

[17] Selon la question posée Q12 : Quelles seront les menaces les plus graves qu'auront à affronter les organismes : entreprises, collectivités, administrations, etc. ? *3 menaces par catégorie d'organisme.*

Nombre	Menaces les plus graves citées concernant les administrations
9	Perte et vol de données ou interception ou accès à des données sensibles
7	Déni de service / blocage / attaque de sites e-administration
4	Compromission de personnes / atteinte à l'image
3	Cyber-extorsion / demande de rançon : cyber-terrorisme
3	Menaces sur la sécurité / l'identité des personnes
3	Fraude notamment sur les documents officiels
2	Atteinte à l'intégrité des données / falsification de documents
2	Menaces sur les infrastructures vitales
1	Propagation de codes malicieux par réseaux sociaux / navigation Web

Références :

Clusif (2010) : Menaces informatiques et pratiques de sécurité en France.
Monnet B, Véry P, (2010) : Les nouveaux pirates de l'entreprise, Mafias et terrorisme, CNRS Editions, 250 pages.
Pons N. (2006) : Cols blancs et mains sales, Odile Jacob.
Pierrat J. (2008) : Mafias gangs et cartels : la criminalité internationale en France, Denoël.

http://datalossdb.org/
http://securityblog.verizonbusiness.com/category/2010dbir/
http://solutions-logiciels.com/actualites.php?titre=La-securite-des-systemes-SCADA-de-plus-en-plus-vulnerables&actu=4715
www.lecercle.biz
www.les-assises-de-la-securite.com *; livres bleus 2006-2010 et annexes*

1.3. Les menaces envers les personnes

Il s'agit de présenter les résultats de l'étude concernant les menaces envers les biens et données des personnes, au cours de la décennie 2011-2020[18].

Pour cette question, il est présenté une synthèse qualitative des citations *; en précisant que les menaces dépendent de l'usage généralisé en présence de vulnérabilités.*

Il est souligné que ces menaces devraient croître du fait :

- de l'existence et du développement de commerces clandestins prospères,
- des faiblesses de sécurité, notamment au niveau des transactions, des bases de données, des moyens informatiques personnels, etc.,
- de l'usage des moyens mobiles, en particulier de *"smartphones"*, et du paiement via l'Internet, qui se généralisent.

Les tableaux suivants présentent de façon décroissante le nombre de citations au regard des menaces correspondantes.

Nombre	Menaces à l'encontre des biens personnels
6	Escroqueries / détournements
2	Vol des éléments mobiles : GPS, téléphones, "*smartphones*", etc.
1	Intrusions physiques / cambriolages, *liés aux systèmes d'alarme et domotiques*

[18] Selon la question posée Q13 : Quelle sera l'évolution des menaces à l'encontre des biens et informations personnels.

Nombre	Menaces à l'encontre des informations personnelles
8	Vol / usurpation d'identité numérique / données RFID
6	Intrusions / vol / utilisation frauduleuse des données personnelles
5	Vol massifs de coordonnées et données bancaires / financières / cartes
4	Atteinte à la vie privée / détournements de moyens / géolocalisation
2	Chantage / divulgation d'informations compromettantes

Références :

Clusif (2009) : Panorama cybercriminalité 2009 ; *"Réseaux sociaux : menaces, opportunités et convergence", "Web 2.0, le cinquième pouvoir?"*
Desgens-Pasanau G., Freyssinet E. (2009) : L'identité à l'ère numérique, Dalloz.
Katenbach L, Joux A., Les nouvelles frontières du Net : qui se cache derrière Internet ?, First Société, 2010, p.227-255.
Pinte J.-P. (2010) : Pour protéger notre vie privée, Revue Défense n° 14 spécial Cybercriminalités, menaces et ripostes, p.38-39, Sept-Oct
Pinte J.-P. (2010) : Gérer son e-réputation sur le Net, Revue trimestrielle de la Gendarmerie Nationale, p.35-40.

http://213.139.102.176/gendarmerie/content/download/179227/1532551/file/p35-40%20Dossier%20Net%20PINTE.pdf
www.huffingtonpost.com/richard-barrington/foreclosure-documentation_b_774154.html
www.lefigaro.fr/hightech/2006/09/26/01007-20060926ARTWWW90414-internet_en_le_futur_trouble.php

1.4. Les menaces envers les propriétés de la sécurité

Il s'agit de présenter les résultats de l'étude concernant les menaces au regard des propriétés essentielles de la sécurité, au cours de la décennie 2011-2020[19].

Pour cela, les quatre propriétés fondamentales de la sécurité (CID-T) et leurs dépendances méritent d'être définies préalablement, comme les menaces et les entraves aux informations et aux systèmes[20].

Ces définitions sont synthétisées comme suit :

Confidentialité **C**	**Propriété** emblématique de maintien d'un secret, avec accès aux seules entités autorisées. **Les menaces** relèvent de l'accès illicite ou de l'interception, de la divulgation, de l'enlèvement ou de la perte. **Les entraves** concernent l'accès à des informations sensibles ou classifiées, par des tiers non autorisés, ou la divulgation volontaire ou accidentelle. **Dépendance** avec l'intégrité (I).

[19] Selon la question posée Q14 : Quelle sera l'évolution de la répartition des menaces à l'encontre de la confidentialité, de l'intégrité, de la disponibilité et de l'imputabilité *? informations et systèmes.*

[20] Rappelons que le terme "objet" s'applique aux informations et aux systèmes, et que par ailleurs : les objets sensibles relèvent de la confidentialité et de l'intégrité *(ex. Données personnelles, classifiées, de recherche et développement, etc.)* ; les objets vitaux relèvent de la disponibilité et de l'intégrité *(ex. Systèmes de contrôle, systèmes et données de commande, etc.).* En outre, la qualification de : "sensible" ou "vital" est préférable aux termes plus équivoques : *"stratégique"* ou *"critique".* Ces quatre propriétés (CID-T) sont essentielles, et il faut souligner les dépendances de trois d'entre elles vis-à-vis de l'intégrité qui apparaît comme fondamentale.

Intégrité **I**	**Propriété** emblématique de maintien des données et des composants sans corruption, dans l'espace et le temps. **Les menaces** relèvent essentiellement de la modification. **Les entraves** concernent la modification, par des tiers non autorisés, ou suite à un incident, ou à des erreurs commises par une personne autorisée. **Dépendance** avec la confidentialité (C).

Disponibilité **D**	**Propriété** emblématique de bonne délivrance dans les conditions définies d'horaires, de délais et de performance. **Les menaces** relèvent de la perturbation ou de l'interruption, de la destruction, de l'enlèvement ou de la perte. **Les entraves** concernent l'accessibilité aux données et la continuité des services en disposant des ressources suffisantes, par des personnes autorisées. **Dépendance** avec l'intégrité (I).

ImpuTabilité **T**	**Propriété** complémentaire attachée au suivi des opérations ou de fonctions réalisées, sans répudiation possible. **Les menaces** relèvent de la modification, de la destruction, de l'enlèvement ou de la perte. **Les entraves** concernent l'accès à un système de contrôle, mais aussi les manipulations non autorisés ou accidentelles, sur celui-ci ou sur des données de preuve. **Dépendances** avec l'intégrité (I) et la disponibilité (D).

Concernant l'ensemble des propriétés

Les menaces tiennent notamment au durcissement de l'environnement concurrentiel et au profit tiré d'informations sensibles, mais aussi aux difficultés de contrôle des informations liées au nomadisme et au *"cloud computing"* par l'exposition des données générées, en transit, et stockées à l'extérieur. Globalement, **pour certains experts**, la progression touchera l'ensemble des propriétés sans distinction. **Pour d'autres**, la confidentialité sera la propriété la plus menacée car elle comprend les objets les plus sensibles. La disponibilité sera également très touchée par des attaques distribuées, des arrêts de services, ou du sabotage d'infrastructures, sur des cibles vitales. **Pour une minorité**, la préoccupation des criminels sera l'imputabilité.

Concernant la confidentialité

Une forte progression des menaces est probable, notamment avec une recrudescence de la malveillance. On peut craindre en effet un intérêt toujours croissant à l'égard des données personnelles et professionnelles, très vulnérables en termes de confidentialité et d'intégrité.

Concernant l'intégrité

L'amplification des menaces relevant de la malveillance avec une dominante immatérielle est plausible, et les causes accidentelles ou dues à des erreurs humaines devraient se stabiliser. Il ressort que l'attaquant prendra avantage des fautes de ses victimes potentielles pour commettre une intrusion à distance, installer un code malveillant compromettant ainsi l'intégrité à d'autres fins, notamment dans le but de collecter des informations utiles.

Concernant la disponibilité

Une diminution des causes accidentelles est possible, contrebalancée par une accentuation de la malveillance, aboutissant malgré tout à une aggravation de compromission de la disponibilité. En fait, la répétition croissante d'attaques à l'encontre des serveurs et des infrastructures, et des dénis de service, tendent à montrer que la disponibilité sera de plus en plus impactée, malgré la réduction des risques avec la redondance, et notamment le recours au *"cloud computing"*.

Concernant l'imputabilité

Les causes accidentelles devraient restées stables malgré l'attention accordée à la sauvegarde des traces sous la pression croissante de la réglementation, mais les causes malveillantes devraient s'accentuer, dans un contexte d'attaques de plus en plus sophistiquées, et de tentatives de dissimulation des traces. Les logiques commerciales sont souvent opposées aux besoins de traçabilité et de conservation des traces. La cybercriminalité de proximité (notamment interne) pourrait augmenter la menace, mais de façon secondaire. Une minorité d'experts juge, qu'en raison des progrès de la sécurité et de la compétence des enquêteurs et juges spécialisés, la préoccupation première des criminels pourrait être de compromettre l'imputabilité.

Références :

Clusif (2010) : Menaces informatiques et pratiques de sécurité en France, rapport, 102 pages.

http://news.netcraft.com/archives/2010/04/15/april_2010_web_server_survey.html
www.huyghe.fr/actu_747.htm
www.cloudsecurityalliance.org/
www.arbornetworks.com
www.ponemon.org/research-studies-white-papers
www.cert.org/
www.memoireonline.com/04/09/2033/m_La-Cybercriminalite-nouveaux-enjeux-de-la-protection-des-donnees3.html

2. LES ATTEINTES

2.1. La répartition des atteintes

Il s'agit de présenter les résultats de l'étude concernant la répartition des atteintes tant en nombre qu'en gravité, au vu des infractions cités, au cours de la décennie 2011-2020[21].

Une mesure précise de la répartition des atteintes, en nombre comme en gravité, est très difficile, alors qu'**il est déjà délicat de prévoir l'évolution de la criminalité** classique générale. L'existence et la pertinence d'outils pour mesurer ces évolutions demeurent un problème que plusieurs démarches tentent de résoudre avec le partage au sein de la profession d'indicateurs de sécurité appropriés et l'élaboration de documents d'états de l'art associés. Par ailleurs, les enquêtes de victimation[22] ne sont pas toujours satisfaisantes au regard de la perception des risques par les personnes répondant aux questions. Cependant, et d'une façon globale, il est prévu une augmentation des atteintes du fait d'un fort accroissement de la connectivité des particuliers, des entreprises et des administrations.

Les tendances probables suivantes d'atteintes ont été identifiées :

Concernant les atteintes à l'identité électronique

L'usurpation d'identité électronique, résultant d'actes d'interception et de vol de données préalables, se développera, notamment du fait de l'Ingénierie sociale[23] maintenant entrée dans la cybercriminalité avec des outils logiciels malveillants et des procédés performants associés aux phénomènes de *"phishing"* et *"spamming"*. Les interceptions de données personnelles à partir des systèmes des particuliers, des entreprises, des collectivités, etc., vont continuer à s'accroître dans le temps, au vu d'une technicité qui, elle aussi, est en progression, et enfin des buts lucratifs ou autres visés.

Concernant les atteintes aux mineurs

La pédopornographie devrait rester au même niveau en ce qui concerne les actes physiques concomitants. Cette forme de criminalité s'appuie sur la *"matière humaine"*, avec des enfants victimes d'actes pédophiles ou eux-mêmes appelés à participer à la réalisation d'infractions. Elle demeure toutefois risquée pour les criminels, au vu de la répression. Ce qui évoluera dans ce domaine, c'est surtout la manière dont les échanges d'images et de vidéos s'effectueront, avec plus de disponibilité et des flux discrets conduisant à une banalisation des actes *; les pédopornographes arguant très souvent du fait qu'ils ne commettraient aucun acte répréhensible, en se considérant seulement comme de simples "voyeurs"*.

Concernant les atteintes aux infrastructures

Les infrastructures critiques seront les cibles d'un cyberterrorisme aux motivations variées. Les réseaux de distribution d'énergie, de transports et de communication devraient connaître

[21] Selon la question posée Q21: Quelle sera l'évolution de la répartition des atteintes en nombre et en gravité au vu des infractions : fraude, interception, vol de données et de propriété intellectuelle, usurpation d'identité, pédopornographie, e-réputation, etc. ? en distinguant les individus et les organismes publics et privés ; préciser notamment si les atteintes aux infrastructures critiques : télécoms, réseaux d'énergie, etc. peuvent devenir un risque majeur ?
[22] Telles celles qui sont réalisées en France annuellement par le Clusif.
[23] De l'anglais *"Social Engineering"*.

des attaques qui auront pour objectif la paralysie d'une nation par privation de services vitaux. De telles attaques pourraient causer des crises sans précédent à plusieurs niveaux : *économique, sécurité, santé, hygiène, paix civile, etc.* En outre, les *"hackers"* et autres cybercriminels, voire des États pourraient s'en prendre de plus en plus à leurs opposants. Il s'agira notamment de chercher à atteindre des sites d'information, avec des attaques de plus en plus nombreuses à l'encontre, soit de certains États, soit de groupes de résistance *(ex : dissidents tibétains en exil)*.

Concernant les atteintes à la réputation

L'atteinte réputationnelle[24] devrait être croissante, en gravité essentiellement, au point de devenir une cause significative, voire définitive, d'**atteinte à l'image** de l'entreprise ou de l'individu.

Concernant les atteintes à la propriété intellectuelle

Le vol de propriété intellectuelle et les différentes formes de contrefaçon prendront une dimension fondamentale, en nombre surtout, pour certains secteurs d'activité *(ex. R&D, innovation, sinon forte technicité)*. La propriété intellectuelle ne pourra jamais être réellement respectée et protégée; outre les œuvres artistiques, de nombreux documents mis en ligne sont plagiés allègrement par d'autres internautes.

Concernant les atteintes aux biens

Les escroqueries *"à la nigériane"*, reposant sur un appel à la charité, sur l'appât du gain et sur des rencontres hypothétiques, en provenance de certains pays[25] et à destination des pays plus développés, seront renforcées par une montée en puissance du taux de pénétration d'Internet et facilitées par la faiblesse des réseaux existants. Ceci vient compléter les fraudes aux moyens de paiement, suite aux vols et à l'exploitation des identifiants bancaires.

2.2. Les facteurs aggravants

Il s'agit de présenter les résultats de l'analyse consacrée aux différents facteurs aggravants dans la commission des infractions citées, au cours de la décennie 2011-2020[26].

Les facteurs aggravants principaux suivants ont été identifiés :

Concernant la mobilité et la virtualisation

La mobilité et en particulier le nomadisme impliquent naturellement une plus grande facilité à véhiculer les codes malveillants et à récupérer des données sensibles. Les systèmes d'information se fragilisent par la généralisation des accès distants et le stockage local de

[24] Ou *"e-reputation"*, concerne notamment l'atteinte à l'image de personnes connues, d'institutions ou d'autres organismes publics ou privés.
[25] En particulier des pays africains francophones pour les Français. Il s'agit de soutirer des sommes importantes à des personnes crédules dénommées *"mugus" ou "mougous"*, par les escrocs, et très souvent par l'intermédiaire complaisant d'un bureau de la Western Union associé au versement d'un pourcentage ou d'une commission à l'agent. Tandis que le phénomène se développe, les sommes en jeu sont suffisantes pour assurer un bon niveau de vie à toute une famille, voire d'un quartier, et parfois plus, et disposer ainsi de protections.
[26] Selon la question posée Q22 : Quels seront les facteurs aggravants : dépendance, crises, mobilité et nomadisme, dispersion en *"nuages"*, etc. ?

fichiers téléchargés, plus sensibles à certaines menaces telles que la perte ou le vol[27]. Par ailleurs, avec les systèmes en nuages, les entreprises comme les particuliers sont en mesure de perdre la vision physique de leurs données, voire l'accès.

Concernant les crises et les inégalités sociales

Une crise rend les utilisateurs moins attentifs et augmente leur crédulité vis-à-vis des escrocs toujours plus imaginatifs. Les crises économiques et sociales favoriseront la cybercriminalité, car elles permettront la croissance du nombre d'auteurs en externe, mais également parmi les collaborateurs des entreprises en mal de reconnaissance, et celle des actes, du fait d'un détournement d'attention des entreprises[28]. Les crises facilitent le recrutement par les différents groupes criminels de bons informaticiens, attirés par l'appât du gain. Un fossé de plus en plus profond risque donc de se creuser entre ceux qui ont accès à ces moyens de communication, à l'information et à de nouvelles formes de socialisation et ceux qui en sont exclus. Par ailleurs, la perte des repères sociaux ou moraux peut rendre les individus plus vulnérables à des sollicitations facilitées par l'Internet, ce qui favoriserait l'essor des entreprises sectaires. Enfin, certaines annonces d'organisations[29] médiatisées pourront conduire à des actes de rétorsion, par *"boycott"*, déni de service, etc., conçus comme justifiés et citoyens, avec toutes les chances d'être suivies d'effets divers, mais pas toujours maîtrisés.

Concernant l'évolution des systèmes d'information

La manière dont semble évoluer l'offre technologique, notamment au travers de la multiplication des interfaces mobiles, *-avec les "téléphones intelligents", les tablettes, l'informatique embarquée et connectée tel ce qui apparaît dans les automobiles, etc.-*, et de la virtualisation des systèmes de stockage, devrait se traduire par une aggravation de l'insécurité dans le cyberespace. Ceci en raison de la très faible mise en œuvre d'architectures sécurisées. Il est vu aussi que les architectures en nuages de type *"cloud computing"* estompent les frontières réelles et numériques, au point où on ne sait plus où sont stockées les données, qui les gère, qui les utilise, etc. De plus, l'offre commerciale liée aux systèmes de télégestion SCADA[30], destinés à la télésurveillance et à l'acquisition de données, s'est déplacée vers des équipements qui utilisent des technologies, protocoles et systèmes d'exploitation identiques à ceux du grand public : *TCP/IP, Ethernet, systèmes d'exploitation, etc.,* ce qui accroît leur vulnérabilité. Aussi, la complexité du réseau mondial fait que les attaques contre les réseaux critiques peuvent être démultipliées et dispersées.

Concernant la dépendance à l'égard des technologies

Selon l'enquête 2010 du Clusif, tous secteurs confondus et quelle que soit leur taille, 73% des entreprises jugent lourde de conséquences une indisponibilité de moins de 24h de leurs outils informatiques. La dépendance à l'égard des systèmes d'information est déjà un facteur vulnérant qui se renforcera, avec le développement du *"cloud computing"*, de la virtualisation et de la mobilité. Les particuliers, les administrations, mais également les entreprises ne prennent que rarement en compte le risque découlant de l'interconnexion de leurs systèmes. Les systèmes de secours permettant de travailler en local suite à des attaques sont rares, voire inexistants ou encore inefficaces face aux catastrophes. L'ensemble des services privés ou publics : *Trésor Public, mairies, hôpitaux, transports en commun, etc.*, pourraient

[27] En particulier, si les données sont sur des dispositifs portables : *"notebooks", "smartphones", clés mémoire, etc.*
[28] L'accroissement du recours à la sous-traitance et à *"l'outsourcing"* à l'étranger, essentiellement pour des raisons économiques, est prompt à des risques de perte de compétences et de maîtrise.
[29] Anonymous, Greenpeace, Wikileaks, etc.
[30] *Supervisory control and data acquisition.*

être entravés ou stoppés dans le but de causer de graves troubles à la santé, la sécurité et l'ordre public.

La dépendance de plus en plus forte des entreprises, le manque de diversité et l'hyper-criticité des systèmes interconnectés, mais aussi la complexité de prise en compte de la sécurité au niveau approprié des services *"en nuages"*, en particulier *"offshore"*, et la concentration des données dans des méga-centres, seront des facteurs aggravants.

Concernant la banalisation de la monétique

La banalisation de l'usage des monnaies virtuelles et/ou électroniques : Ces monnaies sont subdivisées en deux catégories : les monnaies de type *"confiance"* et les monnaies de type *"métaux précieux"*. La première a pour base la confiance entre l'acquéreur et le vendeur. Elle n'a pas de cours légal et n'a de valeur que pour les individus et les entreprises qui l'utilisent *(ex. : Webmoney "WMZ", et UKASH).* La seconde, qui a comme garantie des métaux précieux, se réfère à la valeur de l'or pour établir le taux de conversion à la monnaie électronique *(ex : Egold et Pecunix).* Une fois convertis, les fonds et le compte sont souvent impossibles à retracer. De plus en plus couramment utilisées, les cybercriminels vont donc de plus en plus chercher à s'en emparer. les victimes ayant le plus grand mal à justifier leur préjudice. Les réseaux criminels s'en serviront également pour masquer leurs transactions ou blanchir le revenu de leurs activités. Ils vont aussi s'en servir pour eux-mêmes. Parmi les monnaies électroniques citées ci-dessus, les criminels choisissent alors celles qui leurs garantissent le plus grand anonymat et plus faible traçabilité. Sur les sites Internet et les forums qu'ils fréquentent, *e-gold, Webmoney* et *Western Union* sont souvent privilégiés. En France, à la différence des notaires ou des banques agréées par la commission bancaire, ils ne sont pas soumis à émettre des déclarations de soupçon à TRACFIN[31] en cas de suspicion ou au-dessus d'une certaine somme.

Concernant la pénétration des équipements dans notre quotidien

La disparition progressive de la frontière entre **la vie privée et la vie professionnelle** avec l'usage d'équipements numériques domestiques pour exercer une activité professionnelle[32] entraînera des failles liées à l'hétérogénéité des équipements, tandis que l'accroissement du nombre d'appareils connectés représente aussi des portes ouvertes sur l'intimité du domicile, et des opportunités pour les cybercriminels.

Références :

www.clusif.asso.fr
www.ponemon.org, *"Business Risk of a Lost Laptop", Ponemon Institute, avril 2009*

[31] Pour *Traitement du Renseignement et Action contre les Circuits Financiers clandestins.*
[32] Associé au concept connu sous le non de BYOD, pour *"Bring Your Own Devices"*.

2.3. Les buts prépondérants recherchés

Il s'agit de présenter les résultats de l'analyse consacrée aux buts prépondérants recherchés dans la commission des infractions citées, au cours de la décennie 2011-2020[33].

Concernant la recherche de profits

Le premier but de la criminalité n'a jamais fondamentalement changé : il s'agit de **maximiser les profits financiers** en minimisant les risques, analysés de son propre point de vue. C'est ce qui rassemble toutes les communautés criminelles quelles que soient leurs motivations initiales et leurs zones géographiques d'action. Les atteintes à la vie privée ne sont qu'un moyen parmi d'autres pour arriver à ce résultat. Les tentatives de désorganisation ou de déstabilisation, si elles peuvent être perçues dans un premier temps comme des démarches idéologiques, sont souvent liées à un enjeu financier. Du fait d'une **concurrence** de plus en plus exacerbée, des actions de perturbation s'intensifieront à l'égard des entreprises. Les attaquants poursuivront un gain de compétitivité par des tentatives régulières et massives de pénétration et de pillage de la propriété intellectuelle parfois appuyées au niveau étatique.

Concernant la recherche du pouvoir

Le second but sera certainement la **recherche du pouvoir** , par le contrôle ou la destruction de l'information. En effet, si l'appât du gain reste l'un des buts prioritaires des cyber-délinquants, des actions de déstabilisation des centres vitaux devraient aussi se développer durant les prochaines années. En fait, le recours aux réseaux numériques est une stratégie qui nécessite peu d'investissements, notamment pour des pays émergents qui rencontrent de grandes difficultés économiques. Dans une société où l'information est une arme, la recherche, la détention et la maîtrise de cette dernière constitue un pouvoir évident pesant jusqu'au niveau des États. Il faudra également s'attendre à quelques actions spectaculaires visant des ressources et des infrastructures relevant de motifs idéologiques.

Les atteintes à la vie privée se poursuivront de façon à disposer et exploiter des données personnelles. Ces intrusions auront pour objectif final **la recherche d'un intérêt financier**, avec les données financières, bancaires, publicitaires, ou **la recherche du pouvoir**, avec les réseaux sociaux, le recrutement par des entreprises terroristes, etc.

Il est aussi considéré qu'avec l'émergence de divers **marchés de services cybercriminels**, un secteur commercial concurrentiel se mette en place, avec des acteurs criminels divers quant à leurs motivations, leur origine géographique et leurs capacités organisationnelles et techniques, qui chercheront à atteindre leurs buts criminels, quels qu'ils soient, en profitant des opportunités du cyberespace.

Références :

Verizon (2011à : 2010 Data Breach Investigations report, Verizon/US Secret Services

http://gocsi.com/

[33] Selon la question posée Q23 : Quel sera le but prépondérant recherché : pertes ou gains financiers, atteinte à la vie privée, déstabilisation, désorganisation, désinformation, destruction, terreur, etc. ?

2.4. La possibilité de compromission des États

Il s'agit de présenter les résultats de l'analyse relative à possible remise en cause de la stabilité des États du fait des comportements cités, au cours de la décennie 2011-2020[34].

Les avis sont plutôt partagés sur cette question, alors que les États y sont attentifs, si on en juge par la mise en place de dispositifs de prévention et de détection, à l'instar des États-Unis, *-avec le programme "Perfect Citizen" destiné à la surveillance des infrastructures jugées critiques pour la sécurité nationale-*, et de la Suisse, *-au vu du rapport annuel du Service de renseignement de la Confédération (SRC)-*.

Concernant la fragilité des États

Le rapprochement entre cybercriminels, États voyous et entités non-étatiques transnationales semble se mettre en marche. Les rumeurs d'attaques informatiques menées ou encouragées par des régimes nationalistes, corrompus ou autoritaires se font de plus en plus précises. Alors que le concept de cyberguerre n'est plus réservé à la science-fiction, il n'est pas improbable que des régimes instables, des États en rivalité et des mouvements terroristes ou radicaux, *-comme l'éco-terrorisme-*, fassent appel à des procédés utilisés en cybercriminalité. Après l'arme nucléaire, l'arme cybercriminelle apparaît redoutable et de surcroît *"propre"*, avec peu d'atteintes directes à des vies humaines.

La stabilité des États pourrait très certainement être compromise et ce serait sans doute le but recherché dans le cas d'attaques massives dirigées contre des infrastructures vitales et les réseaux nécessaires au bon fonctionnement de l'activité économique et sociale d'un pays. Des désinformations concertées, ou orchestrées, pourraient ainsi parvenir à une déstabilisation sociopolitique ou à une rétorsion par le boycott économique ou commercial d'un pays. D'ores et déjà, les États européens prennent ce genre de menaces au sérieux et simulent des incidents graves afin d'observer, coordonner et améliorer la mise en œuvre de contre-mesures entre toutes les structures nationales afin de réduire l'impact d'une cyber-attaque d'envergure voire tenter de la résoudre et de revenir à un état stable. L'efficacité des moyens de réaction et de coordination des États industrialisés reste cependant à démontrer.

Les infrastructures sensibles peuvent être une cible pour chantage avec demande de rançon, ou de la part d'organisations terroristes. Leur *"conversion"* aux systèmes standards universellement présents *(ex. Windows)*, l'abandon de systèmes fermés et l'ouverture indirecte de ces réseaux sur l'Internet, via les systèmes de gestion, accroissent d'une part, le nombre de personnes susceptibles de leur porter atteinte, et d'autre part, le nombre de points faibles.

La stabilité des États est forcément menacée, sinon compromise, par l'émergence d'un marché résilient de services criminels centrés sur l'utilisation illicite des technologies Internet. Un tel phénomène permet en effet de faciliter la commission de nombre d'infractions portant atteinte à la stabilité d'un État et d'entretenir une alternative attrayante pour les compétences pointues mal valorisées. Il s'agit notamment de tout ce qui relève d'activités de corruption, ou de blanchiment.

Concernant les facteurs limitant la fragilisation des États

Les sociétés industrialisées sont certes les plus dépendantes, donc les plus vulnérables en cas d'atteinte grave. Toutefois, leurs États possèdent des ressources intellectuelles et

[34] Selon la question posée Q24 : La stabilité des États pourrait-t-elle être compromise ?

matérielles pour faire face, en se coordonnant, même si on ne peut exclure des défaillances graves.

Si la stabilité des États est difficile à compromettre, elle peut néanmoins être affectée en partie dans les cas suivants :

- **actes de rétorsion** envers un pays par des organisations miliciennes ou paraétatiques pour défendre une cause, ciblant la disponibilité des réseaux d'infrastructures ou des e-services,
- **actes de dissuasion** ou d'avertissement envers un État à cause d'une politique jugée contraire à certains intérêts, visant la disponibilité des systèmes d'information de certaines administrations,
- **actes de terrorisme**, ciblant la disponibilité ou l'intégrité de sites Web institutionnels d'administrations sensibles.

Si **les États plus faibles** apparaissent moins dépendants aux technologies de l'information, donc moins vulnérables, il ne faut toutefois pas exclure que ces derniers soient aussi parmi les victimes collatérales, *par exemple*, d'une crise déclenchée par des manipulations informatiques sur les marchés boursiers ou par des attaques sur les infrastructures publiques : *énergie, télécoms, transports, administrations, etc.*

Concernant les États en tant qu'initiateurs d'attaques

Jusqu'à présent les États quels qu'ils soient ont toujours démenti leur implication dans ce type d'attaque. Le temps risque de n'être plus très long avant qu'une preuve indiscutable de leur participation ne soit apportée. Dans l'impossibilité d'entourer ces lieux chaotiques d'un *"cordon sanitaire"* qui empêcherait la mise en œuvre de telles actions, certains États démocratiques pourraient être tentés d'utiliser ces mêmes méthodes à des fins qu'ils jugent louables pour riposter, voire lancer des attaques préventives. Les conséquences d'une telle dérive, sous couvert de la protection de nos démocraties, pourraient cependant s'avérer catastrophiques.

Références :

Guinier D. (2010) : L'informatique dématérialisée en nuages - *Ontologie et sécurité du "cloud computing"*. *Expertises*, n° 351, octobre, pp. 335-344.
Goldstein G.-P. (2010) : Babel Minute Zéro, Thriller, Denoël., 723 pages

http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html?mod=WSJ_Tech_LEFTTopNews
www.lemonde.fr/technologies/article/2010/07/08/citoyen-parfait-le-big-brother-a-l-americaine_1385055_651865.html
www.news.admin.ch/NSBSubscriber/message/attachments/19841.pdf

3. LES AUTEURS

3.1. L'origine des agents menaçants

Il s'agit de présenter l'analyse consacrée à la description prospective de l'origine des menaces, au cours de la décennie 2011-2020[35].

Concernant les difficultés d'évaluation de l'origine

L'évolution de l'origine : ***interne, externe et mixte*, des menaces est difficile à estimer**, du fait de facteurs différents et de contradictions qui apparaissent dans les études ; en particulier parce que les faits sont rarement tous connus dans leur réalité, et qu'il faut bien distinguer le nombre d'incidents et le total des dommages causés. Il sera noté, qu'**en plus du développement de la cybercriminalité**, des pertes sont dues à des pannes ou à des dysfonctionnements, à des négligences ou encore, à des erreurs humaines. L'estimation est généralement de 80% pour les menaces d'origine interne contre 20% d'origine externe, mais ces chiffres ne reposent sur aucune source fiable et contradictoire en termes d'occurrence et d'impact.

Les experts sont donc partagés, en fonction de leur sensibilité aux évolutions et facteurs sous-jacents, tandis que l'argumentation se fonde sur le suivi des évolutions des années précédentes pour la compréhension du phénomène. **Une partie** des experts indique une augmentation de la répartition en direction des menaces internes, **une autre**, qui représente la grande majorité, au contraire, vers les menaces externes, et enfin **une troisième** pense à un **équilibre entre les menaces internes et externes** *; l'origine restant partagée et multiple, avec de surcroît des variations d'un pays à l'autre*. **En externe**, la majorité des experts estime néanmoins qu'il existe un risque croissant lié à la criminalité organisée transnationale, laquelle, bénéficiant des lacunes, poursuivra son essor.

Concernant l'accroissement des menaces internes

L'argumentation en faveur de l'accroissement des menaces internes se fonde notamment sur les tendances suivantes :

- la facilité de réalisation de menaces ciblées,
- la détérioration du climat social interne des organismes publics et privés,
- l'impact des insuffisances et des négligences internes, etc.
- la difficulté à concrétiser des menaces externes du fait de l'augmentation du niveau de sûreté.

Concernant l'accroissement des menaces externes

L'argumentation en faveur de l'accroissement des menaces externes s'appuie notamment sur les tendances suivantes :

- le nombre d'internautes formés aux nouvelles technologies,
- le maillage de la planète, le haut débit, le contexte et les conflits internationaux,
- les incidents liés aux partenaires, et aux agences situées à l'étranger, etc.

[35] Selon la question posée Q31 : Quelle sera l'évolution de l'origine des menaces : interne, externe et mixte ? *et en donner la répartition en % de 2010, 2015 et 2020*

- le développement de la criminalité de masse liée au développement d'Internet dans les pays émergents.
- une très grande interconnexion des systèmes, l'accès facile aux données des entreprises et des personnes connectées en permanence, etc.
- la criminalité organisée transnationale, difficilement contrée par l'amélioration des technologies, poursuivra son essor en raison des lacunes persistantes de la coopération internationale.

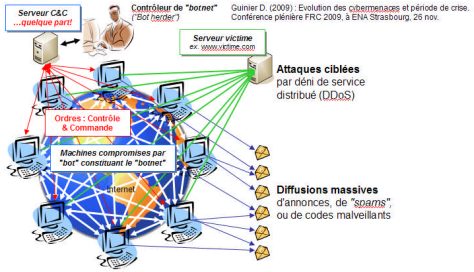
Concernant l'accroissement des menaces mixtes

L'argumentation en faveur de l'accroissement des menaces mixtes repose notamment sur les tendances suivantes :

- la difficulté d'attaques sans connaissance depuis l'extérieur,
- le recours à des moyens subtils d'ingénierie sociale,
- le profit partagé avec un tiers extérieur en période de crise, etc.

Concernant l'évolution du partage des menaces à plus ou moins long terme

Quelques experts jugent que l'évolution sur cinq ans ne permet pas de déterminer une nette tendance. Très peu d'entre eux ont établi des pourcentages, mais la tendance générale indique un essor de la menace externe à terme. **A court terme**, il s'agit de menaces liées à la multiplication de comportements déviants, et des ***"botnets"*** pour **constituer des dispositifs d'attaque efficaces**. **A moyen terme**, il s'agit de la compromission et/ou la destruction partielle ou totale du cyberespace et de ses instruments, y compris spatio-satellitaires. Sur ce point quelques experts envisagent la possibilité d'une catastrophe politico-idéologique et énergétique majeure.



"Botnet" destiné à des attaques ou des diffusions massives

Actuellement, la menace est pour la plupart des experts majoritairement de type interne, et résulte en grande partie d'actions accidentelles ou malveillantes humaines. **Dans les cinq années à venir**, la menace interne devrait diminuer sous l'effet de l'accroissement des mesures de sécurité prises par les entreprises. En revanche, la menace externe devrait augmenter en raison du développement général de l'Internet et des interconnexions des systèmes. L'essor de l'ingénierie sociale devrait conduire à la hausse d'une approche mixant action externe et interne.

A l'horizon 2020, la menace interne, bien qu'en forte baisse selon la majorité des experts, restera présente, notamment par la facilité d'accès plus grande aux systèmes d'information et la bonne connaissance des informations sensibles exploitables. La sécurité des systèmes d'information (SSI) en entreprise aura alors atteint une certaine maturité, et les moyens de lutte contre la fraude en interne seront formalisés. Concernant la menace mixte, l'ingénierie sociale poursuivra son développement pour chercher des complicités internes afin de contrer l'accroissement du niveau de sécurité.

En externe, **la majorité des experts** estime néanmoins qu'il existe un risque croissant lié à la criminalité organisée transnationale, laquelle poursuivra son essor en raison du manque de coopération internationale. De plus, l'informatique en nuages aura fini d'externaliser les risques et rendra prépondérantes certaines atteintes externes.

Références :

Clusif (2009) : Fraude interne, malveillance interne : détection et gestion. Conférence thématique du Clusif du 4 juin 2009.
CSI (2009) : 13th CSI Computer Crime and Security Survey 2008.
CSI (2010) : 14th CSI Computer Crime and Security Survey 2009.

http://accenture.com/dataprivacyresearch
http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf
www.bestpractices-si.fr/index.php?option=com_content&task=view&id=1110&Itemid=37
www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k9-fr.pdf
www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf
www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

3.2. Les profils et la répartition des agents menaçants

Il s'agit de présenter l'analyse consacrée à la classification des agents menaçants par catégorie, au cours de la décennie 2011-2020[36].

Concernant la tendance lourde et les réseaux de compétences

La majorité des experts conclut à une tendance lourde liée à l'organisation industrielle des activités cybercriminelles, avec son modèle économique, ses business plans, ses politiques tarifaires empruntés au monde marchand et même son service après-vente. De ce constat découle une disparition du profil ***"hacker"***cybercriminel indépendant au profit d'un mercenariat recruté pour une mission, en fonction des compétences, et œuvrant au sein d'équipes se partageant le travail, et donc les risques, grâce à une dispersion internationale. A ce titre, des spécialisations nationales semblent se dessiner : *logiciels en Russie, hardware au Japon, etc.* Il y a lieu aussi de ne pas oublier les groupes de ***"hackers"***, et les spécialistes de la propagande, de la déstabilisation et des manipulations, qui auront recours au support des réseaux sociaux et à des méthodes de fabrication ou de falsification réservées jusqu'alors aux faussaires.

Ces réseaux de compétences se vendent au plus offrant qu'il s'agisse de groupes criminels, de terroristes, de grands groupes industriels ou d'États ***"voyous"*** qui prennent sur étagère les outils d'attaque, de dissimulation ou de propagande sophistiqués dont ils ont besoin pour

[36] Selon la question posée Q32 : Quelle sera l'évolution des profils et la répartition des agents menaçants par catégorie : *"hackers" indépendants, groupes sociaux, activistes, groupements criminels organisés, terroristes, États, etc. ?*

atteindre leurs objectifs financiers ou politiques. La cybercriminalité apparaît ainsi dans leur arsenal comme une arme particulièrement efficace au regard de son faible coût.

Quelques experts considèrent que les États vont vraisemblablement convertir une partie de leur potentiel de lutte défensive en outils et forces de frappe offensifs pour tenter de rétablir un principe de dissuasion dans l'espace numérique ajoutant ainsi à la diversité des sources de menace. **Au-delà de cette tendance lourde** qui focalise l'attention, certains évoquent la persistance d'une criminalité de basse intensité *(ex. escroqueries entre particuliers)*, profitant d'opportunités dans la masse et de l'anonymat des flux numériques.

Concernant la difficulté de clarification des profils

Il apparaît illusoire d'établir une claire différenciation des profils, le vivier étant commun et toujours grandissant avec la démocratisation des technologies et les *"employeurs"* entretenant des intérêts parfois convergents. En outre, l'identification de l'attaquant reste aléatoire avec une traçabilité des attaques particulièrement complexe et rarement probante.
Les groupes d'activistes *(sectaires, terroristes ou extrémistes)* représentent des menaces en croissance, recherchant l'effet démultiplicateur médiatique et l'anonymat de leurs actions via les technologies de l'information. Ces mouvements vont de plus en plus utiliser l'Internet comme un élément de soutien à leur action.

Références :

Rosé P., Le Doran S. (1998) : Cybermafias, Denoël.
Rosé P. (1996) : Crime organisé et délinquance informatique, in L'Evolution de la criminalité organisée, actes du Cours International de Haute Spécialisation pour les Forces de Police, La Documentation Française.
Clusif 2010) : Une entreprise criminelle au microscope", Panorama cybercriminalité.
Guisnel J. (1995) : Guerres dans le cyberespace, services secrets et Internet, La Découverte.
CSIS (2008) – Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity, - US Center for Strategic and International Studies, Washington DC, décembre.

3.3. Les niveaux de compétences et les moyens nécessaires

Il s'agit de présenter l'analyse consacrée à l'étude du niveau de compétences ainsi que des moyens nécessaires pour réaliser des actes de nature et de gravité variables, au cours de la décennie 2011-2020[37].

Concernant les niveaux de compétences et de moyens

Sur l'évolution des niveaux de compétences et des moyens nécessaires **les experts sont partagés**. L'évolution devrait être distincte en fonction des diverses catégories d'agents menaçants. Il est en particulier noté l'importance de la maîtrise et de la commercialisation des kits permettant de créer ou de développer une activité cybercriminelle de plus ou moins grande envergure. Avec les nouveaux modes opératoires qui ne manqueront pas d'apparaître, en particulier pour l'automatisation et le camouflage des attaques, **il sera distingué** des groupes criminels spécialisés dans la revente de services criminels, et d'autres plus diversifiés, qui utiliseront ces services ou travailleront au profit de plus

[37] Selon la question posée Q33 : Quelle sera l'évolution des niveaux de compétences et des moyens nécessaires aux actes plus ou moins graves et de plus ou moins grande envergure ?

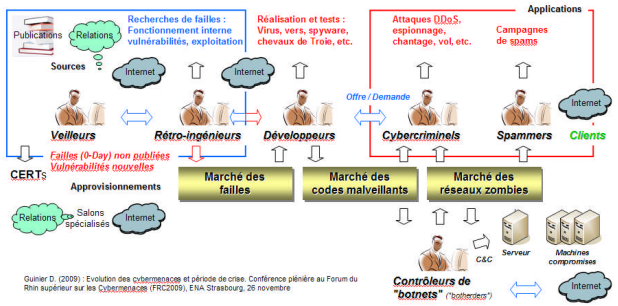
importants. Des **compétences juridiques et financières avancées** seront recherchées pour la mise en œuvre d'actions de blanchiment et de protection des auteurs.

Concernant l'industrialisation et l'économie de la cybercriminalité

Plus les moyens de défense seront complexes, plus le niveau d'attaque devra être élevé. La pénétration des systèmes (*critiques, bancaires, etc.)* est plus facile pour les personnes qui ont contribué à leur réalisation. Il conviendra de s'assurer de la loyauté des personnes créatrices des systèmes. Il en sera de même des personnes luttant contre la cybercriminalité, le risque étant de voir ces personnes franchir la frontière en raison du climat social, du niveau de rémunération ou encore du manque de reconnaissance. Il faudrait alors s'attendre à un plus haut niveau de compétences et d'équipements pour la cybercriminalité organisée, avec des mises à disposition de savoir-faire à destination d'opérations criminelles. Il en découle l'industrialisation et la mise en place d'une véritable économie relevant de la cybercriminalité avec, de façon schématique :

- **des compétences plus élevées pour les créateurs** de moyens : *outils et kits,*
- **des compétences plus faibles ou stables pour les utilisateurs** de tels moyens.

La cybercriminalité est envisagée en tant que service avec la notion de *"CyberCrimeware as a Service !"*. Elle repose déjà sur une offre : *"botnets"* et *"proxies"* loués pour des attaques par déni de services distribués (DDoS) ou des campagnes de *"spams"*, chevaux de Troie vendus et achetés sur des sites spécialisés ou de ventes aux enchères accessibles par le grand public.



Concernant l'argumentation en faveur d'un accroissement

L'argumentation en faveur de l'accroissement du niveau de compétences se fonde aussi sur l'appréhension des TIC et de l'Internet, et des méthodes de programmation dès l'enfance, sur la connectivité permanente dans un contexte de virtualité, et sur le niveau de compétences, *interne ou d'experts et de consultants externes-*, de plus en plus élevé et pouvant tirer partie de la connaissance du système d'information. **Celle en faveur de l'accroissement du niveau des moyens** se fonde sur les organisations qui disposent d'un niveau très élevé : les États, *avec des recherches avancées et des moyens en puissance de*

calcul considérable, et les entreprises qui coopèrent avec les organismes gouvernementaux, et sur les personnes hautement qualifiées nécessaires à la réalisation des moyens.

Concernant l'argumentation en faveur d'une stabilité ou d'une diminution

L'argumentation en faveur de la stabilité ou de la diminution du niveau de compétences se fonde sur le fait qu'un grand nombre d'escroqueries sur l'Internet sont commises par des personnes qui ne disposent pas de moyens sophistiqués, mais seulement d'une connaissance de la psychologie humaine et des comportements des individus. A ceci s'ajoutent les informations et les outils, soit librement disponibles, soit commercialisés sur l'Internet, suffisamment performants pour permettre à des acteurs indépendants et peu compétents d'entrer dans la cybercriminalité, et enfin le partage des savoirs et des travaux via des sites communautaires actifs.

Références :

CSIS (2008) : Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity, US Center for Strategic and International Studies (CSIS), Washington DC, décembre.

www.cnis-mag.com

3.4. La place du crime organisé

Il s'agit de présenter l'analyse consacrée à la place du crime organisée et à son évolution, au cours de la décennie 2011-2020[38].

Concernant l'évolution de la place du crime organisé

Tous les experts se rassemblent autour de l'idée que le crime organisé tiendra une place significative sinon majeure dans le phénomène cybercriminel. La nuance entre les experts se fait plus au niveau quantitatif que qualitatif, à savoir que l'activité du crime organisé en dépit de son poids aura pour priorité de rester toujours la plus discrète possible pour perdurer. La place relative du crime organisé peut, comme le souligne un des experts, être amoindrie par les concurrences et tensions internes mais aussi par l'émergence d'acteurs étatiques ou paraétatiques dotés d'une puissance financière et technique comparable pour défier une potentielle hégémonie.

Concernant la convergence du crime organisé et de la cybercriminalité

Au même titre que les activités humaines deviennent toujours plus dépendantes des nouvelles technologies de l'information et de communication, celles du crime organisé ont bien identifié tout le potentiel : *discrétion, rapidité, dématérialisation, internationalisation, risques faibles, forte profitabilité, etc.*, qu'elles pouvaient en tirer. L'emploi de ces technologies devrait donc aller croissant tant pour la conduite d'un large panel d'activités mafieuses que pour la dissimulation et le blanchiment du produit financier de ces activités, faisant de la cybercriminalité un point de convergence incontournable pour le crime organisé. Si la fracture numérique venait à s'accroître encore en défaveur de l'action des forces de l'ordre, en raison de la différence notable des moyens humains et matériels mis en œuvre, le crime organisé en tirerait un avantage toujours grandissant renforçant son attrait pour les outils numériques par rapport à la conduite *"traditionnelle"* de ses activités.

[38] Selon la question posée Q 34 : Quelle sera l'évolution de la place du crime organisé ? *Sera t-il un acteur majeur ou non ? Pourquoi ? Avec quelles stratégies ?*

Concernant la stratégie et les structures du crime organisé

La stratégie la plus souvent évoquée consiste à **exploiter la mondialisation des connexions pour développer les réseaux criminels à l'échelle mondiale** en s'affranchissant des contraintes géographiques et en exploitant les savoir-faire où ils se trouvent à l'exemple de la division internationale du travail. Une véritable économie du *"crime numérique"* se met en place avec une offre de services adaptée aux besoins du crime organisé, laquelle peut aussi être mise à profit par d'autres entités moyennant finances.

Le crime organisé monte de toutes pièces des structures puissantes, véritables entreprises du crime numérique, comme on le voit aujourd'hui dans l'ancien bloc soviétique et comme on devrait le voir émerger en Afrique et en Amérique du Sud. Il est et sera, de façon moins visible par rapport au nombre d'incidents, un acteur majeur avec des opérations de grande envergure : *détournements de fonds, fraude financière et économique, blanchiment*. Diverses activités auparavant traitées dans le monde réel sont maintenant hébergées dans le monde virtuel : *proxénétisme, prostitution, jeux d'argent, blanchiment, ventes illicites, contrefaçon*, tout passe par l'Internet. Ceci comprend aussi la désinformation en vue de déstabiliser des entreprises ou des États gênants pour les activités de ces groupes.

Références :

CSIS (2008) : Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity, US Center for Strategic and International Studies ,Washington DC, décembre.
Clusif (2010) : Une entreprise criminelle au microscope, Panorama cybercriminalité.
Rosé P., Le Doran S. (1998) : Cybermafias, Denoël.
Rosé P. (1996) : Crime organisé et délinquance informatique, in L'Evolution de la criminalité organisée, actes du Cours International de Haute Spécialisation pour les Forces de Police, La Documentation Française.
GRASCO (2010) : Garantir que le crime ne paie pas – Stratégie pour enrayer le développement des marchés criminels, sous la direction scientifique de C. Cutajar, Presses Universitaires de Strasbourg.

4. LES VICTIMES

4.1. Les secteurs les plus ciblés

Il s'agit de présenter l'analyse consacrée à la description prospective des secteurs socio-économiques qui devraient être les plus ciblés, au cours de la décennie 2011-2020[39].

Concernant l'ordre des secteurs les plus ciblés

Peu d'experts se risquent à déterminer l'ordre prioritaire des secteurs qui seront ciblés dans les dix prochaines années, sauf à reprendre des classifications existantes. Il reste très difficile de classifier les secteurs selon leur vulnérabilité. Ils sont tous concernés, aucun n'est à l'abri de la cybercriminalité, quelque soit la taille des structures. Dans tous les secteurs, des informations stratégiques et des enjeux financiers existent. Si la finance et le commerce électronique sont toujours cités en raison de leur fort attrait lucratif pour les cybercriminels, tous les autres secteurs sont déjà ciblés et verront leur vulnérabilité augmenter avec leur dépendance croissante aux technologies numériques et le caractère stratégique des informations qu'ils gèrent, dès lors qu'ils représentent un potentiel de désorganisation. La menace sera d'autant plus grande que la réflexion conduite pour anticiper les risques et développer les mesures de protection adéquates n'aura pas été aboutie. Par ailleurs, la menace devenant de plus en plus multiforme et empruntant des canaux de plus en plus complexes, il est probable que le taux de réussite des attaques furtives visant à des vols de données confidentielles ou à caractère personnel augmente.

Concernant l'ensemble des secteurs en fonction des buts

Pour la grande majorité des experts aucun secteur n'échappera à la cybercriminalité mais une distinction sera faite en fonction du but des attaques, tels le vol de propriété intellectuelle dans un but économique, *-pour le compte d'entreprises aidées ou non par leurs États-*, le gain financier rapide ou la déstabilisation malveillante, *-incluant le terrorisme, les atteintes à la réputation, les cyber-conflits, etc.-*. Dans le premier cas, il s'agit d'un pillage systématique des grandes entreprises en pointe dans leur domaine. Dans le second, les secteurs des finances et des transactions en ligne seront très régulièrement et massivement attaqués. Dans le dernier, les attaques seront extrêmement ciblées : industrie, énergie, *-dont le nucléaire-*, défense, infrastructures vitales, secteurs à forte composante politique ou sociétale, dans le but de détruire ou de créer autant de désordre que possible pour s'assurer du meilleur impact médiatique possible.

Nonobstant la multiplication des contrefaçons, de nombreux secteurs et notamment le transport, l'agro-alimentaire et l'industrie pharmaceutique sont en véritable guerre économique mondiale aujourd'hui. Ils devraient donc être l'objet d'un grand nombre d'attaques pour l'appropriation des secrets de fabrique et des projets. Enfin, il est très probable que certains secteurs d'activités, à la suite de l'industrie du divertissement, soient contraints à modifier leur modèle économique sous la pression des contrefaçons et les téléchargements illégaux massifs.

[39] Selon la question posée Q41 : Quels secteurs socio-économiques seront les plus ciblés : *finances et transactions en ligne, industrie et transports, énergie et défense, informatique et télécommunications, services, agro-alimentaire, santé, recherche, État et territoires, etc.* ?

Concernant le secteur des TIC

Le secteur de l'informatique et des télécommunications, *-plus généralement des TIC-*, apparaît comme une cible privilégiée avec son indéniable potentiel de déstabilisation dans une société toujours plus dépendante aux nouvelles technologies mais aussi en qualité de vecteur pour atteindre les autres secteurs. De même, il est probable que les tiers traitant d'informations sensibles comme les cabinets d'audit, d'assurances, de conseils, etc., puissent être à leur tour des cibles, dans la mesure où l'environnement réglementaire ou législatif tend à accroître leur rôle et leur périmètre d'interventions.

Références :

CE (2009) : Cybersecurity and politically, socially and religiously motivated cyber attack, Étude du Parlement européen, février
Verizon (2010) : Data Breach Investigations report, Verizon/US Secret Services
Clusif (2010) : Menaces informatiques et pratiques de sécurité en France, 2010

4.2. Les comportements des victimes

Il s'agit de présenter l'analyse consacrée à la description prospective de l'évolution des comportements des victimes, -individus et organismes-, au cours de la décennie 2011-2020[40].

Concernant les personnes physiques

Un consensus général se dégage parmi les experts, affirmant que les personnes physiques, mieux informées et sensibilisées aux risques numériques devraient pouvoir sortir d'un certain fatalisme, synonyme de passivité, en disposant de moyens accrus pour agir : *plates-formes de signalement gouvernementales ou des FAI*[41] *pour les contenus illicites, de bouton de signalement sur les réseaux sociaux, dépôts de plainte en ligne*.

Les signalements et dépôts de plainte devraient croître de façon notable face à l'augmentation des atteintes aux données personnelles. Toutefois, il apparaît clairement que cette tendance pourrait être largement contrecarrée si les moyens répressifs : *forces de l'ordre, magistrats, cadre légal et politique pénale*, n'étaient pas mis rapidement à niveau de ce contentieux de masse, quantitativement et qualitativement.

Peu d'experts, croient en un effort d'investissement particulier dans les solutions de sécurité logique, car les protections, souvent coûteuses, risquent de ne pas être à la hauteur quel que soit le secteur. Le salut pourra venir de leur intégration de série, et non plus en option, dans les logiciels et systèmes d'exploitation. Malgré tout ces solutions pourraient garder l'avantage si les services régaliens de protection proposés aux plaignants n'étaient pas suffisamment perçus comme efficaces.

[40] Selon la question posée Q42 : Quel sera l'évolution du comportement des victimes : *signalement et dépôt de plainte, mesures de protection, etc. ? en distinguant les individus et les organismes*. Cette question invitait les experts à distinguer l'évolution possible des comportements des victimes, selon que l'atteinte est portée à une personne physique ou une personne morale.
[41] Fournisseurs d'accès.

Concernant les personnes morales

Les personnes morales, elles aussi mieux informées et sensibilisées aux risques numériques, devraient pouvoir révéler une tendance générale inverse. Elles investiraient davantage dans les solutions de sécurité, les assurances et la formation de leur personnel, mais seraient toujours particulièrement réticentes à signaler des atteintes cybercriminelles et encore moins enclines à porter plainte pour préserver leur réputation (confiance des usagers/clients) et s'économiser les coûts d'une procédure incertaine. Seuls un cadre légal contraignant et une réponse effective et efficace du système répressif seraient de nature à inciter les personnes morales à mettre sur la place publique leur situation de victime de la cybercriminalité.

Cependant, avec l'essor rapide du phénomène *"phishing"*, les banques, au départ réticentes à communiquer sur le sujet, ont fini par porter plainte et reconnaître ainsi une certaine impuissance face au problème. Leur grande inquiétude était de voir fuir leur clientèle après reconnaissance de la corruptibilité des coffres-forts électroniques au regard de comptes bancaires en ligne. Mais l'action combinée de la police, de la justice, des institutions de coopérations judiciaires internationales, des CERTs[42], a permis de maintenir la confiance et d'imaginer des contre-mesures.

Concernant les attentes des victimes

Un constat commun demeure, l'effort de prévention, de formation, d'éducation des utilisateurs finals, simples particuliers ou relevant d'une personne morale, apparaît à tous comme le meilleur moyen d'infléchir les comportements vers une plus grande vigilance et maturité dans leurs activités sur l'espace numérique. Une forte attente est exprimée à l'égard de l'action étatique qui semble à ce jour sous-dimensionnée et impuissante au regard de l'ampleur du phénomène cybercriminel. A défaut, un expert évoque la mise en place de groupes de pression pour contraindre les gouvernements à réagir.

Le système judiciaire actuel ne peut que difficilement prendre en considération ces dossiers de cybercriminalité tant au stade de l'instruction qu'à celui du jugement. Ceci tient aux délais de procédure, peu compatibles avec ceux de la conservation des données, à la coopération internationale laborieuse hors de l'Union européenne. A ceci s'ajoutent la difficulté technique des dossiers et le faible niveau des réparations octroyées. A défaut d'amélioration rapide, les tribunaux pourraient avoir à connaître de moins en moins de ces litiges. Plusieurs experts pointent le risque de rejet de la société de l'information mais, plus sûrement, de banalisation du phénomène cybercriminel. En l'absence d'une réponse immédiate, sinon satisfaisante, les victimes seraient alors poussées à la résignation. Par ailleurs, des travaux récents montrent clairement cette défiance à l'égard de la capacité policière et pénale à traiter, à laquelle il faut ajouter un sentiment généralisé de culpabilité ou de honte des victimes qui se reprochent leur propre imprudence, et les incite à rester discrets sur leurs mésaventures.

Références :

Clusif (2010) : Menaces informatiques et pratiques de sécurité en France.
Symantec (2010) : Rapport Norton sur la cybercriminalité : l'impact sur les victimes.
Myriam Quéméner, Joel Ferry (2009) : Cybercriminalité, défi mondial, 2ème édition, Economica.

www.cybercrime.gov/reporting.htm#cc
www.internet-signalement.gouv.fr
www.ic3.gov

[42] Pour *"Computer Emergency Response Team"*.

4.3. Les facteurs d'influence sur les comportements

Il s'agit de présenter l'analyse consacrée à la description prospective des facteurs aptes à faire changer le comportement des futures victimes, au cours de la décennie 2011-2020[43].

Concernant les facteurs relevant de la sécurité

Les réponses du panel d'experts sont convergentes avec celles apportées à la question précédente. L'action de prévention et d'éducation, en pleine montée en puissance, mais qui mériterait selon certains d'être mieux coordonnée à l'exemple de la mission de la Prévention Routière, se révèle indispensable sans être suffisante pour changer réellement les comportements. Si cette action peut avoir un certain impact sur la crédulité des usagers les plus vulnérables, les ressorts de la nature humaine : *cupidité, vanité, lubricité,* restent immuables tout comme les comportements fautifs qui s'y raccrochent.

La majorité s'accorde pour dire que le coût de la sécurité devrait être partagé pour ne pas être laissé à la seule charge de l'usager et donc à sa libre appréciation. L'intégration de la sécurité pourrait être imposée aux fournisseurs d'accès, aux éditeurs de logiciels, etc. Un premier pas serait d'offrir un catalogue de conseils pratiques et de parades, indiquant : *que faire en cas de…*, en plus des mesures classiques de sensibilisation et de communication, d'éducation et de formation, de déontologie, etc. La limite pourrait être la *"schizophrénie"* des internautes qui, pour bon nombre adoptent également un comportement identifié comme cybercriminel : *téléchargements illégaux, achats de contrefaçons, curiosités malsaines, etc.*

Concernant les facteurs relevant de contraintes

Pour poursuivre dans l'analogie avec la sécurité routière, la plupart des experts considèrent qu'il sera nécessaire de **passer par des mesures contraignantes** ayant des conséquences personnelles en cas de non-respect ou de négligence avérée. Le but est de **responsabiliser** tous les utilisateurs d'outils technologiques et de leur éviter des comportements fautifs pour leur propre sécurité : *limitation des indemnisations, sanctions, obligations au regard de la protection des systèmes d'information, obligation de signalement, etc.* En cas de poursuite judiciaire, la justification de l'état réel de sa sécurité par rapport à un état de l'art de la profession pourrait s'avérer essentielle. Toutefois, quelques experts s'élèvent contre ce qui reviendrait à une seconde peine visant l'usager victime plutôt que les criminels.

La presse grand public pourrait exercer une pression de plus en plus forte en évoquant les fuites massives de données personnelles et en pointant du doigt les entreprises coupables[44]. Les dirigeants pourraient disposer d'informations exploitables de plus en plus fiables et partagées sur la cybercriminalité[45]. D'autres politiques publiques, plus interventionnistes, pourraient être envisagées[46]. La sécurité numérique pourrait devenir un objectif fondamental de l'État, garantissant un certain nombre d'obligations effectives. L'État en serait également le bénéficiaire pour la sécurité de ses propres systèmes.

[43] Selon la question posée Q43 : Quels seront les facteurs aptes à faire changer le comportement des futures victimes ? *Informations, obligations, pertes non indemnisées, etc.*
[44] Voir notamment l'actualité aux USA, avec les données bancaires et les récents procès médiatisés.
[45] Par exemple : la publication d'états de l'art concernant les principaux types d'incidents et de vulnérabilités, à partir d'indicateurs standardisés.
[46] A l'exemple du projet du gouvernement anglais d'assainir son parc informatique au regard de la menace de *"botnets"*.

Références :

CSIS (2008) : Securing Cyberspace for the 44th Presidency, CSIS Commission on Cyber-security, US Center for Strategic and International Studies, Washington DC, décembre
Symantec (2010) : Rapport Norton sur la cybercriminalité : l'impact sur les victimes.
Clusif (2010) : Menaces informatiques et pratiques de sécurité en France.

4.4. La répartition des victimes par tranches d'âge

Il s'agit de présenter l'analyse consacrée à la prospective sur l'évolution de la répartition des tranches d'âge des particuliers les plus touchées, au cours de la décennie 2011-2020[47].

Concernant l'ensemble des personnes

Les experts ne semblent pas détecter de véritable évolution des tranches d'âges ciblées par la cybercriminalité à un bref horizon. L'avènement des jeunes générations n'y changeant rien, puisqu'elles-mêmes adoptent des comportements à risque. Les plus vulnérables resteront les deux extrémités de la pyramide des âges, dont la maturité reste à parfaire dans les usages des technologiques numériques. Plusieurs experts soulignent par ailleurs que, *-bien plus révélateur que les classes d'âge-*, c'est **la situation de faiblesse** : *physique, psychologique et intellectuelle*, qui désigne les cibles privilégiées, selon la loi de la nature en quelque sorte. Aux plus jeunes et aux aînés viennent ainsi s'ajouter les personnes désocialisées ou isolées, les populations les plus défavorisées et les moins réceptives aux actions de conseils, de sensibilisation et d'information.

Concernant les personnes les plus jeunes

Les plus jeunes entre 10 et 20 ans, bien que *"digital natives"* et en apparence formés à l'usage, conservent les caractéristiques de la jeunesse : *l'insouciance, l'attrait de l'interdit et du risque, la curiosité insatiable et la naïveté, le besoin de s'affirmer, un mélange à haut risque sur les réseaux sociaux.* Les habitudes actuelles des adolescents de partage massif d'informations sur leur vie personnelle, non contrebalancées par la conscience des risques encourus, conduisent à une fragilisation de ces derniers face aux agresseurs potentiels. Cadres de demain, et donc détenteurs des informations sensibles, il apparaît impératif de corriger leurs comportements à risques.

Concernant les personnes les plus âgées

Pour **les seniors au-delà de 60 ans**, c'est l'accès, imposé plutôt que souhaité, aux nouvelles technologies devenues omniprésentes qui va conduire un grand nombre aux situations à risques dans un environnement qu'ils appréhendent mal. Ils relèveront d'un ciblage de plus en plus précis sur leur population, vulnérable et en expansion, en particulier dans le but d'abus de confiance ou d'escroqueries, dont ils seront les victimes.

Références :

www.bva.fr/administration/data/actualite/actualite_fiche/193/fichier_cp_genetic_juin2010_vf902af.pdf
www.tns-sofres.com/_assets/files/2010.05.27-enjeuxnumeriques.pdf

[47] Selon la question posée Q 44 : Quelle sera l'évolution de la répartition des tranches d'âge les plus touchées concernant les particuliers ? *personnes physiques.*

5. LES MESURES

5.1. L'application de la sécurité par les entreprises

Il s'agit de présenter l'analyse consacrée à la description de la tendance des entreprises à appliquer les normes de sécurité et à contrôler la mise en œuvre des mesures et procédures, au cours de la décennie 2011-2020[48].

Concernant les améliorations attendues

Les entreprises fonctionnent essentiellement sur le principe du retour sur investissement. Les normes de sécurité seront d'autant mieux appliquées et contrôlées qu'elles pourront clairement identifier les plus-values, *-en rapport avec la perception des risques encourus et le coût des mesures à prendre-*, ce qui reste encore bien difficile actuellement, faute d'une valorisation complète au regard des incidents informatiques.

Toutefois, un faisceau convergent de pressions permet de constater déjà une amélioration notable de la prise en compte de la SSI qui va se poursuivre sous l'effet de contraintes extérieures aux entreprises[49]. Le rapport fait état de progrès réalisés, la prise en compte théorique de la politique de sécurité des systèmes d'information (PSSI) passant de 55% en 2008 à 73% en 2010 dans les 350 entreprises consultées.

La plupart des experts estiment que les grandes entreprises et les secteurs les plus sensibles : *financiers, services, télécommunications, industrie, transports, énergie, etc.*, devraient être à l'avant-garde, suivis à un rythme moins soutenu par les PME/PMI, plus hésitantes à mettre en place une stratégie complète. L'externalisation, avec son aboutissement, le *"cloud computing"*, pourrait être une stratégie d'évitement de la problématique, mais sans nécessairement être une solution, sans l'application d'une politique de sécurité interne cohérente avec l'ensemble des services mis en œuvre à différents niveaux.

Concernant les exigences extérieures

Cette prise de conscience provoquée favorise déjà la mise en œuvre de procédures de veilles, prévention et gestion d'incidents ainsi que la conformation à des normes lorsque celles-ci sont établies pour l'activité concernée. Il sera en particulier vu la nécessité de mise en place de mesures de protection, avec des plans de reprise ou de continuité d'activité[50] associés à des moyens de secours, et des plans de sauvegarde concernant les données.

A cette tendance lourde s'ajoute une qualité et une pertinence des normes et de directives toujours grandissantes du fait de leur spécialisation croissante en fonction des domaines encadrés : *ISO 27002, ISO 20000, ITIL, PCI DSS, Bâle 3, Solvency2, directives de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ou standardisation européenne*.

[48] Selon la question posée Q51 : Quelle sera la tendance des entreprises à appliquer les normes de sécurité et à faire contrôler la mise en œuvre des mesures et procédures correspondantes ? *par catégorie d'entreprise et par secteur socio-économique.*
[49] L'amélioration a été soulignée dans le rapport d'enquête annuel 2010 relatif aux menaces informatiques et pratiques de sécurité, *réalisé et publié par le club de la sécurité de l'information français (Clusif).*
[50] PRA : plan de reprise d'activité ; PCA : plan de continuité d'activité.

Parmi les pressions extérieures figurent notamment l'encadrement juridique des activités les plus sensibles mais aussi les exigences de sécurité exprimées par les consommateurs, les partenaires et les autorités de régulation pour tous les secteurs d'activité qui font de l'application des normes de sécurité un avantage concurrentiel, *-avec en particulier, la certification indispensable pour certains contrats, et la publicité sur la qualité-*. Il s'agit même pour certains experts d'une condition de survie à moyen terme. Les assurances pourraient se joindre à ce concert en prescrivant des mesures de protection toujours plus exigeantes pour la mise en jeu des indemnisations. Pour prévenir une surenchère technologique coûteuse, une réglementation générique sur des objectifs minima à garantir en matière de protection pourrait utilement clarifier la situation. Un expert souligne toutefois que cette approche, *-pas forcément guidée par la recherche d'une protection optimale mais plutôt par la conformation à une obligation externe-*, ne garantit pas un suivi et un contrôle interne dans la durée, faute d'une appropriation par la gouvernance et le personnel.

Références :

Clusif (2010) : Menaces informatiques et pratiques de sécurité en France *; et également les éditions précédentes*.
Deloitte (2010) : Technology predictions.
Guinier D. (1994) : Catastrophe et management - Plans d'urgence et continuité des systèmes d'information, Ed. Masson, 336 pages.
Guinier D. (2006) : Dispositif de gestion de continuité - PRA/PCA : *une obligation légale pour certains et un impératif pour tous*. *Expertises*, n° 308, Nov. 2006, pp. 390-396.

http://fr.wikipedia.org/wiki/Plan_de_continuit%C3%A9
www.cigref.fr/cigref_publications/RapportsContainer/Parus2010/Position_CIGREF_sur_le_Cloud_computing_Septembre_2010_CIGREF.pdf
www.marchesetcontrats.fr/index.php?option=com_content&task=view&id=2689&Itemid=2

5.2. Les voies d'adaptation face à la cybercriminalité

Il s'agit de présenter l'analyse consacrée à la description prospective des voies suivies pour adapter le schéma de nos institutions et celui de la formation pour faire face au phénomène dans sa diversité, au cours de la décennie 2011-2020[51].

Concernant la sensibilisation, l'éducation et la formation

Dans leur grande majorité, les experts se sont focalisés sur la problématique de la formation identifiant ainsi un enjeu crucial dans le traitement du phénomène cybercriminel, avec la sensibilisation et l'éducation.

A quelques rares exceptions près, le consensus s'établit sur l'insuffisance des formations actuellement en place, qu'elles soient initiales ou continues, destinées au *"top management"* ou à tout un chacun. Avec l'essor des technologies numériques, ce constat semble pris en compte par le système éducatif qui intègre progressivement des modules de sensibilisation à la sécurité et à la protection de l'information et des systèmes d'information (B2I). Toutefois quelques experts relativisent l'intérêt de ces modules en soulignant qu'ils ne consistent souvent qu'en une mise en relation de l'enfant avec la machine, et que le corps enseignant

[51] Selon la question posée Q52 : Quelles seront les voies suivies pour adapter le schéma actuel de nos institutions et celui de la formation initiale et continue pour faire face au phénomène dans sa diversité ? *du risque ordinaire à la cyberguerre*.

dispensant ce module n'est lui-même pas forcément au fait des technologies dont il est censé parler.

Les experts appellent de leurs vœux la poursuite des efforts, et l'intégration systématique de ces problématiques dans tous les cursus scolaires pour éduquer l'ensemble de la population. Une formation plus poussée est même considérée comme impérative pour les dirigeants et les décideurs dès leur formation initiale avec des *"piqûres de rappel"* régulières. Les techniciens spécialisés devraient pour leur part être annuellement recyclés. La mise en place de formations destinées aux acteurs de la chaîne répressive : *justice, forces de l'ordre, experts*, présente un apport indéniable. Il y a lieu de les étendre. Si quelques formations de bon niveau existent, elles devraient se généraliser dans la prochaine décennie en s'appuyant sur quelques projets pilotes.

Concernant la réorganisation des institutions

Quelques experts se sont exprimés sur l'évolution des institutions en soulignant que le livre blanc sur la sécurité et la défense nationale de 2008 avait conduit à une réorganisation pertinente de l'action étatique pour protéger les infrastructures vitales par rapport aux cyberattaques (*Agence nationale de la sécurité des systèmes d'information (ANSSI), Plan et exercices "Piranet", Observatoires zonaux de la sécurité des systèmes d'information (OZSSI)*). Les forces de l'ordre et la magistrature professionnalisent progressivement leur personnel avec un cadre légal qui évolue également pour une meilleure prise en compte du phénomène cybercriminel. Sont notamment citées les plus récentes : *la cyber-infiltration, et le délit d'usurpation d'identité numérique*. Des formations pluridisciplinaires sont organisées associant les avocats, le secteur privé, les services d'enquête spécialisés et les magistrats pour un partage des savoir-faire et de l'état de l'art.

Il est cependant noté qu'il n'y a pas forcément d'adéquation entre la volonté, les discours politiques et les moyens concrets mis en place. Pour l'instant, seulement 0,2% des effectifs des forces de l'ordre disposent des qualifications techniques pour conduire les investigations numériques.

Deux écueils sont signalés. Dans un premier temps, la mise en ordre de bataille des services de l'État ne doit pas cacher que la sécurité est l'affaire et de la responsabilité de tous. La sécurité devrait donc être pensée comme une composante de tous les métiers et les partenariats publics-privés devraient s'intensifier, certains préconisant même le *"leadership"* du secteur privé plus réactif. Dans un second temps, quelles que soient les qualités d'un dispositif national, la cybercriminalité ne pourra être combattue que par une action mondiale.

Concernant la posture offensive

Au-delà de la posture essentiellement défensive qui se dessine, avec de surcroît le renforcement des niveaux de robustesse de l'ensemble des infrastructures[52], et l'intégration des réflexes de gestion de crises, quelques experts souhaiteraient que soit également développée la lutte informatique offensive, *-avec le recrutement, la formation et le développement d'outils spécifiques-*, mais aussi une réflexion sur la dissuasion, la légitime défense, l'ordre public sur le cyberespace.

Références :

http://userpage.fu-berlin.de/~jmueller/its/conf/Madrid02/abstracts/Ghernaouti-Helie.pdf
www.bestpractices-si.fr/index.php?option=com_content&task=view&id=1101&Itemid=57

[52] Y compris spatio-satellitaires, et centres de traitement.

www.bestpractices-si.fr/index.php?option=com_content&task=view&id=1022&Itemid=93
www.ined.fr/fr/pop_chiffres/france/structure_population/regions_departements/
www.mcafee.com/fr/local_content/reports/virtual_criminology_report/virtual_criminology_report_2009_fr.pdf
www.met.police.uk/pceu/documents/ACPOecrimestrategy.pdf

5.3. Les mesures de réduction du phénomène

Il s'agit de présenter l'analyse consacrée à la prospective concernant les diverses mesures les plus promptes à réduire le phénomène, au cours de la décennie 2011-2020[53].

Concernant la nécessité d'une culture appropriée

Certains experts n'ont pas trouvé justifié de distinguer l'impact des mesures selon qu'elles s'appliquent aux particuliers et aux organismes, les premiers composant les seconds, et parce qu'ils considèrent que les mesures évaluées comme les plus pertinentes touchent généralement les deux cibles.

Ainsi, dans la continuité de la question précédente, **l'unanimité** se fait sur le développement primordial des formations et des sensibilisations. L'éducation des usagers aux risques numériques, mais aussi à leurs responsabilités personnelles, est une condition *sine qua non* de la compréhension de toutes les autres mesures envisageables. Une culture de la sécurité, de la lutte informatique défensive, voire offensive, est à inculquer aussi largement que possible. Il est possible de s'appuyer sur une organisation interne conçue pour préserver la sécurité des informations sensibles. Certains pays ont déjà engagé des formations de spécialistes dans ce but.

Concernant les mesures organisationnelles et leur partage

Les mesures organisationnelles sont **particulièrement mises en avant au niveau étatique**, qu'il s'agisse du positionnement institutionnel des organismes pilotes de la lutte contre la cybercriminalité ou de la nécessité d'une coordination nationale mieux affirmée avec une mission interministérielle jugée par beaucoup comme indispensable compte tenu des enjeux. Cette approche se conjugue avec la demande d'une politique publique plus effective et moins déclaratoire passant par des moyens financiers et humains accrus pour faire face à l'ampleur de la menace. La complexité des enquêtes auxquelles se heurteront les policiers notamment au regard des moyens d'anonymisation et de cryptographie, nécessiteront une expertise toujours plus pointue. Des moyens nouveaux d'investigation seront à inventer, techniquement, éthiquement et juridiquement parlant. En attendant, les efforts entrepris pour diffuser les bonnes pratiques, au travers de guides et de forums, doivent être poursuivis et intensifiés.

Enfin, **quelques experts** ont évoqué le partage du fardeau de la lutte contre la cybercriminalité avec le secteur privé. Sont notamment mentionnés un cadre réglementaire toujours plus contraignant pour les fournisseurs d'accès en termes de traçabilité et d'identification ou des normes de sécurisation pour les éditeurs de logiciels ou l'engagement de la responsabilité des sites commerciaux. Les fournisseurs d'accès devront respecter des obligations de plus en plus draconiennes de conservations de données et de protections des utilisateurs.

[53] Selon la question posée Q53 : Quelles seront les mesures : législatives, politiques, techniques, organisationnelles, et humaines les plus promptes à réduire le phénomène ? *en distinguant les particuliers et les organismes.*

Concernant les mesures législatives et techniques

Les mesures législatives et techniques font d'avantage débat. **Certains experts** jugent l'arsenal légal et réglementaire satisfaisant, mais insuffisamment exploité et généralement inapplicable hors des frontières. Il serait à ce propos pertinent d'harmoniser les textes, et de les faire plus largement connaître. **D'autres**, au contraire, pensent inéluctable, au moins souhaitable, l'édification d'un droit dédié, constituant une partie du Code pénal et du Code de procédure pénale. Celui-ci devra conduire à plus de transparence pour l'identification et la comptabilisation des cybercrimes, et à des procédures et des moyens spécifiques octroyés aux agents de la force publique, *-notamment pour l'interception, l'infiltration, et l'anonymat-*, tout en renforçant malgré tout la protection de la vie privée et les données personnelles des usagers. Pour les dispositifs techniques, si leur amélioration est une évidence, ils seront toujours contournables mais surtout trop coûteux pour le commun des usagers.

Concernant les conditions de la réussite

Quelles que soient les mesures envisagées, une des conditions de réussite régulièrement mise en avant est leur **application au niveau international**. Apparaissent prioritaires une harmonisation des dispositifs, des coopérations, la généralisation du gel des données, et la réactivation du réseau 24/7 de partages d'informations et d'alertes, évitant ainsi aux cybercriminels de se retrouver dans des *"paradis numériques"*. Il conviendra à cet effet de réfléchir sur la notion de cyber-frontière.

Au plan international, il faut souligner qu'il n'existe actuellement que la convention de Budapest du Conseil de l'Europe comme outil juridique applicable. Dans ce cadre, le Conseil de l'Europe devrait pérenniser ses réunions d'experts *"Octopus Interface"*[54], qui sont des rendez-vous annuels d'échanges sur les problématiques émergentes comme l'externalisation des données et la protection de la vie privée. Cet instrument est toutefois contesté par de grands pays comme la Chine et la Fédération de Russie qui militent en faveur d'une convention universelle. L'UNODC[55] a initié en janvier 2011 une étude internationale sur le phénomène de la cybercriminalité qui pourrait probablement déboucher sur un tel cadre juridique universel. Au niveau européen, plusieurs projets de directives sont en négociation pour apporter une réponse communautaire. **Ces initiatives sont porteuses d'espoir à condition qu'elles se traduisent par des actions concrètes**.

Références :

INSEAD (2009) : Safeguarding the Corporate IT Assets, Micro Focus

www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_fr.pdf
www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/103537.pdf
www.marchesetcontrats.fr/index.php?option=com_content&task=view&id=1804&Itemid=80

[54] Au sein des conférences organisées par la Division du crime économique, de la Direction générale des Droits de l'Homme et des Affaires Juridiques du Conseil de l'Europe.
[55] *United Nations office on drugs and crime*, l'Office des Nations unies contre la drogue et le crime.

5.4. Les partenariats et coopérations à développer

Il s'agit de présenter l'analyse consacrée à la description prospective des partenariats et des coopérations développés à divers niveaux, au cours de la décennie 2011-2020[56].

Concernant le partenariat public-privé et les initiatives

Les experts reconnaissent tous que la lutte contre le phénomène cybercriminel passe par la mise en commun des efforts et des moyens et déplorent le manque d'initiative dans ce domaine. Le traitement de la cybercriminalité nécessite une extrême réactivité pour compenser la volatilité des données et des traces dans l'espace numérique.

Le partenariat public-privé (PPP) semble le plus prometteur en assurant le partage du fardeau financier, en particulier, mais aussi de l'information disponible. **Diverses initiatives**, comme le club R2GS, les conférences OCTOPUS, le forum international sur la cybercriminalité (FIC) et le forum du Rhin supérieur sur les cybermenaces (FRC), visent à cette mise en commun de la réflexion et des savoir-faire respectifs.

Le PPP apparaît comme très pertinent dans le domaine de la recherche et développement de parades et d'outils de détection avec les entreprises œuvrant dans le domaine des technologies de l'information et de la communication ou avec les laboratoires et les centres d'expertise privés.

Toutefois, plusieurs experts soulignent que ce partenariat reste à équilibrer et que des protocoles doivent être établis pour garantir des relations de confiance et de confidentialité afin de faciliter le partage d'information et la collaboration opérationnelle *(investigations, traçabilité, alertes, gestion de crise)* avec des partenaires privés, très souvent anglo-saxons.

Concernant les centres d'expertise et de réponse aux incidents

Les centres d'experts et de réponse aux incidents liés aux technologies de l'information sont des acteurs importants et incontournables qui commencent seulement à s'ouvrir aux requêtes des forces de l'ordre. Les autorités judiciaires devront compter sur leurs capacités à identifier, remonter, stopper un incident, et leurs facultés à faire conserver les données. Ces réseaux d'ingénieurs et de pairs peuvent mener un *"take down"*[57], sur un serveur n'importe où dans le monde en moins d'une heure, en prenant contact avec les hébergeurs et les fournisseurs d'accès pour faire cesser la fraude.

Il faudra établir un rapport de confiance et convaincre les autorités judiciaires de la valeur des informations transmises par ces centres. Le centre d'expertise gouvernemental CERTA[58], *dépendant de l'ANSSI*[59], et les autres CERTs[60] sont d'ores et déjà en rapport avec l'OCLCTIC[61], et fournissent des renseignements précieux destinés à la lutte contre la cybercriminalité. L'expérience européenne dans le domaine de la formation, avec les centres d'excellence 2CENTERS[62] et leur perspective de mise en réseau, se révèle comme une

[56] Selon la question posée Q54 : Quels partenariats seront développés aux niveaux national, européen et international, et les coopérations : *public-privé, citoyenne, judiciaire, etc.*
[57] Chute d'activité nuisible.
[58] Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques.
[59] Agence nationale de sécurité des systèmes d'information.
[60] Centres d'experts et de réponse aux incidents liés aux technologies de l'information, tels que le CERT-SocGen *(CERT de la Société Générale)*, le CERT-Lexsi, etc.
[61] Office central de lutte contre la criminalité des technologies de l'information et de la communication.
[62] Les 2CENTERS, réunissent universités-entreprises-NTECH et forces de l'ordre.

piste à suivre avec intérêt. Le mixage de ces différents univers les enrichit mutuellement en termes d'approche et de traitement de la menace.

Concernant les instances d'échanges et la coopération internationale

La réponse citoyenne paraît également pouvoir s'intensifier par la mise en place des instances d'échanges à l'exemple du forum des droits sur l'Internet, ou des outils de signalement permettant à l'usager de prendre un rôle actif dans le dispositif de vigilance tout en garantissant une réponse équilibrée en terme de protection des droits individuels.

La coopération internationale naissante, reste un élément clé avec une large marge de progression. La montée en puissance de la menace va la rendre impérative au risque de désastres numériques. Les limites nationales ou européennes sont révolues pour lutter contre la cyberdélinquance. Des partenariats existent déjà au niveau international en termes de coopération policière avec INTERPOL, EUROPOL *(European Police Office)* et le réseau G87/H24. Les autorités judiciaires devront développer les relations avec des CERTs *(Centres d'Experts et de Réponse aux incidents liés aux technologies de l'information)* privés, nationaux et internationaux, afin d'augmenter la réactivité face à des incidents très généralement extraterritoriaux. Certains experts considèrent cependant que la coopération avec quelques États dits : *"voyous"* restera impossible.

Références :

www.2centre.eu
www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_fr.pdfwww.foruminternet.org
www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/103537.pdf
www.fic2010.fr

CONCLUSION

L'analyse des réponses formulées de façon indépendante par les experts aboutit à un large consensus. Elle apporte des indications riches et abondantes au vu des sensibilités des uns et des autres. Elle forme ainsi une vision prospective sur l'évolution de la cybercriminalité à l'horizon 2020 au travers de ses composantes, à savoir les menaces, les atteintes, les auteurs, les victimes, et les mesures. Chacun s'accorde sur le fait que **la cybercriminalité occupera une place prépondérante en couvrant le spectre de la criminalité classique**, tandis que la sécurité reste un problème récurrent.

Alors que la conclusion de la précédente prospective à l'horizon 2005[63] s'est avérée juste dans les faits concernant la sécurité informatique, il est notable que la présente révèle de nombreuses similitudes. Il est cependant noté une amplification et des nouveautés au regard du développement rapide des technologies de l'information et de la communication, de la généralisation de leur usage et de services sans frontières, certains étant en rapport avec la montée du crime organisé. Ce dernier est en mesure de développer ses réseaux à l'échelle mondiale en s'affranchissant des contraintes géographiques et juridiques. Il cherchera aussi à mettre en place de puissantes structures pour saisir de nouvelles opportunités, diversifier et faciliter ses activités criminelles, avec des opérations de grande envergure, *tels que la fraude financière et économique et le blanchiment*, et des activités bien réelles, *telles que la prostitution, les jeux, les ventes illicites et la contrefaçon*, qui seront hébergées dans le monde virtuel et passeront par l'Internet.

Les principes fondateurs de l'Internet que sont l'interopérabilité, l'ouverture et la neutralité, sont prompts à son développement, alors qu'il devient un enjeu économique, politique et géostratégique, avec des dérives et des monopoles qui se dessinent. Une gouvernance globale au niveau international jusqu'à celui des territoires devrait favoriser la régulation et la sécurité, permettre de protéger les intérêts des États, des entreprises et des citoyens, en luttant contre la cybercriminalité tout en évitant les guerres dans le cyberespace dont les premières manœuvres virtuelles apparaissent déjà. Le terrorisme pourrait aussi s'appuyer sur diverses fragilités et développer des méthodes pour les appliquer avec des impacts considérables. Aussi, quelles que soient les qualités du dispositif, **la cybercriminalité ne pourra être combattue qu'au niveau mondial**.

Pour l'essentiel :

Les menaces émergeantes portent sur les données, les transactions, les systèmes, les infrastructures et les services stratégiques, alors que les innovations sont sujettes à des vulnérabilités et à des détournements de finalité. Elles relèvent de divers facteurs, dont certains sont récurrents et d'autres concernent les crises, le durcissement de la concurrence, et les nouveaux usages, qui exposent à de nouveaux risques. Les menaces envers les organismes, et de façon commune aux entreprises, aux collectivités et aux administrations, seront l'indisponibilité, l'atteinte aux données et à l'image. L'évolution des réseaux sociaux, confortée par le goût croissant des utilisateurs, ne manquera pas de générer des menaces à l'encontre des personnes, mais aussi des entreprises, des organisations publiques et des États. Il est souligné les difficultés de gestion des crises et la possibilité d'une paralysie. Les menaces envers les personnes seront les escroqueries et les détournements, les vols, l'usurpation d'identité, les intrusions et l'utilisation frauduleuse des données personnelles.

[63] L'analyse prospective portait sur la période de 1991 à 2005, voir Rosé P. (1992), pp. 137-142.

Les atteintes concernent le vol et l'usurpation d'identité, notamment du fait de l'ingénierie sociale, avec des outils et des procédés performants, tels que les *"botnets"*, associés aux phénomènes de *"phishing"* et de *"spamming"*, aux fins de commettre d'autres délits. La pédopornographie devrait évoluer dans la manière dont les échanges d'images et de vidéos s'effectueront, avec plus de disponibilité et des flux plus discrets. Les infrastructures critiques seront les cibles au vu de motivations variées. Dans ce cas, des attaques pourraient alors causer des crises sans précédent, à divers niveaux. L'atteinte à la réputation devrait être croissante et le vol de propriété intellectuelle et les différentes formes de contrefaçon prendront une dimension fondamentale, sans que la propriété intellectuelle ne puisse être totalement respectée. Des facteurs aggravants ont été énumérés au regard de différents buts, essentiellement liés à la recherche de profits et de pouvoir. Il existe également une possibilité de compromission d'États fragiles, avec des tentations, pour d'autres, d'être les initiateurs d'attaques dont les conséquences pourraient être catastrophiques pour les premiers.

Les auteurs seront internes et externes de façon variable. La majorité des experts conclut à une tendance lourde liée à l'organisation industrielle des activités cybercriminelles, fondée sur des éléments empruntés au monde marchand, avec des réseaux de compétences qui se vendront au plus offrant. Il faudra aussi compter avec une criminalité profitant d'opportunités de masse pour des escroqueries, et sur le développement des réseaux sociaux comme nouveaux vecteurs d'influence. Les groupes de *"hackers"* et d'activistes représenteront aussi des menaces croissantes, recherchant souvent l'effet médiatique de leurs actions via l'Internet, notamment pour disposer de soutiens à leurs actions. L'évolution des niveaux de compétences devrait distinguer des groupes criminels spécialisés dans la revente de services, et d'autres, plus diversifiés, utilisateurs de ces services ou travaillant au profit de plus importants qu'eux. Des compétences juridiques et financières avancées seront aussi recherchées pour la mise en œuvre d'actions de blanchiment et de protection des auteurs. En dépit de son poids, l'activité du crime organisé devra rester aussi discrète que possible pour perdurer.

Les victimes seront issues de tous les secteurs où des informations stratégiques et des enjeux financiers existent. Le secteur de l'informatique et des télécommunications apparaît comme une cible privilégiée, avec son potentiel de déstabilisation dans une société toujours plus dépendante à ces technologies, mais aussi en qualité de vecteur. Les secteurs sont déjà ciblés dès lors qu'ils présentent un potentiel financier ou de désorganisation. Une distinction est à faire en fonction du but des attaques, qu'il s'agisse de piller des entreprises en pointe ou celles de la finance sinon des transactions en ligne qui seront régulièrement et massivement attaquées, ou encore, de détruire ou de créer autant de désordre que possible pour s'assurer du meilleur impact médiatique. Concernant les tranches d'âge des personnes physiques, les plus vulnérables se situent aux deux extrémités du fait d'une maturité restant à parfaire dans l'usage des technologiques numériques. C'est essentiellement la situation de faiblesse physique, psychologique et intellectuelle, qui désigne les cibles privilégiées. Aux plus jeunes et aux aînés viennent ainsi s'ajouter les personnes désocialisées ou isolées, les populations les plus défavorisées, handicapées et les moins réceptives.

Les mesures concernent l'encadrement juridique des activités les plus sensibles et les exigences de sécurité, par diverses sources de pressions, y compris les assurances. Ceci favoriserait la mise en œuvre de mesures de sécurité cohérentes, fondées sur l'application des politiques et des normes de sécurité, et sur la certification, sous condition de garantie de suivi et de contrôle interne dans la durée. L'unanimité se fait sur le développement primordial des formations et des sensibilisations, avec un consensus sur les insuffisances, et sur la nécessité d'intégration dans les cursus éducatifs. Les formations de haut niveau devraient se généraliser dans la prochaine décennie en s'appuyant sur des projets pilotes, et sur le livre blanc sur la sécurité et la défense nationale pour protéger les infrastructures vitales. Au-delà de la posture défensive il est souhaité une réflexion sur la dissuasion et le développement de

la lutte offensive. Les mesures organisationnelles sont mises en avant au niveau étatique, tandis que les mesures législatives et techniques font plus débat. Le partenariat public-privé semble prometteur, tout comme l'existence de centres d'expertise et de réponse aux incidents, sans oublier la faveur d'une réponse citoyenne avec un rôle actif dans le dispositif de vigilance. Les grandes entreprises et les secteurs les plus sensibles devraient être à l'avant-garde, suivis par les PME/PMI, plus hésitantes à mettre en place une stratégie adéquate. Enfin, l'établissement d'un cadre juridique universel reste un élément clé, avec l'harmonisation des dispositifs et des coopérations, aux niveaux international et public-privé.

Annexe 1 : METHODOLOGIE

Il s'agit d'appliquer ***la méthode Delphi*** *de façon à mettre en évidence la* ***convergence d'opinions****, et atteindre un certain degré de consensus, et tenter d'être éclairé au mieux sur* ***l'évolution de la cybercriminalité sur une période à venir de 10 années*** *: 2011- 2020*

Delphi[64] **a été appliquée** en faisant participer un **panel d'experts francophones**, d'origine différente distinguant plusieurs catégories : cyber-enquêteurs, experts en sécurité des systèmes d'information, et autres spécialistes : ***avocats, magistrats, etc.,*** lesquels ont répondu de façon indépendante à un **questionnaire** pour former leur jugement en plusieurs tours, au cours desquels chacun a été invité à reprendre ou reformuler son opinion, à la lumière des **réponses maintenues anonymes pour éviter un effet de leadership**. Ce processus itératif a pour but de réduire la dispersion des réponses, et de préciser l'opinion médiane. Ceci a généralement permis de dégager un consensus, mais aussi d'obtenir une information plus riche et abondante. **Le recours systématique de la voie électronique** a pour effet de faciliter les échanges et de réduire les coûts et temps de correspondances.

Phases de la méthode DELPHI

1.- La phase préparatoire comporte deux parties

- **Le choix des experts**, en fonction de la compétence, de l'expérience, mais aussi de la capacité de prévision, et de leur indépendance, pour disposer d'un panel final de 20 à 30 personnes qui se sont formellement engagées,
- **L'élaboration d'un questionnaire**, avec des questions précises mais ouvertes, si possible quantifiables et indépendantes.

2.- La phase de déroulement fait appel à trois tours

- **Au cours du 1er tour**, le questionnaire est transmis aux experts en précisant l'objet de la méthode, les conditions pratiques du déroulement, le délai de réponse, l'anonymat, etc. Chaque expert explicite sa réponse en évaluant son propre niveau d'expertise relativement à chaque question.
- **Au cours du 2ème tour**, chaque expert se voit présenter les réponses anonymes produites sous forme synthétisée et doit valider, préciser ou encore modifier sa réponse précédente. Il aura à justifier son opinion si elle est fortement distante de celle des autres, en estimant sa capacité de jugement à chaque question.
- **Au cours du 3ème tour**, chaque expert est appelé à commenter les arguments déviants, et à donner sa réponse définitive, au vu d'une opinion consensuelle médiane, voire de la dispersion des opinions.

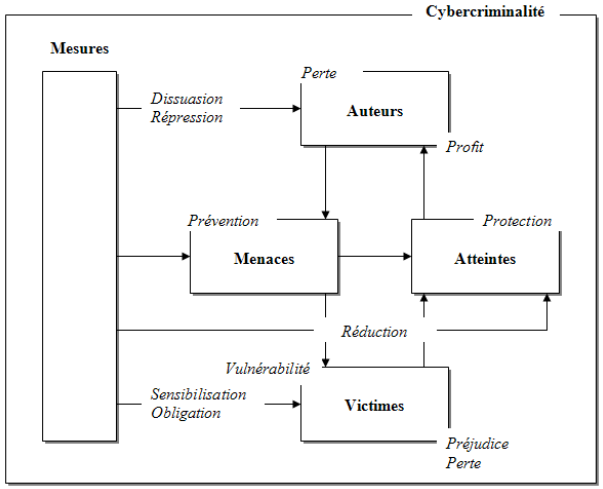
3.- La phase finale

- **Dépouillement et exploitation** finals de l'étude,
- **Reprise des synthèses et mise en forme** en vue de diffusion,
- **Diffusion** de la présente étude finalisée.

[64] Voir également Rosé P. (1992), pp. 30-32.

Modèle thématique fondateur du questionnaire

Pour élaborer le questionnaire en préservant au maximum l'indépendance des questions entre elles, ces dernières ont été fondées sur un modèle thématique présenté sur le schéma suivant avec les entités relatives, leurs relations, et quelques attributs :



Ceci a permis de **déterminer les questions autour des cinq thèmes** retenus suivants :

- **les menaces** qui relèvent de l'enlèvement, de la destruction, de la perturbation, de l'interruption, de la modification, de la divulgation, de l'interception, dégradation d'image,
- **les atteintes** qui relèvent des infrastructures, matériels, logiciels, données, réputation,
- **les auteurs** d'actes délictueux cybercriminels,
- **les victimes** qui, du fait de vulnérabilités, subissent des préjudices par l'application de menaces qui mènent à des atteintes,
- **les mesures** qui visent à réduire la cybercriminalité : législatives, politiques, techniques, organisationnelles, humaines, *dont coopération et coercition*.

Quatre questions par thème ont été arrêtées sous l'égide du comité scientifique, auxquelles ont été ajoutées trois questions générales sur la cybercriminalité et son évolution, en début.

Annexe 2 : ORGANISATION

L'étude s'est organisée autour d'un comité scientifique et d'un comité de rédaction de synthèse pour le montage et la coordination des actions à mener avec les experts.

Comité scientifique de l'étude

Ce comité a en charge la validation de la méthode proposée, selon un calendrier, la recherche des experts, et la communication et la collecte des documents.

- **Lieutenant-colonel Eric FREYSSINET**, chef de la Division de lutte contre la cybercriminalité, Service technique de recherches judiciaires et de documentation, Pôle judiciaire de la Gendarmerie nationale.
- **M Daniel GUINIER**, *docteur ès sciences, CISSP, ISSAP, ISSMP, MBCI,* expert près la Cour Pénale Internationale de La Haye, lieutenant-colonel (RC) de la gendarmerie nationale.
- **M Philippe ROSE**, *docteur ès sciences économiques,* journaliste et écrivain, rédacteur en chef de la revue Best Practices Systèmes d'Information.
- **Lieutenant-colonel Dominique SCHOENHER**, référent intelligence et sécurité économiques de la Région de gendarmerie Nord-Pas-de-Calais[65].

Comité de rédaction de synthèse

Ce comité a en charge de rédiger les différences synthèses en vue d'élaborer un document final, à partir des questionnaires retournés par les experts.

- **M Daniel GUINIER**[66], *docteur ès sciences, CISSP, ISSAP, ISSMP, MBCI,* expert près la Cour Pénale Internationale de La Haye, lieutenant-colonel (RC) de la gendarmerie nationale.
- **M Philippe ROSE**, *docteur ès sciences économiques,* journaliste et écrivain, rédacteur en chef de la revue Best Practices Systèmes d'Information.
- **Lieutenant-colonel Dominique SCHOENHER**, référent intelligence et sécurité économiques de la Région de gendarmerie Nord-Pas-de-Calais.

Experts ayant participé à l'étude

Les experts se sont formellement engagés à participer à l'étude. Ils ont en charge de renvoyer leurs réponses au questionnaire dans les délais requis, au cours des trois tours.

- **M Laurent BOUNAMEAU**, Federal Computer Crime Unit, Police fédérale belge.
- **Mme Sylvia BREGER**, criminologue, directrice de CRIMINONET.
- **M Alain CORPEL**, enseignant-chercheur SSI à l'Université technologique de Troyes (UTT).
- **Mme Chantal CUTAJAR**, professeur affilié à l'Ecole de management de l'Université de Strasbourg, directrice du GRASCO et du Master : Lutte contre la criminalité organisée économique et financière, lieutenant-colonel (RC) de la gendarmerie nationale.

[65] Dont le service était en charge de la diffusion anonyme des réponses au comité pour la synthèse.
[66] En charge aussi d'élaborer le document final dans sa forme à soumettre au comité *ad hoc*.

- **Lieutenant-colonel Eric FREYSSINET**, chef de la Division de lutte contre la cybercriminalité, Service technique de recherches judiciaires et de documentation, Pôle judiciaire de la Gendarmerie nationale.
- **M Gérard GAUDIN**, ingénieur Supélec, fondateur de l'association R2GS, consultant en gestion de la sécurité.
- **M Daniel GUINIER**, *docteur ès sciences, CISSP, ISSAP, ISSMP, MBCI,* expert près la Cour Pénale Internationale de La Haye, lieutenant-colonel (RC) de la gendarmerie nationale.
- **M Joseph ILLAND**, ingénieur général de l'armement, fonctionnaire de sécurité de défense du CNRS.
- **Adjudant-chef Thierry JACQUOT**, enquêteur NTECH, BDRIJ de Strasbourg.
- **M Philippe JOLIOT**, *ingénieur,* expert judiciaire près la Cour d'appel de Nancy, TRACIP, président de l'AFSIN.
- **M Denis LANGLOIS**, *ingénieur,* cryptologue, consultant en sécurité et sûreté des patrimoines matériel et informationnel.
- **M Bertrand LATHOUD**, Information Risk Manager PayPal.
- **Capitaine Olivier NAEL**, chef de la section technique, OCLCTIC.
- **M Jean-François PACAULT**, ingénieur général de l'Armement, chef du service de la sécurité des technologies de l'information et de la communication chez le Haut fonctionnaire de défense et de sécurité des ministères de l'Economie et du Budget.
- **M François PAGET**, secrétaire général du CLUSIF, chercheur en cybercriminalité, membre fondateur de McAfee Labs.
- **Lieutenant-colonel Alain PERMINGEAT**, chef de la division de lutte contre la cybercriminalité du service technique de recherches judiciaires et de documentation.
- **M Jean-Paul PINTE,** *docteur en information scientifique et technique*, maître de conférences, expert en veille et intelligence compétitive à l'Université catholique de Lille, lieutenant-colonel (RC) de la gendarmerie nationale.
- **Me Blandine POIDEVIN**, avocate au barreau de Lille.
- **Mme Myriam QUEMENER**, magistrate au parquet général de la Cour d'appel de Versailles.
- **M Philippe ROSE,** *docteur ès sciences économiques,* journaliste et écrivain, rédacteur en chef de la revue Best Practices Systèmes d'Information.
- **Mme Isabelle TISSERAND,** *docteur de l'EHESS,* coordinatrice du Cercle européen de la sécurité des systèmes d'information.
- **Adjudant-chef Franck VAN DE VELDE**, enquêteur NTECH, BDRIJ de Villeneuve d'Ascq.

Annexe 3 : QUESTIONNAIRE

Questions générales sur la cybercriminalité et son évolution

Q01 : Comment pourrait-on redéfinir ou préciser les domaines d'activités illicites et redéfinir le terme *"cybercriminalité"* pour la prochaine décennie ?

Q02 : Quelle sera la place de la cybercriminalité et ses rapports avec les autres formes de crimes et délits : *contrefaçons, délinquance financière et économique, pédopornographie, trafics de stupéfiants et d'êtres humains, terrorisme, etc.* ?

Q03 : Quel sera l'impact global des évolutions et ruptures technologiques : *informatique en nuages et virtualité, systèmes mobiles, cryptologie, stéganographie, codes malveillants, etc.,* sur la maîtrise ou au contraire la montée de ce phénomène ?

Questions organisées par thème

Thème 1 : Les menaces

Q11 : Quelles sont les menaces émergentes et les nouvelles formes attendues et leur niveau de sophistication ?

Q12 : Quelles seront les menaces les plus graves qu'auront à affronter les organismes : entreprises, collectivités, administrations, etc. ? *trois menaces par catégorie d'organisme*

Q13 : Quelle sera l'évolution des menaces à l'encontre des biens et informations personnels ?

Q14 : Quelle sera l'évolution de la répartition des menaces à l'encontre de la confidentialité, de l'intégrité, de la disponibilité et de l'imputabilité ? *informations et systèmes*

Thème 2 : Les atteintes

Q21: Quelle sera l'évolution de la répartition des atteintes en nombre et en gravité au vu des infractions : fraude, interception, vol de données et de propriété intellectuelle, usurpation d'identité, pédopornographie, e-réputation, etc. ? *en distinguant les individus et les organismes publics et privés ; préciser notamment si les atteintes aux infrastructures critiques : télécoms, réseaux d'énergie, etc. peuvent devenir un risque majeur ?*

Q22 : Quels seront les facteurs aggravants : dépendance, crises, mobilité et nomadisme, dispersion en *"nuages"*, etc. ?

Q23 : Quel sera le but prépondérant recherché : pertes ou gains financiers, atteinte à la vie privée, déstabilisation, désorganisation, désinformation, destruction, terreur, etc. ?

Q24 : La stabilité des États pourrait-t-elle être compromise ?

Thème 3 : Les auteurs

Q31 : Quelle sera l'évolution de l'origine des menaces : interne, externe et mixte ? *et en donner la répartition en % de 2010, 2015 et 2020*

Q32 : Quelle sera l'évolution des profils et la répartition des agents menaçants par catégorie : *"hackers"* indépendants, groupes sociaux, activistes, groupements criminels organisés, terroristes, États, etc. ?

Q33 : Quelle sera l'évolution des niveaux de compétences et des moyens nécessaires aux actes plus ou moins graves et de plus ou moins grande envergure ?

Q34 : Quelle sera l'évolution de la place du crime organisé ? *Sera t-il un acteur majeur ou non ? Pourquoi ? Avec quelles stratégies ?*

Thème 4 : Les victimes

Q41 : Quels secteurs socio-économiques seront les plus ciblés : finances et transactions en ligne, industrie et transports, énergie et défense, informatique et télécommunications, fourniture de services, agro-alimentaire, santé, recherche, État et territoires, etc. ?

Q42 : Quel sera l'évolution du comportement des victimes : signalement et dépôt de plainte, mesures de protection, etc. ? *en distinguant les individus et les organismes.*

Q43 : Quels seront les facteurs aptes à faire changer le comportement des futures victimes ? *informations, obligations, pertes non indemnisées, etc.*

Q44 : Quelle sera l'évolution de la répartition des tranches d'âge les plus touchées concernant les particuliers ? *personnes physiques.*

Thème 5 : Les mesures

Q51 : Quelle sera la tendance des entreprises à appliquer les normes de sécurité et à faire contrôler la mise en œuvre des mesures et procédures correspondantes ? *par catégorie d'entreprise et par secteur socio-économique.*

Q52 : Quelles seront les voies suivies pour adapter le schéma actuel de nos institutions et celui de la formation initiale et continue pour faire face au phénomène dans sa diversité ? *du risque ordinaire à la cyberguerre.*

Q53 : Quelles seront les mesures : législatives, politiques, techniques, organisationnelles, et humaines les plus promptes à réduire le phénomène ? *en distinguant les particuliers et les organismes.*

Q54 : Quels partenariats seront développés aux niveaux national, européen et international, et les coopérations : *public-privé, citoyenne, judiciaire, etc.*

GLOSSAIRE

Attaque informatique : Terme générique désignant une action malveillante dont la cible ou le moyen est l'informatique.
Botnet : Réseau de robots ("bots") malveillants, installés sur des machines compromises ("zombies"), en nombre pour assurer un camouflage actif et diriger des actions sur une ou plusieurs cibles déterminées *(ex. deni de service distribué (DDoS) ou envois massifs de pourriels ("spams")*.
CERT ("Computer emergency response team") : Equipe constituée pour signaler les vulnérabilités et menaces et répondre aux attaques.
Confidentialité : Propriété de la sécurité attachée au maintien d'un secret, avec accès aux seules entités autorisées.
Contrôleur de "botnet" ("bot herder") : Personne en charge du contrôle et du pilotage à distance d'un réseau de robots au travers d'un serveur C&C de Contrôle et Communication.
Cheval de Troie : Code malveillant dissimulé qui permet de prendre le contrôle de l'ordinateur compromis à l'insu de l'utilisateur légitime.
Informatique en nuages ("Cloud computing") : Mode de traitement des données d'un client, dont l'exploitation s'effectue par l'Internet, sous la forme de services fournis par un prestataire. Il s'agit en fait d'un modèle d'informatique dématérialisée permettant l'accès, via un réseau et sur demande, à un ensemble partagé de ressources configurables : *réseaux, serveurs, stockage, applications, etc.*, réparties *"en nuages"* en divers lieux géographiques, alors que l'emplacement et le fonctionnement du nuage sont peu ou pas portés à la connaissance des clients.
Code malveillant ("malware") : Programme développé dans le but de nuire au travers d'un système informatique ou d'un réseau ; *chevaux de Troie, virus et vers sont des codes malveillants caractérisés par la présence de mécanismes de propagation, de déclenchement et d'action, souvent développés dans l'intention de nuire.*
Cyberattaque : Acte malveillant envers un dispositif informatique, généralement via un réseau de télécommunications.
Cybermenace : Action menaçante locale ou à distance visant l'information ou des systèmes d'information.
Déni de service ("Deny of Service" ou DoS) : Action d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.
Déni de service distribué ("Distributed Deny of Service" ou D-Dos) : Action lancée depuis plusieurs sources, notamment par le biais d'un "botnet".
Diffamation : Allégation ou imputation de mauvaise foi, d'un fait qui porte atteinte à l'honneur, à la considération ou la réputation de la personne physique ou morale à laquelle il est imputé.
Disponibilité : Propriété de la sécurité attachée à la bonne délivrance dans les conditions définies d'horaires, de délais et de performance.
Filoutage ou **hameçonnage** ("phishing") : Technique trompeuse visant à obtenir des renseignements personnels en abusant les détenteurs.
Fraude : Acte illicite délibéré réalisé par des moyens plus ou moins subtils, avec la volonté de tromper dans le but de s'approprier un avantage. Elle peut prendre diverses formes qui nécessitent ou non des complicités, et conduit à un préjudice pour la victime.
Ingénierie Sociale ("social engineering") : Méthode visant à obtenir un bien ou une information en exploitant la confiance, l'ignorance ou la crédulité, ou par pression psychologique ou faisant appel à la compassion.
Imputabilité : Propriété de la sécurité attachée au suivi des opérations ou de fonctions réalisées, sans répudiation possible.
Intégrité : Propriété de la sécurité attachée au maintien des données et des composants sans corruption, dans l'espace et le temps.
Intrusion : Introduction et maintien à caractère frauduleux dans un système, en vue de récupération ou de modification, sinon d'altération ou de destruction.
Machine piratée ou "**zombie**" : Machine compromise par un robot malveillant ("bot"), - incluse dans un réseau ("botnet") dirigé par un "bot herder"-.
Pirate informatique ("hacker"): Individu s'introduisant dans un système informatique, par défi intellectuel ou avec intention malveillante ou pour le profit ; *agissant seul ou en groupe.*
Pourriels *("spams")* : Courriers électroniques souvent envoyés en nombre et non sollicités par les destinataires.
TIC : Acronyme pour désigner les technologies de l'information et de la communication.
Usurpation d'adresse ("address spoofing") : Action de substituer délibérément une adresse par une autre : adresse physique MAC (Medium Access Control), adresse IP, adresse de domaine ou de messagerie, etc. ; *de façon similaire à l'usurpation d'identité, qualifiée en délit en droit pénal français.*
Usurpation d'identité : Emprunt temporaire ou définitif de l'identité d'une personne, par appropriation des identifiants de cette dernière. La loi Loppsi 2, prévoit le délit d'usurpation d'identité, *numérique ou non*, puni d'une peine de 2 ans d'emprisonnement et d'une amende de 20 000 euros.

Voir également : www.clusif.asso.fr/fr/production/glossaire/

Dépôt légal en cours