Centre
international
pour la
prévention
de la criminalité

International
Centre
for the
Prevention
of Crime

Centro
Internacional
para la
Prevención
de la Criminalidad

6e Rapport international

PRÉVENTION DE LA CRIMINALITÉ ET SÉCURITÉ QUOTIDIENNE :

prévenir la cybercriminalité


PASSWORD

6e RAPPORT INTERNATIONAL SUR LA PRÉVENTION DE LA CRIMINALITÉ ET LA SÉCURITÉ QUOTIDIENNE : prévenir la cybercriminalité

ISBN :
- Imprimé : 978-2-921916-98-1
- PDF : 978-2-921916-99-8
- Clé USB : 978-2-924939-00-0

Publié par :
Centre international pour la prévention de la criminalité
465, rue Saint-Jean, bureau 803 Montréal (Québec) Canada H2Y 2R6
Téléphone : +1 514 288-6731 / Courriel : cipc@cipc-icpc.org

Ce Rapport est disponible en versions anglaise, française et espagnole sur le site: **www.cipc-icpc.org.**

Clause de non-responsabilité :
Le contenu éditorial de la présente édition du Rapport international sur la prévention de la criminalité et la sécurité quotidienne présente les perspectives et les conclusions des auteurs mais pas nécessairement celles des commanditaires ou des personnes qui ont offert leur soutien ou qui ont été consultées dans le cadre de la préparation de ce document.

Dans ce document, le genre masculin est utilisé comme générique, dans le seul but de ne pas alourdir le texte.

Situé à Montréal, au Canada, le Centre international pour la prévention de la criminalité (CIPC) est le plus important organisme international de prévention de la criminalité. Depuis plus de vingt ans, le CIPC a pour mission de promouvoir l'adoption de normes internationales axées sur la prévention de la criminalité et la justice pénale dans le but de renforcer la sécurité quotidienne et d'améliorer la qualité de vie pour tous. Le CIPC travaille avec les États membres, les organisations internationales et régionales et les autorités à tous les échelons gouvernementaux, et il maintient une présence active dans les Amériques, en Europe, en Afrique et en Océanie. Le CIPC met à la disposition des intervenants une vaste panoplie de connaissances sur le thème de la prévention de la criminalité, ainsi que sur les politiques, pratiques et outils connexes visant à réduire les facteurs de risque associés à la criminalité, à la violence et à l'insécurité.

Cette publication a été principalement financée par le ministère de la Sécurité publique du Canada.

Équipe de rédaction et de production : la sixième édition du Rapport international sur la prévention de la criminalité et la sécurité quotidienne a été rédigée sous la direction de Ann Champoux, Directrice générale du CIPC.

Rédacteur en chef : Pablo Madriaza Ph. D

Recherchistes : Pablo Madriaza Ph. D, Ariane de Palacio Ph. D, Anne-Sophie Ponsot, Pier-Alexandre Lemaire, Cateline Autixier, Sophie Maury

Assistants de recherche : Laura Gonzalez, Ana Orrego, Juliette Sigwalt, Frédérique Bisaillon-Gauthier, Héloïse Brun, Nelly Morin

Directrice de la production : Anne Onana

Le présent Rapport est également le fruit de la collaboration de toute l'équipe du CIPC, composée entre autres de Kassa Bourne.

REMERCIEMENTS

La rédaction d'un tel ouvrage représente une quantité de travail considérable. La réalisation de ce Rapport international a été rendue possible grâce à la généreuse participation de nombreuses personnes. Nous tenons à adresser nos plus sincères remerciements à tous ceux et celles qui ont contribué à cette publication, en particulier à toute l'équipe du CIPC et aux membres de notre Conseil d'administration (2017–2018) pour leur soutien :

- Maître Chantal Bernier, Présidente
- Professeur Peter Homel, Vice-président, Griffith Criminology Institute, Griffith University, Australie
- Monsieur Paul Girard, trésorier
- Docteur Vincenzo Castelli, Administrateur, Onlus Nova Consorzio per l'innovazione sociale
- Docteur Adam Tomison, Administrateur, Australian Institute of Criminology
- Madame Anie Samson, Administratrice, Montréal
- Madame Kalpana Viswanath, Administratrice, membre du comité d'orientation du Réseau mondial pour des villes plus sûres - ONU-Habitat, et du conseil d'administration du Centre international pour la prévention de la criminalité (CIPC)
- Docteure Tina Silbernagl, Administratrice, directrice de programmes - GIZ Inclusive Violence and Crime Prevention for Safe Public Spaces (VCP) programme
- Monsieur Claude A. Sarrazin, Administrateur, SIRCO

Nous tenons également à transmettre nos plus sincères remerciements à nos membres ainsi qu'à nos partenaires qui nous ont conseillés sur le choix des thèmes à aborder et qui ont été d'un apport remarquable et d'un soutien précieux. Cette fois, l'échéancier ne nous a pas permis de tenir des rencontres rédactionnelles en personne. Nous espérons toutefois que les membres du Conseil d'administration, nos membres, nos partenaires et les membres du comité scientifique n'estimeront pas que leur point de vue a été mal interprété. Nous sommes seuls responsables des erreurs éventuelles. Le comité scientifique se compose des personnes suivantes :

- Monsieur Kauko Aromaa, directeur, European Institute for Crime Prevention and Control (HEUNI), Finlande
- Docteure Elena Azaola, Centro de Investigaciones y Estudios Superiores en Antropología Social, Mexique
- Docteur Benoit Dupont, Université de Montréal, Canada
- Monsieur Peter Homel, Australian Institute of Criminology (AIC) and Asia Pacific Centre for the Prevention of Crime (APCPC) Australie
- Docteur Tim Hope, University of Salford, Royaume-Uni
- Docteur Azzedine Rakkah, Centre d'Études et de Recherches Internationales (CERI), France
- Docteure Elrena van der Spuy, Université de Cape Town, Afrique du Sud
- Docteure Anne Wyvekens, Centre National de la Recherche Scientifique, France

Nous tenons également à remercier les auteurs du Rapport dont la connaissance et l'expertise ont permis d'enrichir cette édition, notamment Alex Kigerl, Anna Sarri, Belisario Contreras, Benoit Dupont, Cécile Doutriaux, Carabineros de Chile, Dimitra Liveri, Eleni Darra, Jeff Hearn, Jérôme Barlatier, Judith Germano, Karuppannan Jaishankar, Kerry-Ann Barrett, Matthew Hall et Nabi Youla Doumbia.

Nous avons obtenu les conseils avisés de plusieurs autres experts qui nous ont également apporté un soutien très précieux, notamment les personnes et organismes suivants : Dr Jacqueline Karn de Economic and Social Research Council, Royaume-Uni ; Bernardo Perez, consultant auprès de ONU-Habitat ; Daniel Ventre et Anne Wyvekens du CNRS, France ; Ehren Edwards et Patrick Hénault de Sécurité publique Canada ; Matti Joutsen, Anni Lietonen, Inka Liljia et Natalia Ollus de HEUNI, Finlande ; Elena Azaola de Centro de Investigaciones y Estudios Superiores en Antropología Social, Mexique ; Katharina Peschke, Johannes de Haan, Nail Walsh et Anika Holterhof d'ONUDC, Autriche.

Enfin, de nombreux intervenants, chercheurs et décideurs ont également apporté leur précieuse collaboration à ce Rapport. Il nous est impossible de tous les citer nommément, mais nous les remercions chaleureusement.

MESSAGE DE LA PRÉSIDENTE DU CIPC

Malgré de nombreuses variations au sein des pays, nous constatons depuis l'année 2003 que le taux de la criminalité dite traditionnelle n'a pas cessé de diminuer de manière globale. Pourtant, si l'on considère l'évolution de la cybercriminalité au cours de dernières années, force est de constater que cette dernière n'a pas cessé d'augmenter.

Le 6e Rapport international sur la prévention de la criminalité et la sécurité quotidienne a ainsi pour trame de fond la prévention de la cybercriminalité. La hausse des attaques cybercriminelles, l'incidence de cette nouvelle forme de criminalité au quotidien et l'augmentation des coûts associés à la cybercriminalité dans les différents pays témoignent de la nécessité de développer de nouvelles méthodes et outils de prévention.

Ce Rapport se veut porteur de réflexions, stratégies et initiatives en la matière en offrant aux professionnels du milieu ainsi qu'aux institutions gouvernementales et non-gouvernementales une source de données probantes sur l'état de la cybercriminalité dans le monde et les efforts de prévention pertinents.

Le 6e Rapport international est le résultat d'un travail d'équipe soutenu et n'aurait pu voir le jour sans la contribution du personnel et des membres du CIPC, mais également de nos partenaires universitaires et institutionnels qui ont su, une fois de plus, nous apporter conseil, soutien et contenu. Je veux également reconnaitre la contribution centrale du gouvernement du Canada grâce à qui nous bénéficierons tous des enseignements de ce Rapport.

J'espère que vous trouverez dans ce Rapport les données et l'analyse en appui à vos propres efforts dans la prévention de la cybercriminalité.

Chantal Bernier
Présidente, CIPC

MESSAGE DE LA DIRECTRICE GÉNÉRALE DU CIPC

En tant que nouvelle Directrice générale du Centre international pour la prévention de la criminalité (CIPC), j'ai eu l'immense honneur de coordonner et de superviser la préparation et la publication du 6e Rapport international sur la prévention de la criminalité et la sécurité quotidienne. Le thème central de cette 6e édition est bien entendu la prévention de la cybercriminalité.

Impliqué depuis près de 24 ans dans la prévention de la criminalité et la sécurité, le CIPC a pour mission de promouvoir la prévention de la criminalité, et apporter soutien et assistance aux collectivités, aux municipalités, aux régions et aux pays du monde entier.

Dans un monde toujours plus axé sur la mise en commun d'expertise et de politiques probantes en matière de prévention de la criminalité et avec l'émergence du cyberespace au cours de ces dernières années, il est d'autant plus important de considérer les nouvelles formes de criminalité qui apparaissent et de réfléchir sur les outils et les méthodes de prévention pour pallier au phénomène de la cybercriminalité qui ressort de plus en plus comme une problématique centrale au niveau mondial. Comment prévenir la cybercriminalité et peut-ont établir un ensemble de normes ou de modèles de prévention en la matière ?

Nous avons voulu répondre à ces questions, dans le cadre de notre mandat, au moyen de ce Rapport international axé principalement sur la question de la prévention de la cybercriminalité. Chaque chapitre de cette 6e édition aborde ainsi une dimension de cette prévention. Comme cela a été le cas pour les éditions précédentes, le premier chapitre présente de manière générale les dernières tendances en matière de prévention de la criminalité. Le deuxième chapitre quant à lui aborde le problème de la cybercriminalité et pose les bases pour les chapitres suivants. Le troisième chapitre dresse un portrait sur les cybercrimes, ainsi que les profils des cybercriminels et des cybervictimes. Le quatrième chapitre aborde la notion de prévention de la cybercriminalité et présente les lacunes et les approches dans le contexte actuel. Enfin, le cinquième chapitre présente les partenariats public-privé face à la prévention de la cybercriminalité.

Je suis très fière de ce Rapport, qui est le résultat d'un travail d'équipe et de collaboration. Je tiens à remercier toute l'équipe du CIPC et tous nos collaborateurs pour ce produit de qualité. J'espère qu'il saura vous apporter les informations et les outils pour prévenir la cybercriminalité et mettre en œuvre des stratégies et des initiatives probantes en la matière.

Ann Champoux
Directrice générale, CIPC

TABLE DES MATIÈRES

LISTE DES ACRONYMES ET DES ABRÉVIATIONS

A

ASEAN : Association des nations de l'Asie du Sud-Est

APSA : Architecture africaine de paix et de sécurité

B

BEC : Business Email Compromise

BID : Banque interaméricaine de développement

BSA : Business Software Alliance

C

CCJPC : Commission pour la prévention de la criminalité et la justice pénale

CCPPP : Conseil canadien pour les partenariats public-privé

CCSPJP : Conseil citoyen pour la sécurité publique et la justice pénale

CCSS : CARICOM Crime and Security Strategy

CERT : Centre d'études, de réponses et de traitement des incidents de sécurité du Brésil

CESAP : Commission économique et sociale pour l'Asie occidentale

CESNU : Conseil économique et social des Nations Unies

CIIP : Informations relatives à la protection des infrastructures critiques

CIPC : Centre international pour la prévention de la criminalité

CSIRT : Computer Security Incident Response Team

D

DARE : Programme de sensibilisation aux dangers de la drogue

E

ECSO : Organisation européenne pour la cybersécurité

ENISA : Agence européenne en charge de la sécurité des réseaux et de l'information

EP3R : Partenariat public privé européen pour la résilience

EUCPN : Réseau européen de prévention de la criminalité

EU IRU : Unité de signalement des contenus sur Internet

F

FBI : Bureau fédéral d'enquête

I

IC3 : Centre de plaintes pour les crimes sur l'Internet

ICMEC : Centre international pour les enfants disparus et exploités

IETI : Infrastructures essentielles de technologie de l'information

IQF : Interpeller, poser des questions ou fouiller

ISAC : Information Sharing and Analysis Center

L

LIBE : European Parliament's Committee on Civil Liberties, Justice and Home Affairs

LISTE DES ACRONYMES ET DES ABRÉVIATIONS

N

NIS : Sécurité des réseaux et des informations

O

OCDE : Organisation de coopération et de développement économiques

OEA : Organisation des États Américains

OIT : Organisation internationale du travail

OLAF : Office européen de lutte antifraude

OMS : Organisation mondiale de la santé

ONU : Nations Unies

ONUDC : Office des Nations Unies contre la drogue et le crime

ONU Femmes : Entité des Nations Unies pour l'égalité des sexes et l'autonomisation des femmes

P

PADO : Programme de dévouement intensif

PROMEVIL : Promotion des nouveaux métiers de la Ville

PSD : Département Paix et Sécurité

PSP : Partenariat national pour la sécurité publique

R

RGPD : Règlement général sur la protection des données

RSSI : Responsable de la sécurité des systèmes d'information

RTM : Modélisation des terrains à risque

T

TH : Taux d'homicide

U

UA : Union africaine

UE : Union européenne

UIT : Union internationale des télécommunications

UNGASS : Session Extraordinaire de l'Assemblée Générale des Nations Unies

UNICEF : Fonds des Nations unies pour l'enfance

V

VIH : Virus de l'immunodéficience humaine

VRN : Réseau pour la réduction de la violence

LISTE DES CONTRIBUTEURS

Alex Kigerl

Ph. D, Chercheur et professeur adjoint en justice pénale et criminologie, Washington State University
États-Unis

Anna Sarri

Équipe des Stratégies nationales de cybersécurité
Agence européenne chargée de la sécurité des réseaux et de l'information
Grèce

Belisario Contreras

Responsable de programme cybersecurité
Organisation des États Américains
États-Unis

Benoit Dupont

Professeur titulaire
Directeur scientifique du Réseau intégré sur la cybersécurité (SERENE-RISC)
Titulaire de la Chaire de recherche du Canada en sécurité, identité et technologie
Canada

Carabineros de Chile / Centre de modélisation mathématique de l'Université du Chili (CEAMOS)

Département d'analyse criminelle de Carabineros de Chile et Centre de modélisation mathématique de l'Université du Chili (CEAMOS)
Chili

Cécile Doutriaux

Avocate
Membre de la Chaire Cyberdéfense des écoles de Saint-Cyr
France

Dimitra Liveri

Équipe des Stratégies nationales de cybersécurité
Agence européenne chargée de la sécurité des réseaux et de l'information
Grèce

Eleni Darra

Équipe des Stratégies nationales de cyber sécurité
Agence européenne chargée de la sécurité des réseaux et de l'information
Grèce

ENISA

Agence européenne pour la cybersécurité
Grèce

Jeff Hearn

Professeur émérite, Hanken School of Economics
Finlande

Jérôme Barlatier

Chef d'escadron
Service central de renseignement criminel (SCRC)
France

Judith Germano

Chercheuse principale au NYU Center for Cybersecurity (CCS)
NYU Center on Law & Security (CLS)
Professeure adjointe au NYU School of Law
États-Unis

Karuppannan Jaishankar

Professeur
Raksha Shakti University (Police and Internal Security University)
International Journal of Cyber Criminology
International Journal of Criminal Justice Sciences
Inde

Kerry-Ann Barrett

Spécialiste en politique de cybersécurité
Organisation des États Américains
États-Unis

Matthew Hall

Ph. D, Chercheur à l'Université d'Ulster
Royaume-Uni

Nabi Youla Doumbia

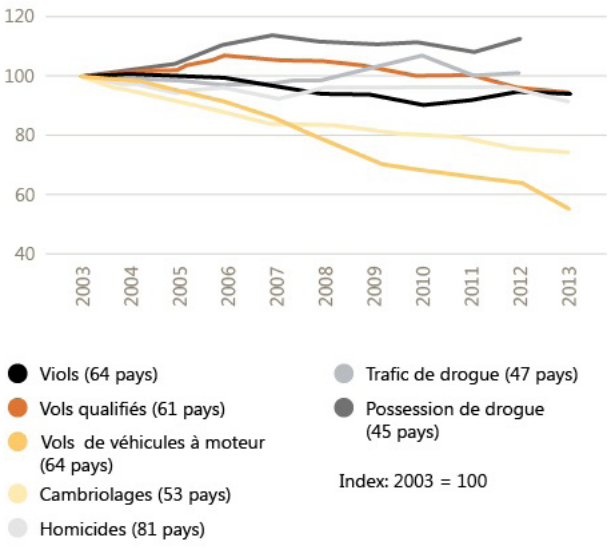
Ph.D en criminologie, Université de Montréal
Coordonnateur de recherche du projet Homicides en Afrique
Canada

INTRODUCTION ET SYNTHÈSE DES CONNAISSANCES

Il ressort des travaux menés dans le cadre de l'élaboration des deux derniers Rapports internationaux du CIPC (CIPC, 2014, 2016) qu'en dépit des énormes variations par région et par pays, le taux de crimes traditionnels, exceptés ceux liés aux stupéfiants, n'a pas cessé de reculer depuis 2003.

En revanche, l'importance du cyberespace n'a quant à elle pas cessé d'augmenter. Ce constat fait, nous nous sommes posé la question suivante : existe-t-il une relation entre la baisse des crimes traditionnels et l'importance croissante du cyberespace? Il semblerait que la diminution des crimes à l'échelle mondiale n'implique pas forcément une tendance vers la disparition de ce type de criminalité, mais plutôt une transformation de cette dernière, les crimes migrant ainsi vers le cyberespace. Cette hypothèse est toutefois difficile à prouver en raison du manque de connaissances sur le sujet. Comme nous allons le voir dans le chapitre 2, les données actuelles dépendent fortement des entreprises privées et de leur agenda économique. Les catégories utilisées pour définir un « crime » ou une « victime » sont larges, fort discutées, et dépendent exclusivement de l'information donnée par les clients. Les échantillons ne sont donc pas représentatifs de la réalité mondiale.

Graphique 1. **Tendances observées dans le monde pour certains crimes, 2003-2013**



Source: ONUDC (2015)

Bien que cette hypothèse semble difficile à prouver, il est impossible de nier l'importance du cyberespace sur la vie quotidienne et contemporaine des personnes, et particulièrement sur le crime. En effet, la cybercriminalité représente aujourd'hui bien plus qu'une simple problématique émergente, en s'imposant comme un enjeu majeur dans la plupart des pays du monde. Dans ce contexte, la prévention de la cybercriminalité devient un besoin immédiat. Est-il possible de prévenir la cybercriminalité ? Existe-t-il des modèles ou cadres de prévention à ce sujet ? Comme dans le cas de la criminalité traditionnelle ou d'autres phénomènes tels que la radicalisation menant à la violence, la prévention a été une réponse tardive à la cybercriminalité. La discussion a en effet davantage été axée sur la cybersécurité et l'empêchement que sur la prévention en tant que telle. En outre, la cybersécurité répond principalement plus aux enjeux de sécurité des entreprises privées et de l'infrastructure numérique que des personnes. En effet, malgré l'évidente difficulté à situer la cybercriminalité dans un espace géographique traditionnel et la tendance à accentuer les facteurs hors frontières, la plupart des victimes individuelles sont des personnes situées localement. Le défi majeur est donc d'identifier les mécanismes qui permettent d'une part de comprendre le processus de victimisation, et d'autre part, d'activer les meilleures stratégies de prévention à partir de l'interface entre un crime délocalisé et ses victimes locales. La question des victimes individuelles a évidemment été abordée dans le cadre de travaux scientifiques, et il existe à ce sujet des mesures précises de prévention. Cependant, celles-ci se concentrent essentiellement sur les comportements des victimes plutôt que sur les actions des malfaiteurs ou d'autres facteurs criminogènes. Cette approche de prévention est donc très embryonnaire.

Tous ces éléments nous ont conduits à la production d'un rapport international axé exclusivement sur la question de la prévention de la cybercriminalité, notamment afin d'identifier les lacunes en termes d'informations et d'approches de prévention. À la différence des autres rapports internationaux, où ont été abordées différentes problématiques autour d'une thématique spécifique, cette édition a été pensée comme un produit complet, chaque chapitre abordant une dimension particulière de la prévention de la cybercriminalité. Comme dans les versions précédentes, le premier d'entre eux effectue une mise à jour des tendances en matière de prévention de la criminalité en général. C'est donc le chapitre 2 qui introduit spécifiquement la thématique de la cybercriminalité et est considéré comme le chapitre cœur de ce rapport. En effet, le problème de la cybercriminalité y est contextualisé, ainsi que les principales thématiques abordées dans les chapitres suivants. Le chapitre 3 est quant à lui

consacré à la cybercriminologie, soit l'étude des cybercrimes, des cybercriminels et des cybervictimes. Le chapitre 4 se penche directement sur la prévention en tant que telle, et dans lequel seront présentées et discutées en profondeur les mesures mises en place et les lacunes d'informations. Enfin, le chapitre 5 aborde une dimension fondamentale de la gouvernance mondiale en matière en prévention de la cybercriminalité : les partenariats public-privés.

Rapport international sur la prévention de la criminalité et la sécurité quotidienne

Le Rapport international est le document phare du Centre International pour la Prévention de la Criminalité (CIPC). Tous les deux ans, le CIPC fait une révision exhaustive des nouvelles tendances en matière de prévention du crime, afin d'alimenter la réflexion et notamment la pratique et la politique publique à ce sujet. Depuis sa quatrième édition, le Rapport international, en plus d'analyser les tendances globales sur la prévention, se penche également sur une thématique spécifique afin de l'aborder plus en profondeur. Dans ce cas et comme nous l'avons vu, la thématique principale est la prévention de la cybercriminalité.

Tout comme les publications précédentes, cette édition considère la prévention sous plusieurs angles. Le point de départ demeure évidemment la recherche empirique sur le sujet, mais sous le parapluie de la prévention, il existe d'autres dimensions qui ont une influence majeure sur les efforts menés sur le terrain pour diminuer la victimisation et favoriser un contexte social plus sécuritaire. Il s'agit notamment des normes internationales, des stratégies nationales et des pratiques locales, qui doivent également être mises en avant. Ce rapport s'inspire ainsi notamment du travail des organismes des Nations Unies et régionaux, des pratiques efficaces et/ou prometteuses, de la réflexion et de la recherche académique. Tout comme le CIPC, il vise à favoriser un dialogue ouvert entre la recherche et la pratique, entre les chercheurs, les preneurs de décisions et les intervenants.

Ce rapport s'adresse ainsi principalement à trois secteurs clé : les décideurs et les élus politiques, dont la mission est de bâtir des sociétés plus sûres et plus inclusives, tant à l'échelle nationale, qu'étatique ou locale ; les praticiens ou les professionnels, dont le travail a un impact majeur dans l'établissement de collectivités plus sûres et saines, entre autres, les secteurs de la police et de la justice, les travailleurs sociaux ou de la santé, les professeurs, la société civile ou encore les organisations non-gouvernementales ; et le milieu de la recherche, incluant les universités et les instituts qui contribuent à renforcer la connaissance et les informations qui prouvent l'efficacité, les coûts et les bénéfices des politiques et des pratiques mises en place en matière de prévention.

L'information présentée dans ce rapport provient d'un large éventail de sources, entres autres, de rapports produits par les agences des Nations Unies, les institutions internationales ou régionales telles que la Banque mondiale, la Commission Européenne, l'Union Africaine, l'ASEAN ou l'Organisation des États Américains ; de gouvernements nationaux ou locaux, de rapports produits par des organisations non-gouvernementales, ainsi que de sources provenant de la recherche ou académiques. Comme toujours, le vaste réseau international du CIPC, composé de gouvernements et d'organisations membres intervenant dans le domaine de la prévention de la criminalité et de la sécurité quotidienne, reste une source privilégiée d'informations.

En 2016, a été publié le 5e Rapport international, dont l'enjeu principal était d'analyser le rôle des villes en matière de sécurité et de prévention de la criminalité (voir Encadré 1 pour le résumé des thèmes abordés dans les versions précédentes). Il avait également pour objectif de souligner l'importance de la Conférence des Nations Unies sur le logement et le développement urbain durable, Habitat III, qui s'est déroulée à Quito en octobre 2016. Avec ce rapport, il convenait de souligner le fait que dans bien des cas, les dynamiques et les caractéristiques urbaines ont une influence sur la criminalité et la violence, mais aussi que les facteurs urbains offrent une base en matière de prévention de la criminalité ainsi qu'un potentiel pour un développement favorable aux individus et aux communautés.

ENCADRÉ 1. **Rapports internationaux sur la prévention de la criminalité et la sécurité quotidienne : 2008 – 2016**

Les Rapports internationaux précédents ont examiné les tendances en matière de criminalité et d'insécurité, abordé des sujets et des thèmes ciblés, et fait le point sur les tendances en matière de prévention de la criminalité et de sécurité quotidienne.

Thèmes abordés :

2008 : sécurité des femmes, sécurité des jeunes, sécurité dans les écoles, sécurité dans les espaces publics

2010 : migration, crime organisé, drogues et alcool

2012 : trafic humain et exploitation, quartiers informels, zones de post-conflit et de post-catastrophe, production de drogues dans les pays développés

2014 : migration et déplacement des personnes à l'intérieur et à l'extérieur des frontières

2016 : les villes et le Nouvel agenda urbain

Tendances en matière de prévention de la criminalité et sécurité quotidienne :

2008 : normes internationales en matière de prévention, réseaux d'échanges internationaux, stratégies

nationales et locales ; prévention fondée sur la connaissance ; le rôle des acteurs institutionnels notamment de la police et des acteurs judiciaires ; nouveaux services en soutien à la sécurité quotidienne (sécurité privée, médiation et résolution de conflits) ; élargir le rôle des gouvernements locaux et des acteurs communautaires

2010 : principales tendances en matière de prévention de la criminalité ; bonne gouvernance (décentralisation des pouvoirs, légitimité, réglementation de la sécurité privée, élargissement du rôle de la société civile) ; approches sociales et éducatives ; formation, perfectionnement professionnel et renforcement des capacités ; évaluation de la prévention de la criminalité

2012 : étude mondiale menée sur les stratégies de sécurité dans les villes et leurs composantes

2014 : migration autochtone, prévention de la traite des personnes, violence faite aux femmes dans les relations intimes

2016 : principales tendances en matière de la criminalité et de sa prévention, la sécurité urbaine, territoire et politiques de sécurité publique à partir perspective latino-américaine, les transports publics et la prévention, la consommation de drogues dans un contexte urbain et la radicalisation menant à la violence dans les villes.

Thèmes abordés

Chapitre 1 : Tendances en matière de criminalité et de prévention de la criminalité

Ce premier chapitre cherche à présenter les grandes tendances en ce qui concerne les chiffres sur la délinquance ainsi que les efforts menés à une échelle internationale afin de la prévenir. Il se divise en trois parties. La première partie concerne notamment les tendances internationales en matière de criminalité. Dans ce contexte, nous avons choisi sept thématiques à aborder : les homicides, les homicides de femmes, la violence envers les enfants et les jeunes, la violence dans les villes, les problématiques criminelles liées aux drogues, le taux d'incarcération et le sentiment d'insécurité. La deuxième partie se concentre sur les efforts récents des organismes internationaux et régionaux en matière de prévention de la criminalité, notamment par rapport aux Nations Unies. Enfin, la troisième partie est une description des dernières études empiriques sur le sujet. À ce titre a été réalisée une revue des documents scientifiques ayant analysé des données empiriques publiées entre 2015 et 2017. Celle-ci cherche à décrire l'information la plus récente en matière de prévention de la criminalité et ainsi, présenter un portrait réaliste des intérêts et des préoccupations de la recherche à ce sujet à l'échelle mondiale. Trois thématiques ont été analysées dans ce rapport : la recherche concernant l'approche communautaire et urbaine, le rôle de la police dans la prévention, notamment l'analyse criminelle et la relation entre les jeunes et la criminalité. Les constats les plus importants de ce chapitre sont les suivants :

- Bien que l'Amérique latine demeure la région au taux d'homicide le plus important au monde, cette violence se concentre dans certains pays de la région, dans certaines villes de ces pays et dans certains secteurs de ces villes. El Salvador et le Honduras sont les pays avec les taux d'homicide les plus élevés au niveau mondial tandis que le Brésil et le Mexique abritent la majorité des villes les plus violentes au monde. En moyenne par pays, 25 % du total des victimes d'homicides en 2015 étaient des femmes. Pour ce qui est de la violence contre les enfants et les jeunes, elle est pratiquement universelle, touchant autant les pays riches que les pays pauvres.
- L'analyse des initiatives des organismes internationaux met en avant l'importance de la coopération et de la coordination entre les pays et entre les régions du monde, liée notamment à un nombre limité de crimes tels que le crime organisé, le terrorisme, la cybercriminalité, le trafic d'êtres humains, les problématiques liées aux drogues, etc. Il a malheureusement été constaté que la plupart des initiatives de coopération ont davantage mis l'accent sur la justice pénale que sur la prévention.
- À partir de la revue de littérature, nous avons pu constater l'importance donnée aux initiatives communautaires et citoyennes de maintien de l'ordre, notamment dans des pays de l'Afrique et de l'Asie. Dans ce cas, ces groupes se focalisent sur la surveillance et le contrôle, en reproduisant ainsi un modèle de police traditionnel. Nous avons également constaté l'importance grandissante de l'analyse criminelle pour la prévention au niveau mondial, notamment au sein des polices et dans les pays d'Amérique du Sud. Enfin, des études récentes ont révélé que les actions de prévention et de réinsertion axées sur la punition, l'augmentation de peines et basées sur des approches agressives de la police ne sont pas efficaces pour prévenir la criminalité.

Chapitre 2 : Les crimes dans un monde numérique

Ce second chapitre tente une problématisation de notre approche des phénomènes de cybercriminalité et se divise en trois volets. Le premier volet ouvre la réflexion autour de la cybercriminalité en s'intéressant à l'environnement spécifique au sein duquel elle s'inscrit, le cyberespace : notamment les dimensions de gouvernance et de facteurs d'inégalités y sont examinées. Le second volet se penche quant à lui sur les difficultés de mesurer la cybercriminalité, des difficultés d'ordre structurel, méthodologique et conceptuel. Enfin, le troisième volet tente, à travers une

revue des données et des informations disponibles, d'établir un panorama mondial de la cybercriminalité.

Plusieurs éléments d'intérêt émergent de ce second chapitre :

- Le cybersepace forme un environnement très particulier, aux conditions et aux dynamiques spécifiques, dont plusieurs s'avèrent cruciales pour comprendre les phénomènes cybercriminels. Notamment, la gouvernance particulière du cyberespace décentre les responsabilités de sécurité, de protection, de lutte et de prévention de la criminalité, qui ne relèvent alors plus de l'exclusivité des autorités publiques. Ce « vide de gouvernance » de la sécurité de tous sur Internet constitue l'une des principales opportunités pour la cybercriminalité.
- Le cyberespace forme en outre un milieu différent du monde « réel » : ainsi, les facteurs et les conditions propres au monde « réel » ont une influence sur ceux du monde virtuel, sans pour autant être les mêmes. Ainsi, par exemple, les questions d'inégalités « macro » identifiées dans le monde « réel » (économiques, sociales, de développement, de genre, etc.) ont une influence sur la construction des inégalités virtuelles (d'accès, de compétences et d'usage), mais elles constituent deux systèmes d'inégalité différents.
- Les deux précédents points sont cruciaux dans notre compréhension des phénomènes cybercriminels et de cybervictimisation. En effet, on n'observe pas de corrélation directe entre les dynamiques cyber (criminels comme victimes) et les inégalités observées dans le monde réel ; ce sont des corrélations indirectes, déformées et complexifiées par le prisme du cyberespace. La recherche académique fait ainsi face à un grand défi : repenser les explications du crime dans le monde cyber.
- L'observation de ces activités cybercriminelles est ardue, d'une part en raison de leur grande hétérogénéité, et d'autre part à cause de leur rapide et constante évolution. Cependant, on peut souligner plusieurs aspects clés de cette sphère criminelle, tout particulièrement intéressants du point de vue qui nous intéresse, celui de leur prévention. Premièrement, l'état des connaissances actuelles sur les facteurs favorisant le développement de ces activités, ainsi que ceux favorisant la cybervictimisation, est très embryonnaire. Il apparaît, au regard du corpus très restreint des études sur le sujet, que des corrélations existent entre les facteurs classiques du monde dit « réel » (par exemple décrits dans l'approche écosystémique des facteurs de risque) et la cybercriminalité ; pour autant, ces corrélations semblent indirectes, obéissant à des processus et des articulations bien spécifiques, notamment transformées par la transition entre monde réel et cyberespace, ce dernier constituant alors un environnement aux conditions particulières.
- Enfin, on observe de grandes lacunes et une qualité très variable dans les données disponibles. Néanmoins, elles nous permettent de tirer quelques conclusions préliminaires, parmi lesquelles, notamment, une distribution différenciée dans l'espace des différents phénomènes cybercriminels, l'émergence de pôles géographiques de cybercriminalité caractérisés par des activités privilégiées et des modes de gouvernance particuliers.

Chapitre 3 : Cybercrimes, cyberdélinquants et cybervictimes

Ce troisième chapitre fait l'état des lieux de ce qui se fait aujourd'hui dans la recherche en criminologie sur la cybercriminalité. Qu'entend-on par cybercriminalité? Que sait-on sur les différents cybercrimes? Qui en sont les auteurs et qui en sont les victimes? Autant de questions que les criminologues se posent et pour lesquelles ils cherchent à voir si les théories criminologiques traditionnellement utilisées pour comprendre la délinquance et la victimisation nous sont utiles dans ce nouvel environnement qu'est le cyberespace ou bien s'il est aujourd'hui nécessaire de concevoir une nouvelle approche afin de mieux appréhender ce sujet. Après avoir regardé les différentes perspectives définitionnelles que nous livre la science ainsi que les principales théories appliquées pour comprendre les divers cybercrimes, nous allons par la suite chercher à mieux connaître les avancées de la criminologie sur trois phénomènes en particulier : le piratage informatique, la cyberfraude et les cyberviolences.

Plusieurs constats apparaissent après l'état des lieux qui est fait :

- La définition de la cybercriminalité est source de débat dans le milieu de la recherche. Les cybercrimes sont considérés tantôt comme « du vieux vin dans de nouvelles bouteilles», tantôt comme « du nouveau vin dans de nouvelles bouteilles » et tantôt comme « du vieux vin sans bouteilles ». Dès lors, chaque chercheur choisira une définition en fonction de ses intérêts de recherche faisant en sorte de créer des données très disparates et difficilement comparables.
- Le manque considérable de données sur les victimes individuelles est dû au fait que les personnes ne rapportent pas les faits aux instances compétentes soit par manque de connaissance sur le sujet, soit par crainte que rien ne soit fait du côté de la justice. Du côté des victimes collectives, le faible report est plutôt dû à la crainte de l'impact des cybercrimes sur leur réputation.
- Un profil unique de cybercriminel ou de cybervictimes ne peut absolument pas être développé. Il existe autant de profils qu'il existe de cybercrimes.
- Les théories criminologiques traditionnelles apportent quelques résultats, mais il reste encore beaucoup de travail à faire pour mieux appréhender la cybercriminalité. Les chercheurs se penchent d'ailleurs sur la création de nouvelles théories spécifiquement adaptées au cyberespace.

Chapitre 4 : Quelle prévention pour la cybecriminalité ?

Le cyberespace fait aujourd'hui l'objet d'une nouvelle discussion, tant théorique, que pratique, en matière de prévention de la criminalité. Plusieurs États utilisent les termes de cybersécurité et de cybercriminalité de façon interchangeable et dirigent leurs efforts vers la protection des infrastructures critiques de l'information, au détriment de la nécessaire réflexion entourant la prévention de la criminalité, dans le contexte du cyberespace. En commençant par bien différencier la cybersécurité et la cybercriminalité, tant au niveau conceptuel qu'opérationnel, ce quatrième chapitre a pour objectif de revoir les principaux développements quant aux approches traditionnelles de la prévention de la criminalité, qui sont les approches développementale, environnementale et partenariale, dans ce nouveau contexte. Enfin, il est aussi question d'analyser ces approches dans leur application, à l'aide de différentes mesures prises, dans l'objectif de prévenir certains des crimes les plus souvent cités dans les conventions internationales, soit la cyberintimidation, l'exploitation sexuelle des jeunes en ligne et la cyberfraude. Plusieurs éléments émergent de ce quatrième chapitre :

- Une coopération internationale et multiniveaux : compte tenu de la multitude de facteurs risque et du fait que la cybercriminalité n'est pas assujettie au concept de frontière, sa prévention nécessite une coopération internationale et multiniveaux, tant pour l'harmonisation des cadres légaux, que le partage d'information et de pratiques prometteuses.
- Une approche intégrée : lutter contre ces crimes demande une approche intégrée, menée par différents acteurs, tels le système de justice criminelle, la protection de la jeunesse, l'industrie des technologies de l'information, le milieu scolaire, le secteur de la santé et les services de police, dans une perspective de prévention développementale et environnementale.
- Développement de la connaissance : le développement d'initiatives en prévention de la criminalité nécessite une quantité d'information importante, notamment en ce qui a trait aux facteurs de risque propres à la problématique ciblée. Toutefois, la connaissance entourant les changements entraînés par l'utilisation d'internet, sur les facteurs de risque traditionnels reste encore embryonnaire.

Chapitre 5 : Les partenariats public-privé en prévention de la cybercriminalité

Ce cinquième et dernier chapitre aborde la question des partenariats public-privé en cybersécurité, et plus spécifiquement la manière dont ils abordent la prévention de la cybercriminalité. En guise d'introduction à la thématique, la première partie a pour objet de définir en quoi consiste un partenariat public-privé, pour ensuite s'attarder sur son émergence en prévention de la criminalité.

La seconde partie dresse un portrait des partenariats public-privé en prévention de la cybercriminalité. Une description des acteurs impliqués dans ces partenariats est présentée, suivie des approches de mise en œuvre et de développement des partenariats, ainsi que leurs composantes. La troisième partie présente un aperçu de partenariats public-privé internationaux et stratégies nationales axés sur la prévention de la cybercriminalité. La quatrième partie se rapporte aux principaux enjeux rencontrés dans le cadre de ces partenariats, et pour conclure la cinquième partie présente quelques recommandations.

Plusieurs constats peuvent être dégagés de ce chapitre :

- Tel que souligné précédemment dans ce rapport, le cyberespace suppose une gouvernance particulière, qui nécessiterait l'implication d'une diversité d'acteurs pour assumer des responsabilités traditionnellement attribuées au secteur public, telle que la gestion de la sécurité. Le secteur privé se voit ainsi graduellement considéré comme acteur indispensable à la cybersécurité, étant propriétaire des infrastructures qui peuvent non seulement être la cible de cyberattaques, mais qui peuvent également en faciliter la réalisation et la prévention. Cette indispensabilité est toutefois très peu contestée dans la littérature, et l'influence du secteur privé dans la production de connaissances à ce sujet peut soulever certains enjeux.
- Les mesures de prévention mises en œuvre dans le cadre de partenariats public-privé sont majoritairement de l'ordre de la prévention situationnelle, visant principalement la protection des infrastructures critiques. Bien que les connaissances en matière de facteurs explicatifs de la cybercriminalité et de la cybervictimisation demeurent très limitées, les ressources disponibles au sein de partenariats public-privé évoquent tout de même la possibilité que ces derniers puissent contribuer de manière importante à une prévention sociale de ces phénomènes. La mobilisation du secteur privé dans des initiatives de prévention dont les retombées ne sont pas immédiates est toutefois un défi important, comme le démontre l'expérience en prévention de la criminalité.
- Finalement, à certains égards, les enjeux rencontrés dans le cadre de partenariats public-privé en prévention de la cybercriminalité sont semblables à ceux de tout partenariat entre les secteurs public et privé. Une divergence en matière d'identités institutionnelles, d'intérêts, d'attentes et de valeurs perçues comme étant conflictuelles ne sont pas l'apanage du domaine de la cybercriminalité. Toutefois, ces enjeux prennent une dimension nouvelle dans le cyberespace, le secteur privé ayant une mainmise importante sur ce dernier.

Références

CIPC. (2014). 4e Rapport international sur la prévention de la criminalité et la sécurité quotidienne. Montréal : Centre International pour la prévention de la Criminalité. Consulté à l'adresse http://www.crime-prevention-intl.org/fr/publications/report/report/article/4e-rapport-international-sur-la-prevention-de-la-criminalite-et-la-securite-quotidienne.html

CIPC. (2016). 5e Rapport international sur la prévention de la criminalité et la sécurité quotidienne : les villes et le Nouvel Agenda Urbain. Montréal : Centre International pour la prévention de la Criminalité. Consulté à l'adresse http://www.crime-prevention-intl.org/fr/publications/report/report/article/5e-rapport-international-sur-la-prevention-de-la-criminalite-et-la-securite-quotidienne-les-vi.html

ONUDC. (2015). L'état de la criminalité et de la justice pénale dans le monde. Rapport du Secrétaire général (A/CONF.222/4). Congrès des Nations unies pour la prévention du crime et la justice pénale. Doha: ONUDC.


CROSS
CRIME
SCENE

CHAPITRE 1

TENDANCES EN MATIÈRE DE CRIMINALITÉ ET DE PRÉVENTION DE LA CRIMINALITÉ

Ce premier chapitre cherche à présenter les grandes tendances en ce qui concerne les chiffres sur la délinquance ainsi que les efforts menés à une échelle internationale afin de la prévenir. Il se divise en trois parties. La première partie concerne les tendances internationales en matière de criminalité. Dans ce contexte, nous avons choisi sept thématiques à aborder : les homicides, les homicides de femmes, la violence envers les enfants et les jeunes, la violence dans les villes, les problématiques criminelles liées aux drogues, le taux d'incarcération et le sentiment d'insécurité. La deuxième partie se concentre sur les efforts récents des organismes internationaux et régionaux en matière de prévention de la criminalité. Enfin, la troisième partie est une description des dernières études empiriques sur le sujet. À ce titre a été réalisée une revue des documents scientifiques ayant analysé des données empiriques publiées entre 2015 et 2017. Celle-ci cherche à décrire l'information la plus récente en matière de prévention de la criminalité et ainsi, présenter un portrait réaliste des intérêts et des préoccupations de la recherche à ce sujet à l'échelle mondiale. Trois thématiques ont été analysées dans ce rapport : la recherche concernant l'approche communautaire et urbaine, le rôle de la police dans la prévention, notamment à travers l'analyse criminelle, et enfin la relation entre les jeunes et la criminalité.

Introduction

Comme dans les éditions précédentes des Rapports internationaux du CIPC, l'objectif de ce premier chapitre est de présenter les grandes tendances relatives aux chiffres de la délinquance ainsi que les efforts permettant de la prévenir.

À la différence des dernières versions, ce chapitre a subi quelques modifications. D'une part, une révision des points structurants abordés dans les cinq dernières versions a été effectuée sur la base de laquelle, nous avons déterminé sept thématiques principales à aborder dans la première partie de ce chapitre. D'autre part, nous avons décidé de réaliser une revue des documents scientifiques ayant analysé des données empiriques publiées entre 2015 et 2017. Cette revue de littérature cherche à décrire l'information la plus récente en matière de prévention de la criminalité et ainsi, présenter un portrait réaliste des priorités et des préoccupations de la recherche à ce sujet, à l'échelle mondiale.

Ce chapitre est divisé en trois parties. La première présente les grandes tendances mondiales en ce qui concerne la criminalité. La deuxième partie aborde les avancements à l'échelle internationale, régionale et nationale en matière de prévention de la criminalité, notamment en ce qui concerne les organismes internationaux et nationaux. Enfin, la troisième partie décrit trois thématiques issues de la revue de littérature, en mettant l'accent sur l'efficacité des mesures mises en place.

Première partie : les tendances en matière de criminalité

Malgré les efforts entrepris pour harmoniser les catégories de crimes à partir de la « Classification internationale des infractions à des fins statistiques » (UNODC, 2015a), les statistiques sur la criminalité restent un enjeu majeur de la politique publique concernant la prévention du crime. Dans un rapport récent de l'ECOSOC, l'Afrique et l'Océanie par exemple ont été exclues de l'analyse des tendances en matière d'homicides volontaires en raison de données fragmentaires ou irrégulières (ECOSOC, 2017). Les données que nous présenterons doivent par conséquent être comprises dans ce contexte.

Homicides

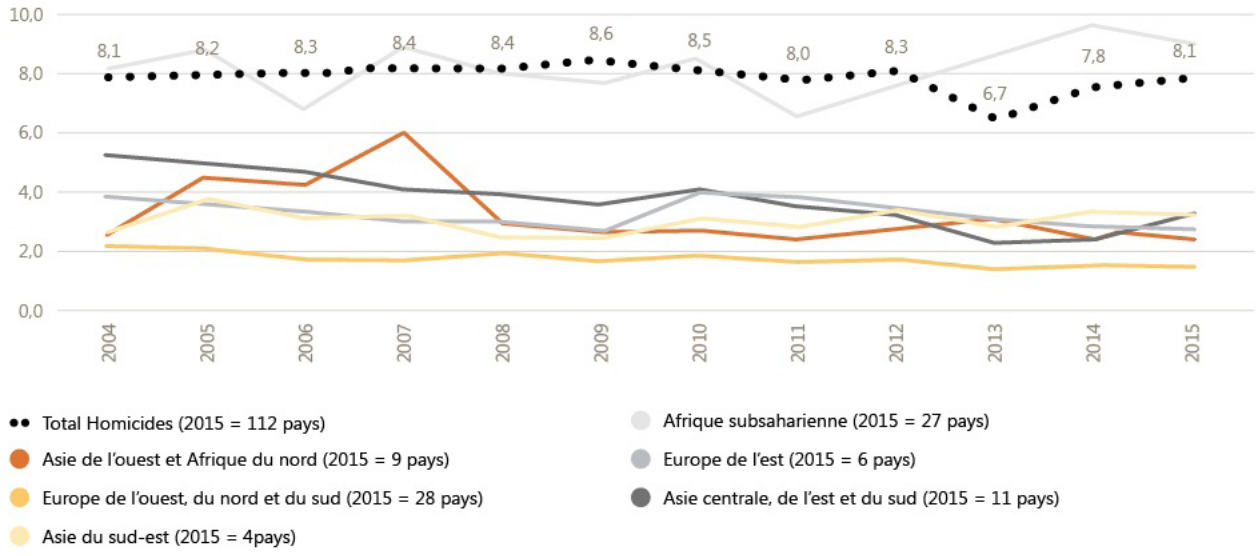
Entre 2004 et 2015, le taux d'homicides (TH) est resté relativement stable, autour de 8 pour 100 000 habitants (8 ‰). Ce chiffre ne montre pourtant pas la grande variation du taux d'homicide par région. En effet, la criminalité ne présente pas une distribution spatiale homogène, mais tend à se concentrer dans des territoires spécifiques. Cette hétérogénéité spatiale se constate à toutes les échelles, depuis le niveau macro (certains pays présentent des taux de criminalités plus élevés que d'autres), jusqu'au niveau local et micro-local (certaines villes et, au sein de ces villes, certains territoires précis concentrent la majorité des activités criminelles).

Encadré 1.1. **Les 10 pays avec le taux d'homicide le plus élevé au monde (2015)**

Le Salvador	108,6
Honduras	63,8
Venezuela	57,1
Jamaïque	43,2
Afrique du Sud	34,3
Trinidad et Tobago	30,9
Brésil	26,7
Colombie	26,5
Guyane	19,4
Mexique	16,3

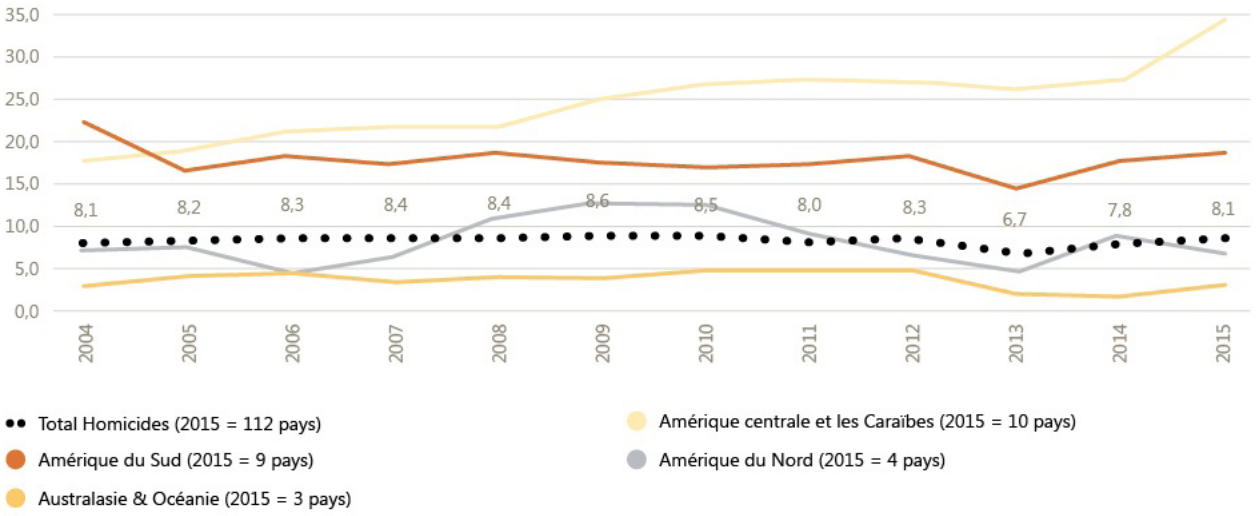
Source : ONUDC

Graphique 1.1. **Taux d'homicide pour 100 000 habitants par région (partie 1)**



Source: ONUDC

Graphique 1.2. **Taux d'homicide pour 100 000 habitants par région (partie 2)**



Source: ONUDC

Les graphiques 1.1 et 1.2 présentent les TH par région. L'Amérique latine reste la région avec le TH le plus important au niveau mondial. Ceci est dû en grande partie à l'augmentation continue des homicides en Amérique centrale et dans les Caraïbes depuis 2004, notamment une augmentation de 24% entre 2014 et 2015. Le Salvador (108,6 %ooo) et le Honduras (63,8 %ooo) sont les pays ayant les taux d'homicides les plus élevés au niveau mondial. D'après les données statistiques de l'ONUDC, la violence des gangs de rue et le crime organisé sont à l'origine d'une grande partie de ces homicides. En 2011, 65,4 % des homicides aux Bahamas, 50 % en Jamaïque et 37,1 % au Costa Rica étaient le fruit de l'action du crime organisé et des gangs de rue. En 2012, ce chiffre atteignait 16,8 % au Salvador et 52,1 % au Panama.

L'Amérique du Sud présente un TH moins élevé, mais néanmoins important. Entre 2006 et 2012, cette région a connu une certaine stabilité autour d'un TH de 18 %ooo. À partir de 2013, le TH montre un retour à la hausse pour atteindre 19,1 %ooo

en 2015, principalement en raison de taux élevés au Venezuela (57,2 %ooo), au Brésil (26,7 %ooo) et en Colombie (26,3 %ooo). Ce dernier pays est un cas intéressant, puisque malgré un TH encore très élevé, on observe une diminution progressive des homicides depuis 2004. Le Venezuela a connu la tendance inverse, passant d'un TH de 36,9 %ooo en 2004 à 57,2 %ooo en 2015. L'Amérique du Nord en revanche a connu une variabilité assez importante entre 2004 et 2015 avec une diminution progressive depuis 2009, période pendant laquelle le TH de la région a été le plus élevé (12,3 %ooo).

Les données statistiques de l'ONUDC, concernant l'Afrique subsaharienne sont incomplètes sauf dans le cas des années 2005, 2010 et 2015. Ces trois points de repérage nous permettent d'observer une tendance à l'augmentation du TH depuis 2011, qui atteint 9,2 %ooo en 2015, au-dessus du TH moyen mondial. Un cas particulier en Afrique est celui de l'Afrique du Sud qui est le cinquième pays avec le TH le plus élevé au monde (34,3 %ooo) et où la tendance est à une constante augmentation depuis 2010. D'après les données de l'*Institute for Security Studies*, suite à un déclin entre 2004 et 2012, les homicides en Afrique du Sud ont augmenté de 22 % entre cette même année et 2017[1]. Dans la même lignée que l'Afrique du Sud, la République Démocratique du Congo (13,4 %ooo) et la République Centrafricaine (13,1 %ooo) présentent des TH élevés. Cusson et al. (2017), dans un ouvrage récemment publié, observent au contraire une diminution importante du TH entre 2008 et 2012 en Afrique de l'Ouest, sauf dans les cas du Nigeria et du Niger. La Côte d'Ivoire par exemple a connu une diminution de 75 %, la Guinée Conakry et la Guinée-Bissau de 60 %. Une croissance économique stable, la démocratisation des pays et la progression des classes moyennes pourraient expliquer selon les auteurs cette diminution, notamment en raison d'une augmentation des services de sécurité privée et de meilleures pratiques policières (Cusson et al., 2017).

Une autre région qui a connu une augmentation, même si elle est légère, est l'Asie du Sud-Est. Notamment, depuis la crise économique de 2008, cette région est passée d'un TH de 2,5 %ooo à 3,3 %ooo en 2015. Une grande partie de cette augmentation est due aux Philippines, car le pays est passé d'un TH de 7,5 %ooo à 9,8 %ooo entre 2004 et 2015. Une tendance qui continuera probablement de s'accroître au cours des prochaines années, dans un contexte de répression violente des consommateurs et trafiquants de drogues, notamment marqué par des exécutions extrajudiciaires (Kreuzer, 2016).

Le autres régions du monde ont globalement connu une tendance vers la diminution du taux d'homicide et sont toujours depuis 2004 en dessous du taux moyen mondial. L'Europe de l'Ouest, du Nord et du Sud, ont un TH très peu élevé et connaissent une diminution légère, mais constante depuis 2004, avec en 2015 un TH de 1,4 %ooo. Le TH de l'Australie a baissé de 34 % entre les années 2004 et 2015, avec un TH de 0,98 %ooo pour la dernière année. Cependant, on notera que le Moyen-Orient et l'Afrique du Nord ont connu une augmentation entre 2004 et 2007, pour ensuite aller vers une stabilisation du TH autour de 3 %ooo.

Encadré 1.2. **Les armes à feu et les tueries de masse**

Dans de nombreux pays, tout particulièrement aux États-Unis, la relation entre l'accès aux armes à feu et les homicides fait désormais l'objet d'un débat accru, notamment en raison des tueries de masse qui y choquent régulièrement l'opinion publique. D'après la base de données du site *Mother Jones*, entre 2015 et le mois de mars 2018, vingt-sept fusillades se sont produites aux États-Unis[2], ayant eu comme résultat 258 personnes assassinées et 728 blessés. Dans une grande partie de ces cas, des fusils semi-automatiques ont été utilisés. Les cadres législatifs très permissifs et la culture des armes aux États-Unis sont régulièrement évoqués, le pays ayant le taux d'armes à feu par habitant le plus important du monde: 89 armes à feu pour 100 habitants (Small arms survey, 2007). Une étude récente estime à 22 %, le taux de personnes étant propriétaires d'armes à feu, avec une moyenne de 4,8 armes par habitant, c'est-à-dire 265 millions d'armes à feu dans le pays (Azrael, Hepburn, Hemenway, & Miller, 2017). Cette même étude signale qu'en 2015, 36 252 personnes sont décédées à cause d'armes à feu et que plus de 80 000 ont été blessées. 60,7 % de ces décès étaient le résultat de suicides et 37,1 % d'homicides. D'après les données statistiques de l'ONUDC en 2012, 60 % des homicides aux États-Unis étaient causés par des armes à feu, tandis qu'à l'échelle mondiale, ce pourcentage était de 32 % en 2011.

La relation entre crimes et armes à feu a été largement débattue aux États-Unis. Entre 1994 et 2004, l'achat d'armes semi-automatiques a été interdit dans le pays [Federal Assault Weapons Ban]. Une évaluation sur les effets de cette interdiction sur les crimes violents n'a pas montré de différence significative, en raison notamment du fait que ces armes ne sont généralement pas utilisées pour commettre ce type de crime (Koper, Woods, & Roth, 2004). En revanche, le taux d'homicide au Mexique a augmenté significativement après la fin de cette interdiction, notamment dans les villes proches de la frontière (Chicoine, 2017), ce qui pourrait indiquer une corrélation, notamment rendue possible par un important trafic d'armes entre les deux pays.

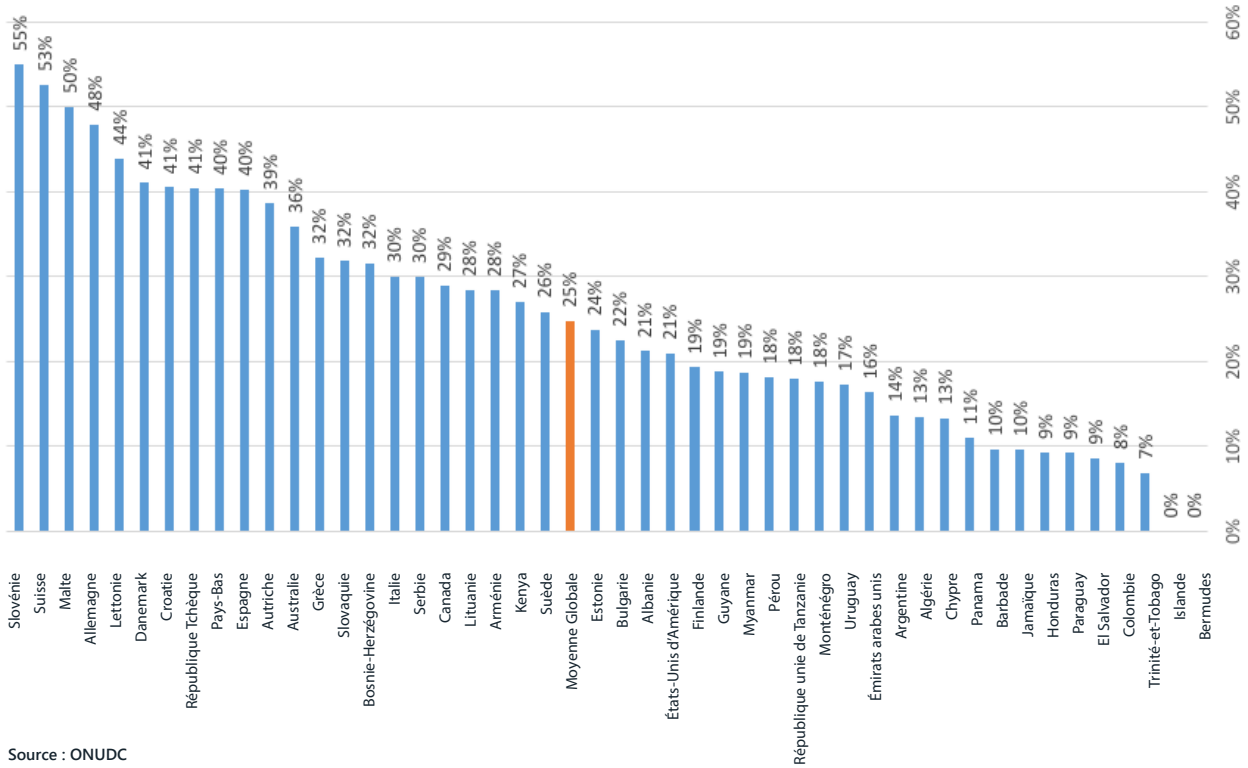
Un ratio d'armes à feu supérieur n'est pas systématiquement corrélé à des taux d'homicides plus élevés (Small arms survey, 2007). Cependant, Levan (2013) suggère qu'il n'existe pas de relation causale entre le port d'armes et les crimes, mais que le port d'armes constituerait plutôt un facilitateur de la violence. C'est le cas notamment de la violence conjugale, où la présence d'une arme à feu dans le foyer triple le risque d'homicide (Levan, 2013).

Les femmes victimes d'homicides

Le ratio moyen de femmes victimes d'homicides était de 25 % au niveau mondial en 2015. D'après les données statistiques de l'ONUDC, ce chiffre est resté relativement stable entre 2006 et 2014 (entre 28 % et et 29 %).

Comme il a été souligné à plusieurs reprises, il existe une sur-représentation des hommes tant dans les crimes ordinaires que dans les homicides (ICPC, 2016). Cependant, si l'on observe le Graphique 1.3, on peut voir que les pays avec un TH plus important sont aussi ceux où le pourcentage de femmes victimes d'homicides est moins important[3]. En d'autres mots, là où la violence est plus importante, ce sont les hommes qui sont les principales victimes.

Graphique 1.3. **Part des femmes victimes d'homicides volontaires par rapport au total des victimes des deux sexes (ratio femme/homme) en 2015**



Source : ONUDC

La violence contre les enfants et les jeunes

Selon un rapport publié en 2017 par l'initiative mondiale *Know violence in Childhood* basée à New Dehli en Inde, trois enfants sur quatre dans le monde (1,7 milliard) - ont été victimes d'une forme quelconque de violence au cours de l'année 2015, dont 100 000 victimes d'homicides[4] (Shiva Kumar & Stern, 2017).

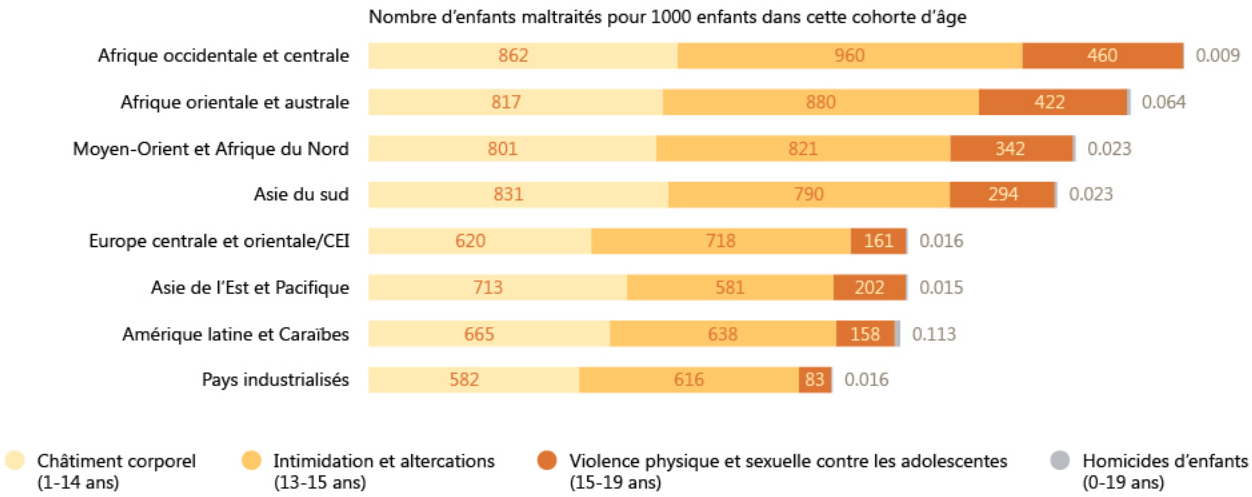
D'après ce rapport, la violence contre les enfants est pratiquement universelle, touchant autant le Nord que le Sud. C'est le cas du châtiment corporel et de l'intimidation subis par six à neuf enfants sur dix à l'échelle mondiale (voir Graphique 1.4). Malgré cette transversalité, les différences régionales se font sentir. L'Afrique, le Moyen-Orient et l'Asie du sud par exemple, présentent les taux de violences physiques et sexuelles les plus importants. En revanche, les homicides d'enfants (0-19 ans) sont plus enregistrés en Amérique latine (TH = 11,3 ‰) et en Afrique occidentale et centrale (TH = 9,9 ‰).

Tableau 1.1. **Les pays avec les taux d'homicides d'enfants les plus élevés**

Pays	
Salvador	27
Guatemala	22
Venezuela	20
Lesotho	18
Brésil	17
Swaziland	16
Panama	15
République démocratique du Congo	14
Nigéria	14
Colombie	13
Honduras	13
Jamaïque	13
Rwanda	13

Source : Shiva Kumar & Stern (2017, p. 18)

Graphique 1.4. **Charge régionale de la violence contre les enfants (2015)**



Source: Shiva Kumar & Stern (2017, p. 18)

Les villes et la violence

Le Conseil citoyen pour la sécurité publique et la justice pénale (CCSPJP), basé à Mexico publie chaque année un classement des villes présentant les taux d'homicides les plus élevés au niveau mondial (Tableau 1.2). En 2017, l'Amérique latine y est largement surreprésentée, avec 42 villes sur les cinquantes présentées dans la liste. En moyenne, ces 50 centres urbains ont un TH de 59,17%ooo et sont en grande majorité situés au Brésil (17) et au Mexique (12). En dehors de l'Amérique latine, 4 villes aux États-Unis, 3 villes en Afrique du Sud et une ville en Jamaïque font également partie de ce classement. Il convient ici de souligner le fait que les États-Unis sont le seul pays dit « développé » à figurer à ce palmarès, ce qui illustre la réalité de la violence dans certains centres urbains du pays, une violence qui tend à empirer : St-Louis par exemple avait un TH de 49,93 %ooo en 2015 qui a augmenté pour atteindre 65,83 %ooo en 2017. Baltimore avait un TH de 33,9 %ooo en 2015 qui est passé à 55,5%ooo en 2017. D'autres villes aux États unis ont connu des augmentations semblables. Chicago par exemple a connu une augmentation de 80 % entre 2015 et 2016, tandis que d'autres villes importantes comme New York et Los Angeles ont maintenu une diminution progressive (Fagan & Richman, 2017). D'après ces auteurs, ceci s'explique par des facteurs locaux, notamment par la méfiance des citoyens envers le gouvernement de la ville et la police, l'augmentation des tensions entre les petits gangs de rue et plus particulièrement, les épidémies récurrentes de drogues illégales au sein des villes. Le cas le plus récent étant celui l'épidémie des opioïdes (voir Encadré 1.3).

Tableau 1.2. **Les villes avec les taux d'homicides les plus élevés au monde (pour 100 000 habitants)**

Position	Ville	Pays	Taux d'homicides pour 100 000 habitants
1	Los Cabos	Mexique	111,33
2	Caracas	Venezuela	111,19
3	Acapulco	Mexique	106,6
4	Natal	Brésil	102,56
5	Tijuana	Mexique	100,77
6	La Paz	Mexique	84,79
7	Fortaleza	Brésil	83,48
8	Victoria	Mexique	83,32
9	Guayana	Venezuela	80,28
10	Belém	Brésil	71,38
11	Vitória da Conquista	Brésil	70,26
12	Culiacán	Mexique	70,1
13	St. Louis	États Unis	65,83
14	Maceió	Brésil	63,94
15	Cape Town	Afrique du Sud	62,25
16	Kingston	Jamaïque	59,71
17	San Salvador	El Salvador	59,06
18	Aracaju	Brésil	58,88
19	Feira de Santana	Brésil	58,81
20	Juárez	Mexique	56,16
21	Baltimore	États Unis	55,48
22	Recife	Brésil	54,96
23	Maturín	Venezuela	54,43
24	Guatemala	Guatemala	53,49
25	Salvador	Brésil	51,58

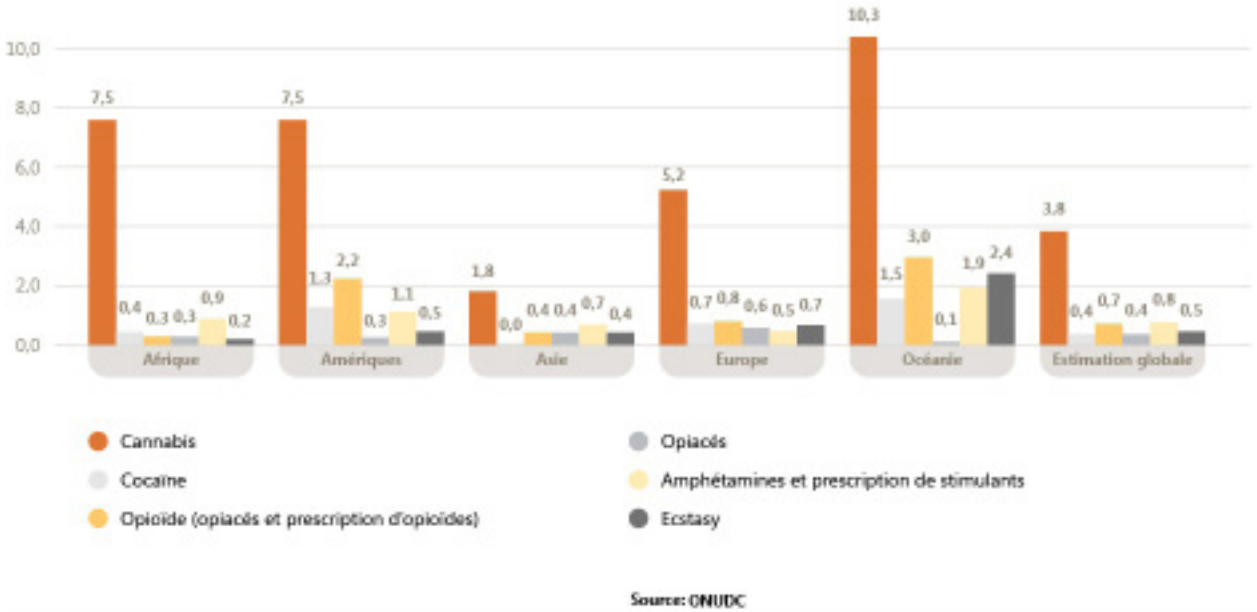
Source : CCSPJP (2018)

La diversification du marché des drogues et la légalisation du cannabis

D'après le Rapport mondial sur les drogues (UNODC, 2017b), 5% de la population adulte mondiale, auraient consommé des drogues au moins une fois en 2015, principalement du cannabis (Graphique 1.5). Environ 29,5 millions d'entre elles souffrent de troubles liés à cet usage. Les opioïdes restent les drogues les plus dangereuses, suivies par les amphétamines, qui sont la cause de nombreux décès prématurés par surdose ou par des maladies infectieuses transmises à l'occasion de pratiques d'injection inappropriées (UNODC, 2017b). Les opioïdes sont également les drogues les plus associées à la commission de délits (ICPC, 2015).

Le marché des drogues continue à se diversifier, notamment en raison de la persistance de drogues traditionnelles et l'apparition de nouvelles substances psychoactives (UNODC, 2017b). Comme l'indique DuPont (2018), ceci peut s'expliquer également par la décentralisation de la production des drogues synthétiques.

Graphique 1.5. **Prévalence de la consommation de drogues par région en 2015 (%)**



Source: ONUDC

Encadré 1.3. **La crise des opioïdes aux États-Unis**

Si les dommages causés par les opioïdes posent problème dans de nombreux pays, ils sont particulièrement manifestes aux États-Unis. L'utilisation abusive d'opioïdes pharmaceutiques et un usage croissant d'héroïne et de fentanyl, phénomènes combinés et interdépendants, ont débouché dans ce pays sur une véritable épidémie ainsi que sur une augmentation de la morbidité et de la mortalité liées aux opioïdes.

Environ un quart des décès liés à la drogue (y compris par surdose) ont lieu aux États-Unis. Majoritairement liés à l'usage d'opioïdes, les décès par surdose ont plus que triplé dans ce pays entre 1999 et 2015, passant de 16 849 à 52 404 par an. Au cours de la seule année 2017, ils ont augmenté de 11,4 %, atteignant ainsi le niveau le plus haut jamais enregistré. De fait, chaque année, le nombre de décès liés au mésusage d'opioïdes dépasse largement celui des décès dus à la violence ou aux accidents de la route aux États-Unis.

Un lien a été établi entre l'apparition de dérivés de médicaments soumis à prescription considérés comme des nouvelles substances psychoactives (NSP), en particulier d'analogues du fentanyl, et le nombre grandissant de surdoses, y compris mortelles, chez les usagers d'opioïdes. Ces dernières années, plusieurs opioïdes de synthèse récemment mis au point ont été associés à l'augmentation des incidents graves et des décès. Les comprimés et poudres contenant des opioïdes de synthèse, qui sont vendus sur le marché illicite, constituent une menace pour la santé publique, d'autant plus que la concentration et la puissance de leurs principes actifs sont variables.

Source : UNODC (2017b, p. 10)

La production de la cocaïne a également augmenté de 30 % entre 2013 et 2015 et celle de l'opium d'un tiers entre 2015 et 2016 (UNODC, 2017b). Dans le premier cas, ceci s'explique notamment à cause de l'augmentation de la production en Colombie et dans le deuxième cas, en raison de l'amélioration du taux de rendement des champs en Afghanistan. Même si l'identification des réseaux de trafic s'est améliorée, le flux du trafic s'est également diversifié (UNODC, 2017b).

Une évolution majeure est la légalisation du cannabis en Uruguay, et désormais dans huit États aux États-Unis ainsi que dans le District de Columbia (UNODC, 2017b). Le Canada a annoncé récemment que l'usage récréatif du cannabis sera légalisé le 17 octobre 2018. L'Afrique du Sud, suite à un arrêt de justice de 2017 a légalisé de facto la consommation de cannabis, une décision confirmée par la Cour Constitutionnelle en septembre 2018. Plusieurs pays, notamment en Europe, en Amérique et en Océanie ont récemment légalisé son usage médicinal. Sans faire encore l'unanimité à l'échelle mondiale, l'on observe une transition de la guerre contre les drogues vers une approche de santé publique axée sur la dépénalisation (ICPC, 2015) et dans certains cas, la légalisation, notamment du cannabis.

L'évolution de la population carcérale et son influence sur le crime

En ce qui concerne les taux d'incarcération, on observe trois périodes. Entre 2004 et 2007, le taux d'incarcération est variable. Entre 2007 et 2012, l'on observe une tendance vers une augmentation progressive du taux d'incarcération qui correspond à la période de la crise économique de 2008. À partir de 2012, ce taux commence progressivement à diminuer.

Le taux d'incarcération par région présente des variations importantes. L'Amérique du Nord, notamment à cause des États-Unis, a le taux le plus élevé d'incarcérations au niveau mondial (449,9 personnes emprisonnées pour 100 000 habitants), 2015 étant l'année où l'on observe le taux le plus élevé de la période étudiée dans la région. Les États-Unis ont en effet le taux d'incarcération le plus élevé à l'échelle des pays (675,6 %ooo), suivi de loin par Trinité-et-Tobago (547,54 %ooo) et le Salvador (532,84 %ooo).

La région d'Amérique centrale et des Caraïbes présente le second taux d'incarcération le plus élevé, même si depuis 2011 l'on observe une diminution progressive. En revanche, l'Amérique du Sud, située autour de la moyenne mondiale a connu une augmentation presque linéaire depuis 2005 (152,2 %ooo), pour atteindre en 2015 le taux le plus élevé de la période étudiée (235,6 %ooo). L'Europe de l'Est a connu une évolution inverse. En effet depuis 2004 (263 %ooo), la région enregistre une chute au niveau du taux d'incarcération, particulièrement accentuée à partir 2011. Dans un rapport récent de l'ECOSOC (2017), cette diminution s'explique par l'effet dissuasif du taux de condamnation pour homicide qui est plus important que dans d'autres régions.

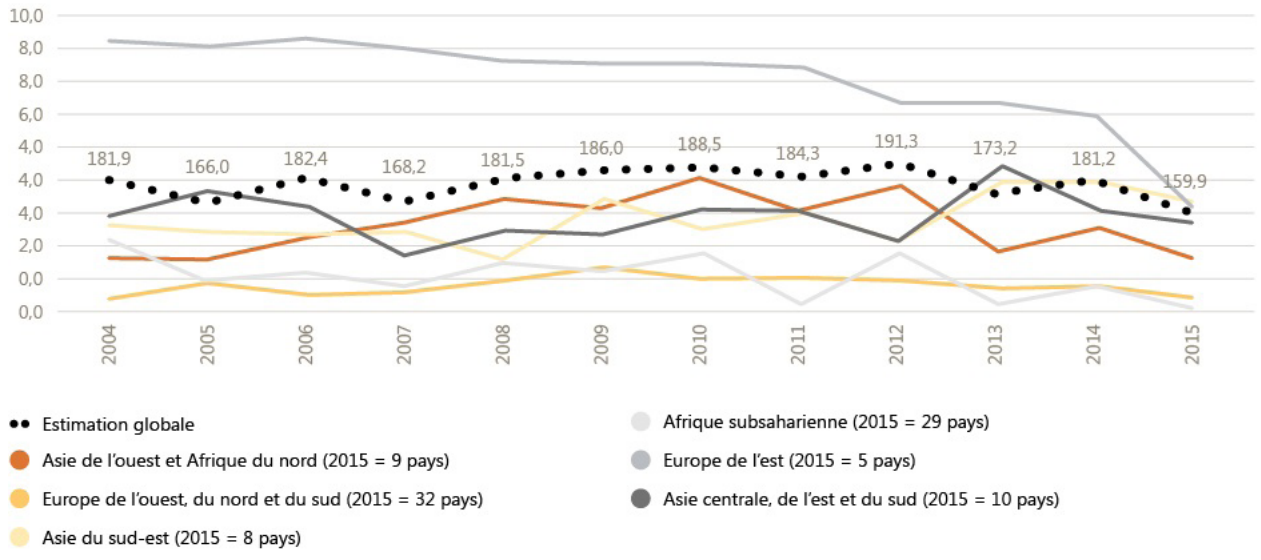
Ce même rapport remet toutefois en question l'influence du système pénal sur la criminalité : « Le fait qu'il y ait davantage de personnes en prison n'entraîne pas nécessairement une baisse des taux d'homicide, et le recul du taux d'incarcération n'engendre pas automatiquement une vague de criminalité » (ECOSOC, 2017, p. 10). En effet, plusieurs recherches ont remis en question l'impact dissuasif du système pénal sur le crime (Cullen, Jonson, & Nagin, 2011; Harding, Morenoff, Nguyen, & Bushway, 2017; Loeffler, 2013; Roeder, Eisen, Bowling, Stiglitz, & Chettiar, 2015). Roeder et al. (2015) par exemple expliquent que le taux d'incarcération a eu un effet très limité à partir des années 1990 et plutôt nul à partir des années 2000 aux États-Unis. Pour leur part, Cullen et al. (2011) expliquent qu'il existe très peu de preuves confirmant l'effectivité de l'emprisonnement sur le taux de récidive et qu'au contraire, il en existe en ce qui concerne l'effet criminogène des prisons.

Tableau 1.3. **Taux mondial d'incarcération (2004-2015)**

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Taux pour 100 000 hbts de personnes incarcérées	181,9	166,0	182,4	168,2	181,5	186,0	188,5	184,3	191,3	173,2	181,2	159,9
% de personnes incarcérées avec une sentence	73,5	72,3	68,0	70,5	67,3	68,1	68,6	72,6	65,1	69,7	71,0	80,0
% de personnes étrangères incarcérées	0,04	0,04	0,04	0,05	0,04	0,05	0,04	0,04	0,04	0,04	0,04	0,07
% de jeunes incarcérés	0,30	0,69	0,76	0,73	0,69	0,76	0,95	1,09	1,00	0,99	0,98	0,92
% de femmes adultes incarcérées	3,74	4,32	4,76	4,85	4,72	4,39	4,59	4,60	5,59	4,53	5,94	6,74

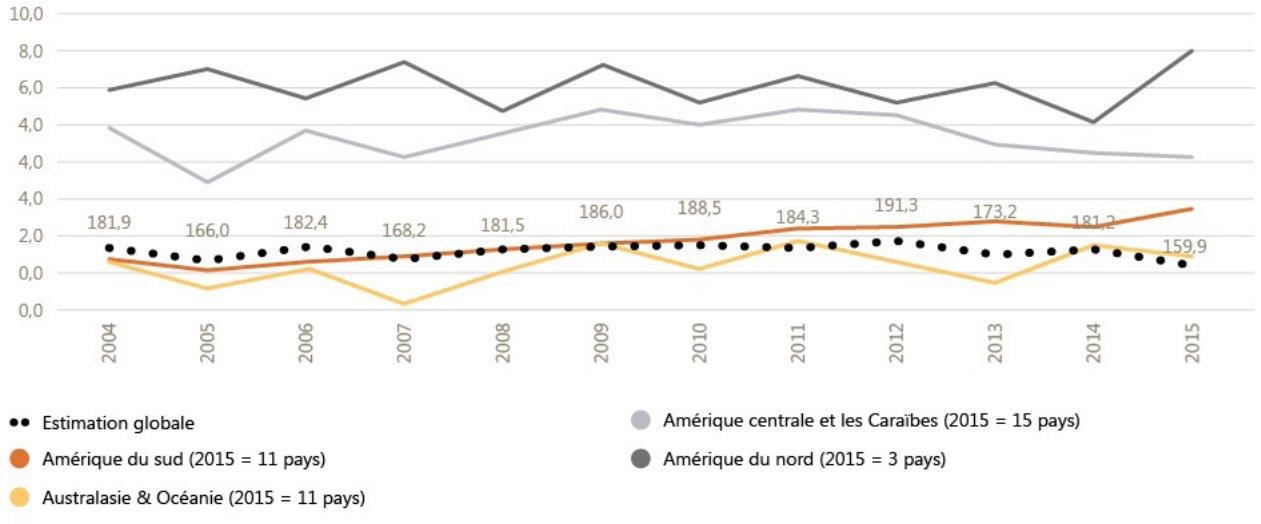
Source: ONUDC

Graphique 1.6. **Taux d'incarcération pour 100 000 habitants par région (partie 1)**



Source: ONUDC

Graphique 1.7. **Taux d'incarcération pour 100 000 habitants par région (partie 2)**



Source: ONUDC

Le sentiment d'insécurité

C'est autour des années 1960 que l'on commence à étudier le sentiment d'insécurité, notamment à partir d'une préoccupation croissante sur les attitudes et les perceptions des citoyens sur la politique publique (Gouseti, 2017). L'un des enjeux principaux était évidemment d'analyser le lien entre les crimes effectifs et ce sentiment d'insécurité (Lewis & Salem, 2016). Pourtant, la littérature n'établit aucune relation directe entre ces deux dimensions à une échelle individuelle (Zhao, Lawton, & Longmire, 2015). Pour la plupart des chercheurs, le sentiment d'insécurité est un phénomène multifactoriel qui dépend de plusieurs variables, dont le crime (CIPC, 2016b; Jackson & Gouseti, 2014). Pour d'autres, la recherche sur le crime et celle sur le sentiment d'insécurité représentent deux champs d'études associés, mais indépendants (Johnson, 2016). Le sentiment d'insécurité a trois composantes : la réaction affective, la composante comportementale, qui implique les actions entamées afin d'éviter la victimisation (installation d'alarmes, éviter le transport public, etc.) et la composante cognitive, c'est-à-dire l'évaluation du risque de victimisation ainsi que l'évaluation des conséquences de la victimisation (Gouseti, 2017).

Encadré 1.4. **Facteurs individuels ayant une influence sur le sentiment d'insécurité**

- L'expérience vécue, par exemple une victimisation passée (directe ou indirecte).
- Le genre : les hommes craignent par exemple davantage des grands groupes et les femmes des individus isolés et des agressions sexuelles.
- L'âge : les personnes âgées ont tendance à se sentir plus en insécurité alors qu'elles sont comparativement moins fréquemment victimes.
- La capacité de se défendre.
- L'état de santé.
- Le niveau de formation : les plus diplômés étant moins enclins à l'anxiété.
- La vulnérabilité sociale : le fait d'avoir un emploi ou non par exemple ou le fait d'appartenir à une minorité.
- Le rang social : les personnes disposant de ressources éducatives, professionnelles et financières voient la délinquance comme un enjeu mineur.

Source : CIPC (2016b)

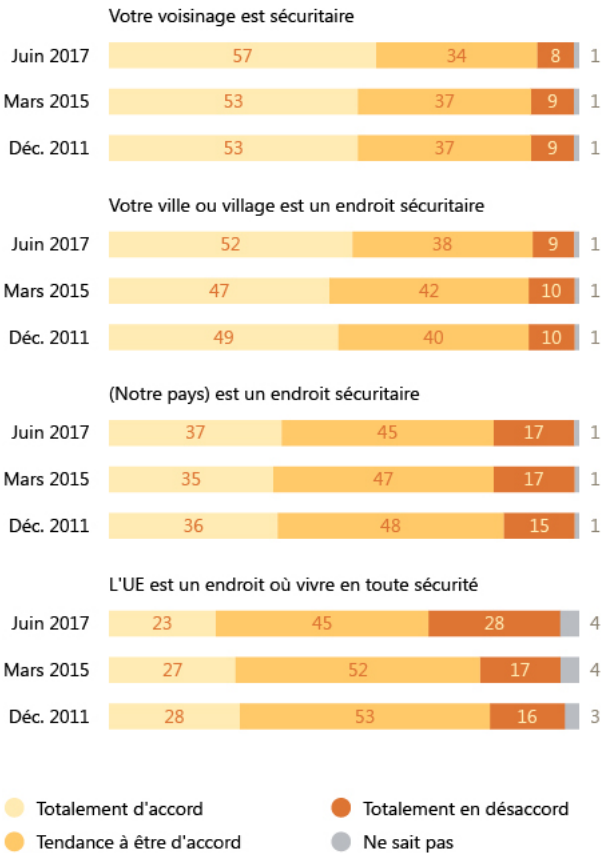
Aucune étude internationale existante ne permet de faire une comparaison internationale du sentiment d'insécurité sur une même base méthodologique. Les sondages de tybe « baromètres » sont probablement ce qui se rapproche de ce modèle. Cependant, l'Eurobaromètre et les autres « baromètres » sont faits en fonction de besoins différents, ce qui rend difficile la comparabilité. Ni l'Arab-baromètre ou l'Asie-baromètre par exemple ne posent de questions spécifiques de façon régulière sur le sentiment d'insécurité. Dans le cas du dernier, seule la deuxième vague (9 pays = 2005-2008) du baromètre incluait une question qui y était associée, où 86,1 % des personnes interrogées se sentaient en sécurité ou très en sécurité (*Asian-Barometer*, 2008).

Le dernier Euro-baromètre concernant la perception de sécurité nous donne un aperçu de cette problématique en Europe (*European Commission,* 2017). Neuf Européens sur dix disent se sentir en sécurité dans leur ville ou leur quartier. En revanche, le pourcentage de personnes percevant l'Union européenne comme une région sécuritaire a chuté de 11% entre 2011 et 2017. Ceci s'explique notamment en raison des attentats terroristes perpétrés depuis 2015. En effet, la plupart des personnes interrogées considèrent que le terrorisme, le crime organisé et la cybercriminalité sont les principaux enjeux de sécurité dans la région.

Dans le cas de l'Amérique latine, la situation est complètement différente (*Corporación Latinobarómetro*, 2017). En 2017, presque la moitié des personnes interrogées disaient avoir peur d'être victimes d'un délit, une part qui a augmenté de façon presque linéaire depuis 2009. Le pourcentage des personnes interrogées qui disent n'avoir jamais eu peur au cours de 2017 est de 15 %. Cependant, bien que ce pourcentage semble logique, si l'on considère les taux élevés d'homicide dans la région, la variation entre pays est un élément important à ne pas oublier. Dans certains pays comme le Chili ou l'Uruguay, qui ont des taux de criminalité très bas, le pourcentage des personnes qui déclarent n'avoir jamais eu peur d'être victimes d'un délit atteint 16% et 20% respectivement. En revanche, des pays comme le Honduras (23%) ou le Guatemala (24%), qui ont des taux d'homicide très élevés enregistrent des pourcentages plus importants de personnes indiquant n'avoir jamais peur. Ces chiffres indiquent alors la profonde déconnexion qui existe entre sentiment d'insécurité et criminalité.

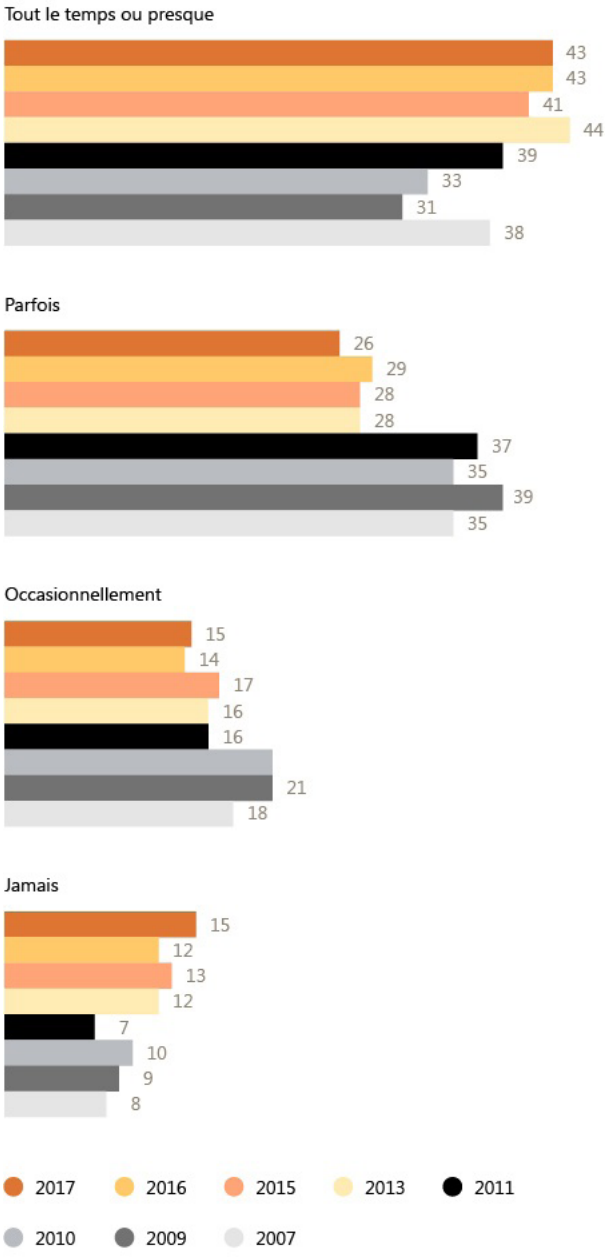
Dans le cas de l'Afrique, le dernier Afro-Baromètre (2017) indique que 68,9 % des personnes interrogées n'ont jamais eu peur d'être victimes d'un crime dans leur maison. Les variations entre les pays sont également importantes. Madagascar est le pays où ce pourcentage est le moins important (40,3 w%), suivi par l'Afrique du Sud (46,6 %). Cependant, le taux d'homicide à Madagascar est très bas (2010= 0,62 %ooo selon les données statistiques de l'ONUDC) comparé à l'Afrique du Sud, qui est le cinquième pays avec le taux d'homicide le plus élevé au monde (voir Encadré 1.1).

Graphique 1.8. **Dans quelle mesure êtes-vous d'accord ou pas avec chacune des affirmations suivantes sur la sécurité publique? (Europe)**



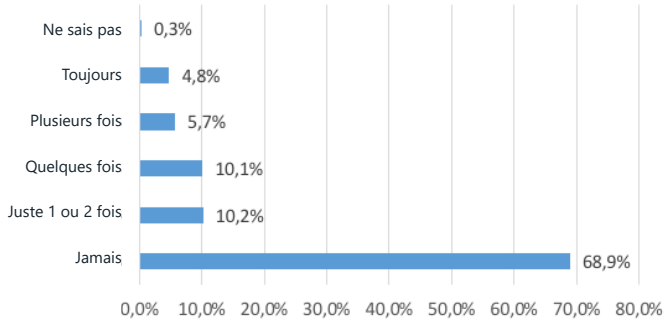
Source: Commission européenne (2017)

Graphique 1.9. **À quelle fréquence vous inquiétez-vous d'être victime d'un crime violent ?**



Source: Corporación Latinobarómetro (2017)

Graphique 1.10. **Crainte d'être victime d'un crime dans sa propre maison (Afrique = 36 pays)**

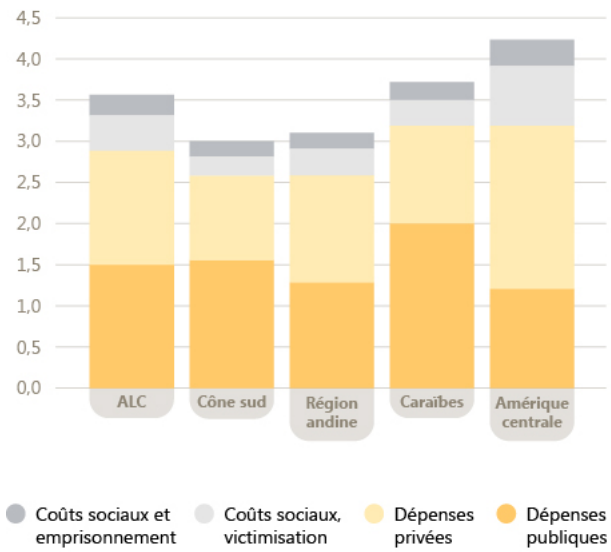


Source : Afro-Baromètre

Encadré 1.5. **Les coûts associés à la criminalité et à la violence en Amérique latine**

Une étude récente de la Banque interaméricaine de développement a fait une mise à jour sur les coûts associés à la criminalité dans la région (*Banco interamericano de desarrollo*, 2017). Les calculs se basent sur trois types de coûts : coûts sociaux, coûts pour le secteur privé, coûts pour le gouvernement.

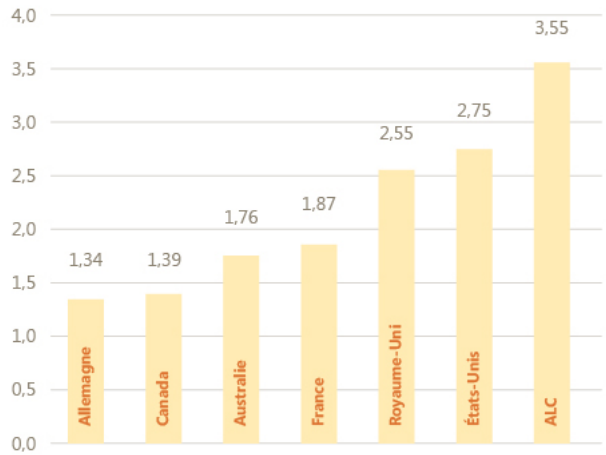
Graphique 1.11. **Coûts associées à la criminalité en Amérique latine (% du PIB)**



Source: Banco interamericano de desarrollo (2017, p. 28)

Les estimations faites indiquent que la région a enregistré une perte variant entre 114 500 millions et 170 400 millions de dollars américains en lien avec les crimes, ce qui représente en moyenne 3,5 % du PIB régional. La sous-région qui a le pourcentage le plus élevé est l'Amérique centrale, suivie des Caraïbes. D'une part, les deux pays où les coûts sont les plus élevés de la région sont aussi les pays où il y a plus de violence et de criminalité à l'échelle mondiale, à savoir le Honduras (6,5% du PIB) et El Salvador (5,9% du PIB). D'autre part, les pays avec un taux très bas d'homicide comme le Chili ou l'Uruguay affichent également des coûts plus bas. À l'inverse, le Mexique qui a pourtant un taux élevé de criminalité, est également le pays où le coût de la criminalité représente le pourcentage le plus bas de la région.

Graphique 1.12. **Comparaison internationale des coûts associés à la criminalité (% du PIB)**



Source: Banco interamericano de desarrollo (2017, p. 29)

L'étude fait également une comparaison entre six pays occidentaux et l'Amérique latine (voir Graphique 1.12). Dans tous les cas et dans toutes les composantes, le coût du crime en Amérique latine est supérieur à celui des pays occidentaux. Cependant, dans le cas des coûts d'emprisonnement, l'Australie et le Royaume-Uni sont à la hauteur de la région et les États-Unis la surpassent, ce qui est cohérent avec les taux élevés d'incarcération du pays. 14 des 17 pays de l'Amérique latine ont des coûts plus élevés que dans les pays occidentaux. Le Chili et le Pérou par exemple ont des coûts similaires à ceux des Etats-Unis, même avec un taux d'incarcération moins élevé.

Deuxième partie : développements internationaux et régionaux en matière de prévention de la criminalité

Dans cette partie, nous allons décrire les nouveaux avancements en matière de prévention du crime à l'échelle des organismes internationaux et régionaux.

Initiatives à l'échelle internationale

a) La Déclaration de Doha

Comme il a été souligné lors du 5e Rapport international, le Treizième Congrès des Nations Unies pour la prévention du crime et la justice pénale a eu lieu à Doha en2015 (CIPC, 2016a). L'un de résultats de ce Congrès a été l'adoption de la **Déclaration de Doha sur l'intégration de la prévention de la criminalité et de la justice pénale** (ONUDC, 2015b). Comme son nom l'indique cette déclaration vise l'un des problèmes les plus importants en matière de sécurité, à savoir la désarticulation fréquente entre le système de justice pénale et les stratégies de prévention du crime qui sont vus comme deux dimensions liées, mais indépendantes. Suite à cette déclaration, l'ONUDC a lancé un **Programme mondial** afin de soutenir quatre aspects clés de cette intégration : renforcer l'intégrité judiciaire et prévenir le système judiciaire de la corruption (des institutions solides, fiables et transparentes) ; promouvoir la réhabilitation et la réintégration des prisonniers afin de leur donner une nouvelle chance dans la vie (des systèmes de justice pénale justes, humains et efficaces) ; prévenir la criminalité chez les jeunes à travers des programmes sportifs et des formations aux compétences de base (prévention de la criminalité chez les jeunes) et soutenir l'intégration de la prévention du crime et de l'État de droit à tous les niveaux d'éducation (éducation pour la justice).

b) Prévention de la violence par l'OMS

L'OMS a lancé une **campagne mondiale pour la prévention de la violence** dont l'objectif est d'appliquer les recommandations publiées dans le Rapport mondial sur la violence et la santé en 2002, par la sensibilisation du public aux problèmes soulevés par la violence, et en insistant sur l'importance de la santé publique en la matière, qui permet de s'attaquer à la fois aux causes et aux conséquences de tels actes, tout en encourageant la prévention dans ce domaine (2017).

En 2017 également, l'OMS a lancé le « **Plan d'action mondial** pour renforcer le rôle du système de santé dans le cadre d'une réponse multisectorielle nationale pour lutter contre la violence interpersonnelle, en particulier contre les femmes et les filles, et contre les enfants » (WHO, 2017). Ce plan est le résultat de la résolution WHA67.15 de la 67e Assemblée mondiale de la santé et cherche à s'adresser spécifiquement aux femmes, filles et enfants en raison des particularités de la violence dont ils sont victimes, basée notamment sur des inégalités de genre et la discrimination (WHO, 2017). Il propose une série d'actions pratiques que les États membres peuvent entreprendre pour renforcer leurs systèmes de santé afin de lutter contre cette violence.

Encadré 1.6. **Objectifs du Plan d'action mondial pour renforcer le rôle du système de santé dans le cadre d'une réponse multisectorielle nationale pour lutter contre la violence interpersonnelle**

Les objectifs sont :

1. Traiter la santé et les autres conséquences négatives de la violence interpersonnelle, en particulier contre les femmes et les filles, et contre les enfants, en fournissant des services et des programmes de santé intégraux et de qualité, et en facilitant l'accès à des services multisectoriels.
2. Prévenir la violence interpersonnelle, en particulier contre les femmes et les filles, et contre les enfants.

Orientations stratégiques :

Afin d'atteindre ces objectifs, quatre orientations stratégiques sont proposées pour répondre à la fois au mandat du système et à l'approche de santé publique pour lutter contre la violence interpersonnelle.

1. Renforcer le leadership et la gouvernance du système de santé.
2. Renforcer la capacité de prestation des services de santé et la capacité de réponse des agents de la santé.
3. Renforcer la programmation pour prévenir la violence interpersonnelle, notamment les actions de prévention de la violence que le système de santé peut directement mettre en œuvre, en identifiant les personnes à risque et en menant des activités de promotion de la santé, ainsi que les actions de prévention de la violence auxquelles il peut contribuer par des actions multisectorielles.
4. Améliorer l'information et les données probantes.

Source : WHO (2017)

c) Premier programme à l'horizon 2030 pour les enfants: le Sommet des solutions pour mettre un terme à la violence

Les 14 et 15 février 2018, se tenait à Stockholm en Suède une conférence de haut niveau sur la violence à l'encontre des enfants: « **Premier programme à l'horizon 2030** pour les enfants : le Sommet des solutions pour mettre un terme à la violence » (Global Initiative to End All Corporal Punishment of Children, 2018). Ce programme s'inscrit dans les 17 objectifs de développement durable à l'horizon 2030 que les dirigeants du monde se sont engagés à atteindre, et en particulier l'objectif n°16.2 qui vise à prévenir et à mettre fin à la violence et à l'exploitation des filles et des garçons dans le monde entier. Un premier partenariat mondial a été lancé à ce titre en juillet 2016, à l'initiative des gouvernements, de l'UNICEF, de l'OMS et de diverses autres parties prenantes. Il compte 15 pays pionniers, tandis que le Japon, le Brésil et les Émirats arabes unis ont annoncé leur intention d'y adhérer lors du Sommet de février à Stockholm. Le seul pays ayant pris part à cette initiative, et considéré comme une économie développée, est la Suède.

d) Des rencontres de haut niveau

26ème session de la Commission pour la prévention du crime et la justice pénale (mai 2017)

La 26ème session de la Commission a été l'occasion de se pencher plus en avant sur onze projets de résolution portant sur diverses questions tenant notamment à la lutte contre la traite des êtres humains et le trafic des migrants, les liens entre terrorisme et criminalité transnationale organisée, les systèmes pénitenciers et l'emprisonnement, l'inclusion de la perspective de genre dans la lutte contre la criminalité transnationale organisée, ou encore la cybercriminalité (UNODC, s. d.).

7ème Conférence des États-parties à la Convention des Nations unies contre la corruption (novembre 2017)

Du 6 au 10 novembre 2017, se tenait à Vienne la 7ème Conférence des États-parties à la Convention des Nations Unies contre la corruption, réunissant plus de 1700 délégués venus d'environ 180 pays. Au cours de cette conférence huit résolutions ont été adoptés, notamment en lien avec le renforcement de la coopération internationale et le renforcement du système de prévention depuis une approche globale et multidisciplinaire (Conférence des États parties à la Convention des Nations Unies contre la corruption, 2017).

61ème session de la Commission des stupéfiants (mars 2018)

La Commission des stupéfiants est l'organe directeur de l'Office des Nations Unies contre la drogue et le crime (ONUDC), qui a pour objectif de guider et d'assister les États dans la mise en œuvre de ses recommandations, notamment par le suivi des mesures prises et la diffusion des pratiques à adopter (Comission on narcotic drugs, s. d.). Cette 61ème session visait essentiellement à rapprocher les perceptions des États, organisations internationales et organisations de la société civile en matière de résolutions relatives à la lutte contre la crise sur les opiacés de synthèse, à la protection des enfants, au renforcement de la prévention en matière de drogues au sein des écoles, aux mesures pour éviter la transmission mère-enfant du VIH et aux préparations au débat ministériel de la Commission en 2019. En somme, elle a permis l'adoption de 11 résolutions ainsi qu'une mise à jour de la classification des substances.

Réunion de haut niveau sur l'évaluation du Plan d'action mondial des Nations Unies pour la lutte contre la traite des personnes (septembre 2017)

Les 27 et 28 septembre, une réunion plénière de haut niveau de l'Assemblée générale des Nations Unies s'est tenue à New-York, afin d'évaluer non seulement les progrès accomplis dans la mise en œuvre du Plan d'action mondial de lutte contre la traite des personnes adopté en 2010, mais également les lacunes et les

difficultés qui ont pu émerger (ONU, s. d.). Dans le cadre de la réunion, la « Déclaration politique sur la mise en œuvre du Plan d'action mondial des Nations Unies contre la traite des personnes » a été adoptée et elle s'engage notamment à mettre fin à l'esclavage moderne.

Concernant la prévention, les États-membres ont souligné l'importance de poursuivre les efforts pour lutter efficacement contre la traite des êtres humains, notamment en s'attaquant aux causes profondes et aux facteurs de développement d'un tel trafic tels que la pauvreté, le chômage, la migration, etc.

Les initiatives régionales, nationales et locales

a) L'Afrique

L'Architecture africaine de paix et de sécurité qui s'occupe de la prévention des conflits, de la gestion des conflits et de la consolidation de la paix au sein de l'Union africaine (UA) a lancé en 2016 sa « **Feuille de route 2016-2020** » [APSA roadmap 2016 – 2020] (APSA, 2016). Cette feuille de route fournit une compréhension partagée des résultats à atteindre par toutes les parties prenantes de l'APSA en mettant en évidence la nécessité d'accroître la collaboration et la coordination. Elle se focalise sur cinq priorités : la prévention des conflits, la gestion des crises et des conflits, la construction de la paix et la reconstruction dans le cas du post-conflit, les thématiques sécuritaires stratégiques, la coordination et la collaboration. C'est notamment dans la quatrième priorité que les enjeux liés à la criminalité sont pris en considération. Dans ce cas, cette priorité est liée aux flux illégaux des armes légères et de petit calibre, au contre-terrorisme, aux flux financiers illicites ainsi qu'au crime organisé transnational et à la cybercriminalité.

La Commission de l'Union africaine a mis en œuvre un plan d'action visant à « **faire taire les armes à feu d'ici 2020** » [Silencing the Guns by 2020], projet vu par la communauté internationale comme une impulsion majeure pour l'Afrique, et en particulier pour les pays qui continuent d'être en proie à des conflits (ISS, 2018). L'institut d'études de sécurité de l'Afrique a identifié trois défis par rapport à ce plan d'action : le financement, le désarmement des communautés fragiles et le maintien de la justice et de la primauté du droit tout au long du processus. Dans la même veine, le Département Paix et Sécurité (PSD) de l'Union africaine a lancé le « **Programme Genre, Paix et Sécurité (2015-2020)** » qui vise à développer des stratégies efficaces pour l'intégration du genre dans la paix et la sécurité, notamment en ce qui concerne la participation effective des femmes en Afrique à ce sujet, la protection en temps de conflit et la reconnaissance publique pendant la phase de post-conflit (Union Africaine - Département Paix et Sécurité, 2016). Ce programme développera un partenariat pour la coordination et la formulation des politiques dans ce domaine entre la Commission de l'Union africaine, l'ONU et les Communautés économiques régionales. Ce plan cherche également à se baser sur la connaissance et la recherche afin de guider l'élaboration de stratégies et de mécanismes à long terme pour répondre à ces priorités.

En 2016, l'ONUDC a lancé le : **Programme Régional 2016-2021** pour l'Afrique de l'est « Promotion de l'État de droit et de la sécurité humaine en Afrique de l'Est » (ONUDC, 2016). Ce plan a pour objectif de poursuivre le renforcement de l'État de droit et de la sécurité humaine dans la région au travers de cinq piliers : la lutte contre la criminalité transnationale organisée et toute forme de trafic, la lutte contre la corruption, la prévention du terrorisme, la prévention de la criminalité, la prévention de la consommation de drogue, ainsi que le traitement et la prise en charge des soins et des troubles liés à la toxicomanie. Chaque pilier est associé à des résultats attendus pour la fin de 2021. Dans le cas du pilier associé à la prévention du crime et la justice pénale, les trois résultats attendus sont associés particulièrement à cette dernière. L'ONUDC attend que les États membres procèdent à des réformes efficaces, économiques et pérennes des institutions judiciaires et maintien de l'ordre, améliorant ainsi l'accès à la justice ; que les États membres mettent en place des processus de justice pénale de meilleure qualité, plus efficaces et empreintes d'équité, notamment pour répondre aux besoins des groupes vulnérables et finalement, que les États membres mettent en place des programmes complets de prévention du crime, de réadaptation et de réinsertion.

b) L'Amérique du Nord

En 2014, le **Réseau pour la réduction de la violence** [violence reduction network] (VRN) a été lancé aux États-Unis (Lopez, 2017). L'initiative vise à permettre aux organismes locaux d'application de la loi de travailler avec les partenaires fédéraux pour identifier les problèmes et mettre en œuvre des stratégies afin de produire des résultats significatifs pour l'ensemble de la collectivité. Des ressources sont ainsi fournies aux organismes locaux, par le biais de programmes de formation et d'assistance technique, et d'outils visant à améliorer le partage de l'information. Selon une évaluation récente, le VRN atteint pour l'instant ses objectifs et répond avec succès aux besoins des services de police tout en améliorant de façon significative la communication entre les organismes locaux et fédéraux dans le domaine de la criminalité. Étant donné les résultats positifs du VRN, le gouvernement fédéral a lancé en juin 2017, sous le mandat du département de justice, le **Partenariat national pour la sécurité publique** [National Public Safety Partnership] (PSP). Le PSP élargit la porte du VRN en permettant de renforcer le soutien dans les enquêtes, les poursuites et la dissuasion des crimes violents, en particulier les crimes liés à la violence armée, aux gangs et au trafic de drogue. PSP permet de faciliter les échanges entre le gouvernement fédéral et les villes afin d'améliorer les stratégies locales de réduction de la violence, basées sur des données probantes et en fonction des besoins locaux.

Suite à la préoccupation grandissante au Canada en ce qui concerne les gangs de rues, le gouvernement fédéral a annoncé en 2017 un nouveau fond qui financera les actions de prévention en termes de **violence liée aux armes à feu et aux gangs**

(Ministère de la sécurité publique, Canada, 2017b). Cette initiative cherche à réunir les

> « efforts fédéraux, provinciaux et territoriaux afin de soutenir les initiatives de prévention; de renforcer l'expertise et les ressources fédérales uniques et d'en tirer parti pour améliorer la collecte de renseignement sur le trafic illégal d'armes à feu; et d'investir dans la sécurité des frontières pour interdire les biens illicites, y compris les armes à feu et les drogues » (Ministère de la sécurité publique, Canada, 2017b, paragr. 2)

Malgré le fait que le « **Plan d'action national de lutte contre la traite de personnes** » vient d'arriver à terme en 2016, plusieurs réalisations ont été accomplies entre 2015 et 2016 (Ministère de la sécurité publique, Canada, 2017a). Tout particulièrement dans le contexte de la prévention, plusieurs campagnes de sensibilisation et de formation ont été lancées, notamment la campagne nationale sur la traite d'Autochtones à des fins sexuelles, ainsi que dans des collectivités rurales, urbaines et du Nord et la campagne de sensibilisation à la traite de personnes à l'intention des jeunes et leurs proches (parents, enseignants et fournisseurs de services) qui cherchaient à leur expliquer les méthodes employées par les trafiquants, ainsi que les effets de la victimisation.

Encadré 1.7. **Répertoire en prévention du crime de Sécurité publique Canada**

Le ministère de la Sécurité publique du Canada vient de lancer un Répertoire en prévention du crime qui permet pour la première fois un accès centralisé national aux programmes de prévention du crime basés sur des données probantes à l'échelle pancanadienne. Ce répertoire dénombre plus 190 programmes évalués et mis en œuvre dans toutes les provinces et territoires du pays et permettra aux chercheurs, aux preneurs de décision et aux intervenants dans le domaine d'avoir accès à une information solide. Le nouveau Répertoire en prévention du crime de Sécurité publique Canada vous permet également de chercher des programmes par sujet, population, emplacement, résultats, etc.

Source : Sécurité publique Canada (2018)

c) L'Amérique latine et les Caraïbes

L'OEA a lancé le **Réseau interaméricain de prévention de la violence et du délit** [Red Interamericana de Prevención de la Violencia y el Delito], suite à la Résolution 2866 de l'Assemblée générale en 2014 (OEA, s. d.). Ce réseau a été créé afin d'établir et soutenir le dialogue, l'échange de connaissances et de pratiques entre les décideurs, les chercheurs, les spécialistes, les représentants du gouvernement, le secteur privé et le grand public dans ce domaine à l'échelle des Amériques.

En 2015, l'Assemblée de l'OEA a adopté la « **Convention interaméricaine sur la protection des droits de l'homme des personnes âgées** » [Convención interamericana sobre la protección de los derechos humanos de las personas mayores], dont l'article 9 concerne directement la violence et sa prévention auprès des aînés. Cette résolution encourage les gouvernements membres à adopter des mesures législatives et de prévention contre la violence faite aux personnes âgées, à sensibiliser et former la population et les fonctionnaires à cette thématique, à promouvoir et renforcer les services de soutien des victimes ainsi que faciliter la dénonciation (Asamblea General, OEA, 2015). L'Assemblée générale en 2016 a adopté la résolution « **Promotion de la sécurité continentale: une approche multidimensionnelle** » [Promoción de la seguridad hemisférica: un enfoque multidimensional], qui a pour but d'encadrer les activités de l'Assemblée en ce qui concerne la sécurité, notamment en matière de prévention du délit et de la violence, la lutte contre le trafic d'êtres humains et d'armes à feu, le crime organisé et la coopération policière (Asamblea General, OEA, 2016). Dans le cadre du « Programme interaméricain de promotion et de protection des droits de l'homme des migrants, y compris les travailleurs migrants et leurs familles » [Programa interamericano para la promoción y protección de los derechos humanos de las personas migrantes, incluyendo los trabajadores migratorios y sus familias], l'Assemblée a souligné l'importance de promouvoir la prévention de la violence et des délits auprès la population migrante. En 2017, l'Assemblée a adopté la résolution « **Promotion de la sécurité continentale: une approche multidimensionnelle** » [Promoción de la seguridad hemisférica: un enfoque multidimensional], laquelle, qui dans la même veine que celle de 2015 encadre le travail en matière de sécurité de l'Assemblée (Asamblea General, OEA, 2017). Dans ce cas, elle a mis l'accent particulièrement sur les délits qui ont une influence sur l'environnement, ainsi que sur l'influence du changement climatique sur la sécurité.

d) L'Asie du Sud-est

L'un des aspects clés dans la région est l'amélioration de la coopération intra-régionale, notamment en matière de crime organisé. Une conférence régionale de haut niveau de l'**Association des nations de l'Asie du Sud-Est (ASEAN)** a eu lieu en 2017 afin de discuter et s'accorder sur des recommandations pour la mise en place effective du « Traité d'entraide juridique en matière pénale » (UNODC, 2017a). Parmi les difficultés retrouvées, les représentants des pays membres ont souligné le manque de compréhension à l'égard du système juridique d'autres pays de la région et l'absence d'un langage standard et une communication faible tant au niveau national qu'entre les pays partenaires.

L'exploitation sexuelle des mineurs est probablement l'un des principaux enjeux de l'Asie du Sud-est, liée également au tourisme sexuel (UNODC, 2014). Le bureau régional de l'ONUDC a lancé en 2014 une série de rapports qui cherchent à améliorer la réponse et la législation des pays concernés dans la région à ce sujet, notamment au Cambodge, au Laos, au Myanmar et au Vietnam. Parmi les recommandations le plus importantes, l'ONUDC a signalé

l'amélioration du service et la réponse de la police, l'amélioration du cadre légal et l'amélioration de la coopération intra-régionale.

L'une des particularités de la région de l'Asie du Sud-est est la grandissante préoccupation concernant **le trafic de la faune et du bois**. Pour répondre à cet enjeu, tout récemment, les pays membres de l'ASEAN se sont réunis à Bangkok pour le lancement d'un réseau **régional de polices** afin d'améliorer les réponses coordonnées à ce sujet (UNODC, 2018).

La région est également très concernée par les problématiques liées aux drogues. En effet, elle est l'une des régions préférées pour la production de drogues synthétiques et de l'opium. Face à ces enjeux, plusieurs pays ont commencé à prendre des mesures afin de combattre cette problématique. Tout récemment par exemple, le Myanmar a lancé une **nouvelle stratégie nationale de contrôle des drogues** (The Republic of the Union of Myanmar, 2018). Cette stratégie est l'une des retombées de la session extraordinaire de l'Assemblée générale des Nations Unies sur le problème mondial de la drogue (UNGASS) en 2016 et cherche à produire un changement significatif de la politique publique vers une approche basée sur des données probantes et de santé publique, tout en préconisant des stratégies concrètes concernant les effets négatifs de la production, du trafic et de l'usage de drogues.

e) L'Europe

Un nouvel **Agenda européen en matière de sécurité** a été élaboré par la Commission européenne pour les années 2015-2020 (European Commission, 2015). Ce nouvel agenda est basé sur cinq principes : a) veiller au respect absolu des droits fondamentaux; b) davantage de transparence, de responsabilité et de contrôle démocratique pour susciter la confiance des citoyens; c) veiller à une meilleure utilisation et mise en œuvre des instruments juridiques en vigueur de l'UE; d) adopter une approche intersectorielle et interagences plus unifiée et e) concilier les dimensions intérieure et extérieure de la sécurité. Sur la base de ces cinq principes, il existe également la volonté et la promotion d'un travail en partenariat ainsi que la coordination des efforts en matière de sécurité. En effet, en termes opérationnels, ce nouvel agenda souligne l'importance d'un meilleur échange d'informations au sein de l'Union européenne, d'une meilleure coordination des opérations sur le terrain, ainsi que donner une place plus importante aux formations, au financement d'actions et à la recherche et l'innovation dans ce domaine. Dans ce cadre, le nouvel agenda priorise trois thématiques à traiter pendant le quinquennat : **le terrorisme, le crime organisé et la cybercriminalité**. Une grande partie des efforts de la Commission européenne en matière de terrorisme et de prévention de la radicalisation est davantage associée à la justice et à la prosécution pénale. Elle a promu, par exemple, la création en 2016 du Centre européen de la lutte contre le terrorisme au sein d'Europol, qui doit travailler en collaboration avec l'agence Eurojust. Elle a également créée l'Unité de signalement des contenus sur Internet (EU IRU) au sein du même organisme policier afin de lutter contre la propagande extrémiste. Un rôle que joue également le Forum européen sur la sécurité urbaine (FESU) dans ce domaine. En matière de prévention, le nouvel agenda promeut l'éducation, la participation des jeunes et le dialogue interconfessionnel et interculturel, ainsi que l'emploi et l'inclusion sociale. Quant au crime organisé, l'un des objectifs est de « désorganiser les réseaux criminels organisés participant à l'immigration clandestine en renforçant les enquêtes transfrontières avec le soutien des agences de l'UE » (European Commission, 2015, p. 19). Trois types de crimes organisés seront priorisés : le trafic d'armes à feu, le trafic d'êtres humains et l'exploitation sexuelle des enfants. L'un des aspects clé à traiter est justement le financement de ces réseaux, souvent associés à la corruption, à la fraude et à la contrebande. Le « paquet anti-blanchiment » cherche en effet à faciliter la détection et le suivi des transferts d'argent. Finalement, dans le cas de la cybercriminalité le nouvel agenda met l'accent sur la mise en œuvre intégrale de la législation européenne en vigueur et sur les efforts de coopération avec le secteur privé.

L'Office européen de lutte antifraude (OLAF) vient de sortir son plan stratégique 2016-2020 (European Commission, 2016). Cet office a pour but de mener des enquêtes indépendantes sur la fraude et la corruption, renforcer la confiance des citoyens dans les institutions de l'UE et développer des politiques de l'UE pour lutter contre la fraude. La prévention est davantage présente dans le troisième point. Dans ce cas, l'OLAF a pour objectifs le développement de la politique et de la législation anti-fraude, la réduction du commerce illicite des produits du tabac et le soutien aux États membres dans la lutte contre la fraude, la corruption et d'autres activités illégales.

Troisième partie : les tendances récentes en matière d'études empiriques sur la prévention de la criminalité

Sur la base d'une revue de littérature effectuée entre les années 2015 et 2017, nous avons pu identifier des études empiriques traitant spécifiquement du sujet de la prévention de la criminalité[5]. Cette revue nous a permis de dresser un portrait de la réalité actuelle sur le sujet, d'un point de vue scientifique. Ces documents scientifiques ont été classifiés à partir de mots-clés et de la zone géographique d'intérêt. Quant aux thématiques abordées, elles sont résumées dans le Tableau 1.4 ci-après :

Tableau 1.4. **Thématiques récentes abordées dans la littérature scientifique (2015-2017)[6]**

Communauté	17
Police	15
Jeunes	14
Violence	10
Prévention situationnelle	9
Autres	7
École	6
Politique publique	5
Sentiment de sécurité	4
Justice Pénale	4
Santé mentale	4
Territorialité/urbain	4
Genre	3
Surveillance	3
Minorité	2
Articulation	2
Prévention tertiaire	2
Famille	2
Crime organisé	2
Drogues	1
Armes	1
Violence domestique	1
Problèmes sociaux	1
Intervention	1
Sécurité	1

Malgré la richesse de la collecte de données et compte tenu des limites en termes d'espace dans ce chapitre, nous nous sommes limités à quatre thématiques qui apparaissent comme les plus importantes pour la recherche empirique actuelle: l'approche communautaire et urbaine, le rôle de la police dans la prévention, l'analyse criminelle et la relation entre les jeunes et la criminalité. Dans certains cas, des articles scientifiques pertinents de 2018 ont également été pris en considération.

ENCADRÉ 1.8. **Les lacunes de l'approche « top down » dans la prévention de la criminalité : l'exemple des territoires palestiniens**

Homel et Masson (2016) expliquent, à partir d'une expérience dans les territoires palestiniens, les lacunes présentes dans les approches « top down » propres aux bailleurs de fonds internationaux, comparativement aux bénéfices des approches « bottom up ». Les approches « top down » sont élaborées depuis l'optique des bailleurs de fonds et des décideurs, sans prendre en considération l'opinion des acteurs locaux. En revanche, les modèles « bottom up » se basent sur l'idée que les stratégies locales doivent se concevoir depuis le terrain en partenariat avec ces acteurs locaux. Dans la première approche, les auteurs indiquent que les insuffisances découlent notamment d'un manque d'appropriation locale ; de la difficulté à gérer les problèmes de gouvernance ; de l'impact de la cooptation d'élites politiques et sécuritaires ; et au fait de négliger les opinions et les besoins des citoyens. En revanche, une approche par le bas utilisée dans les territoires palestiniens s'est révélée être efficace pour résoudre les problèmes de sécurité locaux dans un contexte urbain et de conflit social. Ce processus a commencé avec une consultation publique qui a mené à la conformation d'un comité local de sécurité, dont les membres ont participé à l'élaboration d'un accord de partenariat et à l'élaboration d'un plan d'action local.

L'approche communautaire : entre le partenariat avec la police et les groupes de surveillance communautaire

Une grande partie de la recherche actuelle concernant la relation entre la prévention de la criminalité et la communauté est associée à l'approche communautaire de la police (Gill, Weisburd, Bennett, Telep, & Vitter, 2011). Cette approche a souvent été associée de son côté à une police plus proche et sensible aux besoins de la communauté, ayant une connaissance approfondie du contexte local. La dite approche cherche à améliorer la légitimé de la police et la confiance de la population à son égard. Ce modèle encourage également l'engagement des citoyens dans le maintien de l'ordre (Smith & Scott, 2013). Cet engagement peut impliquer autant la consultation et la participation des citoyens au sein de comités locaux que la participation directe et parfois, le remplacement des actions de la police plutôt que la collaboration locale entre les deux. C'est le cas notamment de travaux de surveillance comme dans le cas du modèle *neighbourhood watch.* La plupart des documents répertoriés ont justement mis l'accent sur cet engagement de la population locale. Un élément intéressant est le nombre important d'articles qui analysent cette problématique dans des régions autres que l'Amérique du Nord.

En Malaisie par exemple, depuis 2007, il existe une approche communautaire qui cherche à établir des partenariats locaux entre la police et les acteurs communautaires (Hassan & Abdullah, 2017). Ishak (2016) analyse la perception d'effectivité de cette approche et révèle que 72,1 % des personnes interrogées considéraient l'action de la police comme efficace pour le contrôle du crime. Il compare également cette approche communautaire aux modèles de « surveillance communautaire » [neighbourhood watch]. Dans ce cas, il démontre que la perception d'efficacité est beaucoup moins importante. De leur côté, Hassan et Abdullah (2017) essayent d'expliquer les facteurs sociodémographiques qui ont une influence sur la participation des Malaisiens dans le comité de soutien à la police communautaire ainsi que les conséquences de cette participation. Le fait d'être un homme, marié, travaillant dans le secteur privé et le fait d'être propriétaire d'un immeuble dans la zone expliquent en grande partie cet engagement. Ceux qui participent au sein de ces comités ont plus de confiance en soi, sont plus conscients de ce qui se passe dans le quartier, se sentent plus utiles à la communauté, et se sentent plus appréciés au sein de celle-ci. Une dernière étude en Malaisie a évalué qualitativement l'utilisation d'alarmes comme moyen de prévention de la criminalité (Lyndon, Selvadurai, Sum, & Abidin, 2017). D'après les résultats, ce système a été corrélé avec une baisse des niveaux de criminalité, ainsi que créernotamment en permettant la création d'un réseau pour le maintien de la sécurité au niveau local, ce qui a favorisé à son tour les relations entre les voisins.

Au Pakistan, une étude a essayé de comprendre comment certaines caractéristiques au sein de deux quartiers ont une influence sur les niveaux de la violence, dans un contexte où l'action de la police est considérée comme inefficace (Aqil, 2016). Parmi les facteurs dentifiés, l'affaiblissement du lien et de la cohésion sociale, le rôle des organisations sociales ainsi que l'absence des lieux de réunion publique sont signalés comme étant importants.

Au Nigeria, Ijimakinwa et ses collègues (2016) ont comparé la capacité de repérage des problématiques liées à la criminalité entre les « groupes de surveillance communautaire » et la police. Ce type de groupe a émergé comme alternative dans un contexte de perception d'inefficacité, de corruption et de brutalité de la police (Ijimakinwa et al., 2016; Ojebuyi, Onyechi, Oladapo, Oyedele, & Fadipe, 2016). Ijimakinwa et ses collègues (2016), concluent que l'engagement communautaire dans ces actions de surveillance peut augmenter la satisfaction envers la police, ainsi que le partage d'informations concernant les crimes et les enjeux de sécurité. Pour leur part, Ojebuyi et ses collègues (2016) analysent plus en profondeur l'efficacité de l'action de ces groupes. Il existe une grande variété au niveau de ces groupes au Nigeria : les groupes de surveillance, les miliciens religieux et ethniques, la sécurité privée, etc. Une grande partie du sentiment de sécurité est associée à l'action de ces groupes. Selon les auteurs, ceci s'explique par une stratégie de communautarisation de la sécurité, où ce type d'organisme est omniprésent dans les espaces publics, a essayé de communautariser les problèmes privés et le rôle l'État en finançant la police (carburant, véhicules, construction de poste de police, etc.), ce qui a facilité la dénonciation et le travail de renseignement.

En Colombie, Bonilla (2016) analyse la perception quant à la participation des citoyens dans la construction de la sécurité et sur l'efficacité de la police communautaire, dans le contexte de réforme de la police en Amérique latine. Cette réforme est associée au processus de démocratisation de la région et ainsi à un rôle plus actif de la citoyenneté (CIPC, 2016a). Dans les résultats, la police communautaire était plus positivement évaluée (77 %) que la police en général (33 %) et était considérée comme plus efficace pour résoudre les problématiques liées à la délinquance à l'échelle locale. Cette évaluation positive s'explique notamment par la perception de réponse rapide et de proximité de cette police. En revanche, seuls 26% considéraient les comités locaux de sécurité comme une instance effective de prévention. Ribeiro et ses collèges (2016) ont réalisé une étude au Brésil pour connaître la perception qu'ont les policiers de la police communautaire. Dans ce cas, la « police communautaire » fait référence à l'action de la police en partenariat avec la communauté. L'étude démontre que la police au Brésil utilise le concept de « police communautaire » pour un large éventail de pratiques qui ne sont pas toujours en lien avec le concept à la base de cette approche : les actions répressives à proprement parler, les groupes de surveillance communautaire, etc. Au contraire, ces pratiques diverses démontrent que la police brésilienne utilise un concept innovateur avec un ensemble de pratiques traditionnelles de contrôle et de répression.

Ces groupes d'articles mettent en avant la tendance vers une approche de communautarisation de la sécurité. Si dans le cas de l'Occident et de l'Amérique latine, cette tendance est associée au travail de coordination et de partenariat avec la police, dans le cas des pays en développement, elle est davantage associée au remplacement du travail de la police par des groupes issus de la communauté elle-même. Dans ce dernier cas, la prévention n'est pas toutefois abordée en tant que telle. Au contraire, ce type de groupe se focalise plutôt sur la surveillance et le contrôle que sur les facteurs à la base de la criminalité, en reproduisant ainsi un modèle de police traditionnel.

Encadré 1.9. **La théorie des « fenêtres brisées » mise à l'épreuve**

Wilson et Kelling (1982) expliquent dans leur célèbre article les principes à la base de la théorie des « fenêtres brisées ». Ils disent que les incivilités sociales (flânerie, consommation d'alcool, etc.) et les incivilités physiques (terrains vacants, bâtiments abandonnés, etc.) incitent les personnes à la peur, ce qui les fait abandonner le quartier. Ce fait facilite la diminution du contrôle informel et l'augmentation du désordre, ce qui attire plus de délinquants potentiels dans la zone et augmente la criminalité. La relation entre les incivilités et le crime a été à la base du modèle de « tolérance zéro » à New

York, cependant la littérature ne fait pas l'unanimité sur ce sujet (A. A. Braga & Welsh, 2016).

Une méta-analyse récente essaie d'évaluer l'efficacité des stratégies policières sur les incivilités afin de réduire le crime (Anthony A. Braga, Welsh, & Schnell, 2015). Cette méta-analyse suggère que ces stratégies sont associées à un effet global statistiquement significatif, mais modeste sur la réduction de la criminalité. Cependant, cet effet global doit être observé en détail. Les interventions communautaires et de résolution de problèmes, conçues pour modifier les conditions de désordre social et physique à certains endroits ont fait preuve d'une grande efficacité pour diminuer les crimes. En revanche, les stratégies agressives de contrôle policier qui ciblent les incivilités individuelles comme dans le cas du contrôle préventif ne génèrent pas de réduction significative de la criminalité.

Dans une autre étude, David Weisburd et ses collègues (2016) analysent l'efficacité de la stratégie policière qui consiste à interpeller, poser de questions ou fouiller [stop, question, and frisks] (SQF) des personnes soupçonnées de commettre des délits, laquelle fait partie de la boîte à outils du modèle de « tolérance zéro ». Cette approche a été fort critiquée en raison du profilage racial. Les policiers ont eu tendance à interpeller les jeunes, les minorités notamment issues de certains quartiers dit « sensibles » (D. Weisburd, Wooditch, et al., 2016). Les résultats indiquent que cette stratégie a un faible effet positif de dissuasion sur la criminalité, particulièrement quand elle est utilisée dans les zones associées aux « hotspots ». Cependant, les auteurs considèrent que le fait d'être efficace dans une certaine mesure, n'implique pas forcément qu'elle soit également efficiente. En effet, sur un total de 700 000 SQF, le crime diminuait à peine de 2%. De plus, cette diminution était associée aux crimes de basse intensité. Par ailleurs, le critère empirique -signalent-ils- ne peut pas être le seul critère à considérer dans une société démocratique, quand ce qui est mis en jeu est également la légitimité de l'action policière et de la police elle-même.

Ces constatations suggèrent que les services de police devraient adopter un «modèle de coproduction communautaire» plutôt que de se tourner vers un modèle de police à tolérance zéro axé sur un sous-ensemble d'incivilités sociales, comme dans le cas de l'arrestation et du contrôle préventif des ivrognes, des adolescents, des itinérants, etc.

L'analyse criminelle comme outil de prévention pour la police

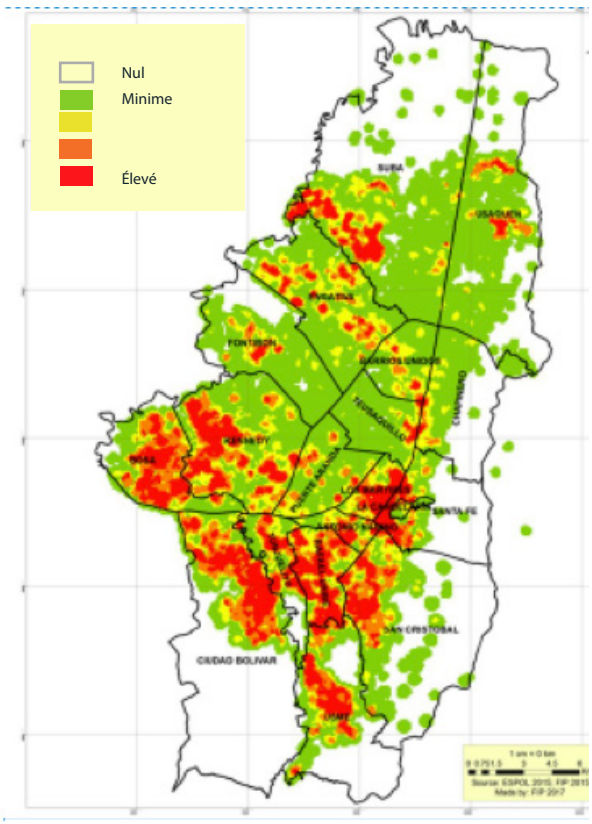
L'analyse criminelle au travers des systèmes d'information géographique a été l'une des révolutions les plus récentes dans le contexte des outils de prévention, notamment dans le travail policier. Ce type d'analyse a permis non seulement d'analyser avec précision la distribution spatiale du crime, mais aussi de parvenir à sa prédiction (Anthony A. Braga et al., 2017). La contribution des Carabineros du Chili à la fin de ce chapitre nous offre une perspective sur ce type d'analyse provenant de l'Amérique du Sud. La recherche indique que le crime se concentre dans des zones spécifiques (hotspots) et non sur l'ensemble d'une ville ou d'un pays (Anthony A. Braga et al., 2017; D. Weisburd, Braga, Groff, & Wooditch, 2017). Une étude récente par exemple, montre qu'au cours des seize dernières années, huit types de crimes présentaient une certaine stabilité en termes de concentration spatiale dans certains segments de rues et d'intersections de la ville de Vancouver (Andresen, Curman, & Linning, 2017). La loi de la concentration des crimes a ainsi modifié le travail policier en adoptant davantage un modèle de patrouilles préventives et intelligentes comme alternative au modèle traditionnel de présence et occupation policière. Ceci a permis de réduire effectivement le crime dans ces zones identifiées (A.A. Braga, Papachristos, & Hureau, 2012; Sherman & Weisburd, 1995; D. Weisburd, Braga, et al., 2017). Cependant, même si cette approche de concentration policière a été effective dans la réduction du crime et que les bénéfices de cette réduction s'aperçoivent également aux alentours des points chauds, il existe très peu d'études qui évaluent l'effet de ces actions sur des zones urbaines larges. David Weisburd et ses collègues (2017) ont démontré que la mise en place de « hotspots policing » a eu également des bénéfices pour les zones urbaines larges en réduisant par exemple de 10% les vols. Dans une autre étude, Sarit Weisburd (2016), s'est posé la question contraire, à savoir si l'affectation fréquente de policiers à des appels 911 en dehors de leur zone de surveillance avait un impact sur la réduction du crime. Elle estime qu'une diminution de 10 % de la présence policière peut augmenter la criminalité de 4,6 w%. Une étude, cette fois-ci aux Pays-Bas, a mis l'accent sur la temporalité du crime (Montoya, Junger, & Ongena, 2016). En effet, le cambriolage pendant le jour et celui pendant la nuit répondent à des facteurs différents. Pendant le jour, le contrôle d'accès et la territorialité[7] expliquent le cambriolage tandis que pendant la nuit, autant le contrôle de l'accès que la sélection des cibles sont les facteurs les plus importants.

L'Amérique du Sud a donné récemment une grande importance à ce type d'analyse. Une étude dans la ville de Bogotá en Colombie montre par exemple l'applicabilité des modèles d'estimation de Kernel pour définir le point de concentration des crimes (Barreras, Dıaz, Riascos, & Ribero, 2016). Une autre étude dans la ville de Montevideo, Uruguay, démontre l'effectivité des caméras de vidéosurveillance sous contrôle de la police pour la prévention des crimes dans les secteurs où ces caméras ont été installées. Un résultat qui va à l'encontre des méta-analyses à ce sujet (Welsh & Farrington, 2007). Cependant, l'analyse démontre que cette efficacité a également produit un déplacement de la criminalité plutôt qu'une diminution.

Encadré 1.10. **Le « hotspot policing » comme outil de prévention pour la police à Montevideo, Uruguay**

L'un des exemples les plus récents de l'application réussie de l'analyse criminelle à l'intérieur de la police dans le but de favoriser la prévention du crime est le **Programme de dévouement intensif** [Programa de Alta Dedicación Operativa] (PADO) de la police de Montevideo, Uruguay (BID & Ministerio del Interior de la República Oriental del Uruguay, 2018). Ce programme s'est basé sur une réforme du système de patrouille qui a impliqué à son tour, un changement organisationnel important basé sur la professionnalisation de la police, la formation continue et l'utilisation de nouvelles technologies. En utilisant le logiciel PredPol pour faciliter la prédiction du crime, la police a réorganisé les patrouilles, qui fonctionnaient auparavant sur une implantation aléatoire sur le territoire, vers des patrouilles intelligentes concentrées sur les points chauds de la criminalité. L'évaluation d'impact du programme a montré que sa mise en œuvre a permis de faire diminuer les vols avec violence de 22 %.

FIGURE 1.1. **Risque de présence de points de vente des drogues illicites à Bogotá**



Source : Escudero & Ramírez (2018, p. 10)

Une grande partie de ces études s'appuient sur la densité des crimes sur une zone spécifique, cependant le crime est le résultat de plusieurs facteurs spatiaux. La modélisation des terrains à risque [risk terrain modelingwv-RTM] permet en effet d'évaluer le poids de ces facteurs sur la criminalité et ainsi d'identifier les zones à risque (Caplan, Kennedy, & Miller, 2011). Ce type d'analyse a été important dans le cas des pays avec un taux peu élevé de criminalité. Au Japon par exemple, Ohyama et Amemiya (2018) montrent que le RTM double la capacité de prédiction d'autres outils. Cet outil a également été utilisé dans le cas des pays avec une haute concentration de crimes. En Colombie par exemple, ce type d'analyse a permis d'évaluer l'effet de la ségrégation socio-économique sur la victimisation par la criminalité violente à Bogotá, en identifiant les facteurs écologiques (Giménez-Santana, Caplan, & Drawve, 2018). Escudero et Ramirez (2018) ont utilisé la même approche dans le cas du marché des drogues illicites dans la même ville. Dans ce cas, ils soulignent l'importance de cet outil pour surveiller et évaluer le marché des drogues et ainsi élaborer des stratégies de prévention adaptées à cette réalité.

Un autre type d'étude a mis l'accent sur d'autres façons d'aborder l'analyse criminelle. En Corée du Sud, une étude a prouvé l'utilité de l'information provenant des appareils électroniques (Internet des objets) pour prédire le risque d'être victime d'un crime dans le cas des piétons, notamment dans le cas du harcèlement sexuel dans la rue (Suh & Song, 2016). Au Japon, Nakamura et Murae (2017) ont évalué l'utilisation des cartes de sécurité, élaborées par des acteurs locaux. Ces cartes cherchent à identifier les sites où un crime est susceptible de se produire et les sites où le crime se produit rarement, ce qui en fait un outil très utile dans le cas de diagnostics locaux de sécurité. L'étude a montré que les cartes de sécurité peuvent améliorer la compréhension des caractéristiques propres aux endroits dangereux ou sécuritaires. Parmi les facteurs clés de l'efficacité de ces cartes, les échanges intergénérationnels et la communication ont été les plus importants.

Jeunes, violence et criminalité

Encadré 1.11. **Stratégies nationales de prévention de la violence chez les jeunes : une étude comparative internationale**

En 2017, le CIPC a réalisé une étude comparative internationale de six stratégies nationales de prévention de la violence chez les jeunes (Afrique du Sud, Canada, Colombie, États-Unis, France et Norvège), dont l'objectif a été d'identifier comment la coordination est assurée lors de la mise en œuvre des politiques de prévention. Cette étude a pu constater que :

- Ces stratégies ont été influencées par un recul des approches préventives larges, dites de prévention sociale ou primaire, au profit d'approches utilisant des activités de prévention très ciblées. De plus, aucun pays considéré n'a mis en place de straté-

gie intégrée de prévention de la violence chez les jeunes.

- Le niveau local a une importance capitale dans le processus de coordination autant dans la mise en œuvre opérationnelle des actions de prévention que dans leur développement. Cependant, il existe une réelle difficulté à coordonner les actions de manière efficace et cohérente à l'échelle locale ainsi qu'entre les niveaux local et national.
- En termes de participation, cette étude nous a permis de souligner le manque de systématisation des processus participatifs incluant un éventail élargi d'acteurs.

Source : CIPC (2017)

Les gangs de rues ont probablement été l'un des plus grands défis de la politique publique de prévention axée sur les jeunes et de ce fait, l'un des sujets les plus traités dans les documents répertoriés. Une étude a voulu analyser l'impact de la trêve avec les « maras » au El Salvador en 2012 sur le taux d'homicide (Katz, Hedberg, & Amaya, 2016). Les résultats ont montré une diminution significative des homicides dans ce pays suite à cette trêve. Dans une autre étude, Huey et ses collègues (2016) ont réalisé une méta-analyse sur les interventions associées aux gangs de rues en Amérique du nord. Dans cette méta-analyse, seules 37% des interventions abordaient la problématique depuis l'angle de la prévention. Plus particulièrement, ces chercheurs s'intéressaient aux effets des interventions sur le comportement antisocial ainsi que sur l'appartenance au gang. Les résultats étaient hétérogènes. Les interventions n'ont pas vraiment eu d'effet significatif sur le comportement antisocial. Pour ce qui est de l'appartenance, l'effet a été faible, même s'il était statistiquement significatif[8]. De leur côté, Sharkey et ses collègues (2017), à partir d'une recherche qualitative, ont dégagé quelques recommandations pour faciliter le désengagement envers les gangs, lesquelles ont été obtenues à partir d'entretiens effectués auprès de jeunes assistant à un programme de probation. Ces recommandations mettaient en avant le besoin d'un travail exhaustif et coordonné avec tous les membres de la communauté (famille, amis, polices, enseignants, etc.). Elles mettaient également l'accent sur le fait que ce type d'intervention ne doit pas forcément cibler uniquement les membres de gangs, mais considérer les besoins spécifiques des jeunes en général.

Encadré 1.12. **Le programme « GREAT » d'intervention sur les gangs de rues : un programme en évolution**

Le programme GREAT (The Gang Resistance Education and Training) est probablement l'un des programmes d'intervention sur les gangs de rues les plus connus à l'échelle mondiale et reconnu pour son efficacité. Cependant, l'un des aspects plus intéressants de ce programme n'est pas son efficacité, mais le fait qu'il a évolué et s'est amélioré au cours de plusieurs processus d'évaluation. Ceci a permis de démontrer qu'une évaluation ne sert pas seulement à déterminer si une mesure est efficace ou non (stratégie noir et blanc), mais aussi à favoriser le processus d'amélioration continue. En effet, le programme GREAT avait été critiqué au départ parce qu'il s'était inspiré d'un autre programme qui fut un échec (DARE), et mal évalué, parce que il n'a pas eu l'effet escompté sur l'appartenance aux gangs, malgré le succès sur d'autres variables (Campie et al., 2017; Esbensen, Osgood, Peterson, Taylor, & Carson, 2013). Une deuxième évaluation a montré des résultats semblables, ce qui a amené le programme à être reformulé afin d'incorporer plus en détail les facteurs de risque associés à l'appartenance aux gangs (Campie et al., 2017). La troisième évaluation a pourtant été positive (Esbensen et al., 2013). En effet, à la suite de la reformulation, le programme s'est avéré avoir un impact sur l'appartenance et sur les relations avec les pairs délinquants.

Une autre série d'études s'intéressait plus particulièrement à la violence des jeunes. Une étude a cherché à évaluer si la « Safe and Successful Youth Initiative » dans l'État du Massachusetts avait eu un impact sur la violence dans les communautés ciblées (Campie et al., 2017). Ce programme travaille avec des jeunes, âgés de 17 à 25 ans ayant un risque avéré de violence, soit parce qu'ils ont déjà commis des crimes soit parce qu'ils font partie d'un gang de rue. L'objectif du programme est de chercher à avoir une influence sur leurs compétences personnelles, leurs expériences relationnelles et sur l'environnement situationnel. À la différence d'autres types d'approches aux États-Unis, ce programme n'utilise pas une stratégie policière agressive. Les dix villes ayant adopté cette intervention ont connu une baisse de 2,8 crimes violents chaque mois pour 100 000 habitants par rapport à trente autres villes de l'État et aussi une diminution entre 5 et 5,7 de victimes de violence chaque mois pour 100 000 habitants, notamment chez les victimes âgées de 14 à 24 ans. Un autre résultat intéressant indiquait que le fait de participer au programme diminuait le risque d'incarcération.

Tableau 1.5. **Facteurs pris en compte dans l'étude de Jennings et ses collègues (2016)**

Facteurs protecteurs	Facteurs de risque
Facteurs individuels	
Sans impulsivité Réussite scolaire Sans maltraitance physique Sans abus sexuel	Attitudes Pro-délinquantes Négligence
Facteurs familiaux	
Relation positive parents-enfants	Pauvreté Chômage du chef de famille
Facteurs concernant les relations entre pairs	
Relation positive avec les pairs	Pairs délinquants
École - quartier	
Climat scolaire positif	Exposition à la violence
Facteurs biologiques	
Retard précoce du développement	Faible poids à la naissance Complication prénatale Complication périnatale
Facteurs culturels	
Sans stress culturel	Acculturé

Source : Jennings et al. (2016)

Jennings et ses collègues (2016) ont étudié les facteurs de risque et de protection par rapport au recours à la violence dans une population de jeunes portoricains âgés entre 5 et 13 ans aux États-Unis. À partir d'une étude longitudinale de trois vagues de collecte de données, ils ont trouvé que l'effet cumulatif des facteurs de risque augmentait entre 18 % et 43 % les chances d'avoir recours à la violence chez les jeunes âgés de 5-9 ans et entre 37 % et 63 % chez les jeunes âgés de 10 à 13 ans. Au contraire, l'effet cumulatif des facteurs de protection jouait un rôle fondamental sur la diminution des chances d'avoir recours à la violence (cohorte 5-9 ans = 19 %-45 % ; cohorte 10-13 ans = 21 %-33 %). Dans les conclusions, les chercheurs ont mis l'accent sur l'importance de la prévention précoce pour prévenir le recours à la violence, notamment dans le cas de la communauté Latina aux États-Unis. Dans la même veine, Souveraine et ses collègues (2016) ont analysé les facteurs associés aux jeunes à risque de devenir des délinquants réguliers en Afrique du Sud.

Les facteurs associés à la délinquance persistante étaient la maltraitance et la violence dans le foyer et dans l'école, et des proches avec des antécédents criminels. La sévérité du crime était également associée aux mêmes facteurs, mais aussi à la victimisation et à la performance et la motivation scolaire. Enfin, l'âge de la première infraction était associé à la maltraitance et la violence dans le foyer ainsi qu'à la violence aux alentours du foyer.

Une méta-analyse a fait une mise à jour de la connaissance concernant l'effectivité des programmes de prévention de délinquance persistante chez les jeunes à risque (de Vries, Hoeve, Assink, Stams, & Asscher, 2015). L'étude montre que ces programmes ont un résultat global positif, mais peu important. Parmi les composantes les plus significatives, les programmes orientés sur le comportement, de modélisation et de contraction comportementale ainsi que ceux focalisés sur la formation des parents ont fait preuve d'une efficacité plus importante. La méta-analyse démontre également que les programmes multi-composants, ainsi que ceux qui se conduisent en dehors du contexte familial sont plus effectifs que les programmes individuels ou en groupe.

Une autre étude a mis l'accent sur les difficultés pour mettre en place un programme de prévention de la délinquance au Chili basé sur des données probantes (Pantoja, 2015). Il s'agissait d'un programme de thérapie multi-systémique pour les familles, soutenu par le sous-secrétariat de prévention du crime. L'auteur souligne que, bien que le programme ait été novateur, plusieurs obstacles ont empêché que sa mise en œuvre soit un succès, notamment un cadre de conditions défavorables et l'absence d'un leadership en matière d'innovation. Une étude qualitative sur la mise en place du programme « Ke Moja » a évalué les défis rencontrés lors de sa mise en application (Khosa, Dube, & Nkomo, 2017). L'objectif de ce programme est de prévenir la consommation de drogues dans les écoles en Afrique du Sud. Les chercheurs ont signalé que malgré le fait que le programme soit considéré comme une réussite, le manque d'appropriation de la part des acteurs locaux, dû à une approche « top down » (voir Encadré 1.8) et une motivation peu élevée à cause des salaires insuffisants des moniteurs, faisaient partie des grands défis du programme.

Encadré 1.13. **Une méta-revue de l'efficacité des programmes de prévention et de réinsertion**

Weisburd, Farrington et Gill (2016, 2017) ont réalisé un bilan sur l'efficacité des programmes de prévention de la criminalité et de réinsertion d'anciens détenus sur la base de 155 revues de littérature dans le domaine. Ils identifient sept dimensions où cette efficacité a été testée :

1. **Prévention et développement social.** Ce sont des programmes définis comme des interventions communautaires visant à prévenir les comportements antisociaux, qui ciblent les enfants et les adolescents jusqu'à l'âge de 18 ans, et qui cherchent à changer les facteurs de risque de l'individu, la famille ou l'école.

   Les résultats sont globalement positifs dans ce type de programme, en effet ils arrivent à réduire la délinquance et l'agressivité. Particulièrement autant les programmes plus intensifs et plus durables que les programmes axés sur les enfants à risque plus élevé ont fait preuve d'une grande efficacité.

2. **Intervention communautaire.** Ces programmes englobent plusieurs stratégies, allant de l'engagement citoyen jusqu'aux interventions pour les jeunes à risque et les services correctionnels et de réinsertion communautaire. Plusieurs programmes dans ce domaine ont fait preuve d'efficacité.

   Les programmes de prévention primaire (mentorat par exemple) se sont avérés efficaces dans ce domaine tandis que dans le cas des programmes de prévention secondaire, les résultats étaient moins consistants. Les programmes qui travaillent sur la reconstruction et l'établissement de liens sociaux avec les jeunes à risque ont montré une grande efficacité ainsi que les programmes correctionnels communautaires qui se concentrent sur les facteurs de risque ou qui relient l'infracteur à la communauté. En revanche, les programmes de dissuasion générale ou de punition ont eu les résultats les plus négatifs, voire contreproductifs.

3. **Prévention situationnelle.** Ces programmes comprennent l'atténuation des vulnérabilités dans l'environnement bâti, ou les moyens de modifier le comportement des délinquants et des victimes afin de réduire la probabilité d'un crime.

   Des mesures telles que l'amélioration de l'éclairage public, les circuits fermés de caméra, les stratégies de prévention de la re-victimisation, la surveillance des quartiers et les mesures de contre-terrorisme ont montré des effets souhaitables sur la prévention du crime.

4. **Maintien de l'ordre.** Ce sont des programmes de formation, d'interventions ou reliés aux activités de la police qui visent à influer sur le crime.

   Les programmes de « hotspots policing », les programmes orientés sur la résolution de problèmes, les patrouilles dirigées pour réduire la violence armée, les approches dissuasives ciblées et l'utilisation de l'ADN dans les enquêtes offrent des résultats positifs dans la réduction du crime. Les programmes de police communautaire augmentent la satisfaction et la perception de la légitimité de la police.

   En revanche, les programmes de seconde réponse ainsi que le programme DARE de prévention de consommation des drogues n'ont pas été d'une grande efficacité.

5. **Sentences et dissuasion.** Ce sont les programmes qui cherchent à évaluer l'effet de la sentence et de la dissuasion sur la prévention de la criminalité.

   Ni la sévérité de la sanction, ni les programmes

généraux de dissuasion n'ont eu d'influence sur la criminalité. Les programmes obligatoires de traitement de la toxicomanie pour les femmes, les tribunaux de la toxicomanie pour les jeunes et la peine de mort ont eu des résultats incertains. En revanche, les peines non privatives de liberté et des interventions judiciaires en milieu carcéral ont contribué à réduire le comportement criminel. Parmi les initiatives prometteuses, on compte les tribunaux de santé mentale et d'autres programmes de santé mentale.

6. **Interventions correctionnelles.** Ce sont des programmes de formation, professionnels, religieux, liés à la toxicomanie, psychosociaux, associés aux délinquants sexuels et à la santé mentale offerts à l'intérieur des prisons.

   Les programmes cognitivo-comportementaux de groupe pour les délinquants en général et pour les délinquants sexuels, les programmes de médicaments hormonaux pour les délinquants sexuels, et les communautés thérapeutiques en milieu carcéral pour les délinquants toxicomanes, ont fait preuve d'une grande efficacité. Les programmes axés sur l'éducation de base et postsecondaire des adultes, ainsi que les programmes de formation professionnelle pour les délinquants en général ont également montré une bonne base scientifique d'appui. En revanche, les thérapies orientées sur les insights pour les délinquants sexuels n'ont pas été effectives.

7. **Traitement de drogues.** Les effets positifs les plus importants et les plus constants ont été observés pour le traitement par la naltrexone et les communautés thérapeutiques. Ces deux types de traitement travaillent tant sur la base de la médication que sur l'intervention sociale et se sont avérés efficaces pour réduire la consommation et la récidive. Le seul programme travaillant exclusivement sur la médication qui a montré un effet prometteur était celui de la substitution par la buprénorphine. D'autres types de programmes de substitution ainsi que d'autres programmes de réintégration et de surveillance ne se sont pas révélés assez concluants.

Conclusion

La première partie, consacrée aux tendances de la criminalité, nous a permis de constater l'énorme variation entre les régions et au sein de celles-ci. Bien que l'Amérique latine demeure la région avec le taux d'homicide le plus important au monde, la violence se concentre dans certains pays de la région et dans certaines villes de ces pays. Un pays comme les États-Unis par exemple qui à l'échelle globale a connu une diminution constante de crimes depuis les années 1990, a des villes avec un taux d'homicide plus important que la majorité des villes en Amérique latine. Ceci est une preuve que la criminalité, notamment le crime traditionnel, doit s'observer et se prévenir principalement d'un point de vue local. Au lieu d'analyser les régions, il faut dans ce cas, analyser les caractéristiques communes aux villes avec des taux élevés de criminalité, ce qui implique le besoin d'une connaissance approfondie et comparable à l'échelle de villes. Les villes en effet deviennent de plus en plus importantes à l'échelle globale et comme telle, l'échelle urbaine devient également un niveau de gouvernance spécifique aussi important que la gouvernance internationale et nationale.

En revanche, l'analyse des initiatives des organismes internationaux met en avance l'importance de la coopération et de la coordination entre les pays et entre les régions du monde, liée notamment à un nombre limité de crimes tels que le crime organisé, le terrorisme, la cybercriminalité, le trafic d'êtres humains, les problématiques liés aux drogues, la corruption, etc. Il s'agit justement de crimes liés à la mondialisation de problématiques criminelles où les frontières ne sont plus une limite à considérer. Le crime organisé en est le meilleur exemple. Les organisations criminelles ont des réseaux d'échanges et des branches dans différents pays et utilisent par exemple les flux migratoires pour faciliter le trafic d'êtres humains, de drogues, etc. Un seul pays ne peut pas à lui seul confronter l'ensemble de la problématique. Il est nécessaire de coordonner les stratégies d'un point de vue de la justice pénale et de la prévention, ainsi que de faciliter un meilleur partage d'informations et encourager une réelle volonté de coopération avec d'autres pays. Nous avons malheureusement constaté que la plupart des initiatives de coopération ont davantage mis l'accent sur la justice pénale que sur la prévention.

Est-il possible de considérer à la fois une approche internationale et locale de la prévention de la criminalité ? À l'œil nu, les deux tendances semblent être contradictoires et dépendantes d'organismes différents. Cependant, comme nous l'avons constaté dans le cas de la cybercriminalité, bien que les criminels agissent au-delà des frontières, les victimes sont pour la plupart locales. Ceci nous fait penser la nécessité de considérer ces deux tendances sous un même angle. Au lieu d'étudier séparément ces deux dimensions, il est de plus en plus urgent de penser le crime aujourd'hui d'un point de vue global. La globalisation est un néologisme anglais qui explique « l'apparition simultanée de tendances universalisantes et particularisantes dans les systèmes sociaux, politiques et économiques contemporains » (Blatter, s. d., paragr. 1). Hobbs (1998) est l'un des premiers à appliquer ce concept à la criminalité à partir du crime organisé, en expliquant comment le crime organisé est modélisé à la fois par l'influence de sa portée internationale et l'action au niveau local. Cependant cette approche peut également s'appliquer aux

crimes traditionnels locaux. Le défi dans un contexte de crimes globaux est ainsi d'analyser les interfaces entre l'échelle internationale et l'échelle locale afin de mettre en place des stratégies de prévention exhaustives. Encore une fois, la coordination entre ces deux dimensions est l'un des grands enjeux de la prévention de la criminalité aujourd'hui.

Contribution

Modèle prédictif

Élaboré par Carabineros du Chili (police) en collaboration avec le Centre d'analyse et de modélisation en sécurité (CEAMOS) de l'Université du Chili

> Avec un taux de précision moyen de 35 %, ce modèle est utilisé principalement dans les postes de police et joue un rôle central dans la définition des trajectoires des patrouilles préventives effectuées par les policiers chiliens dans les grandes villes du pays.

Au Chili, la criminalité est l'un des trois sujets les plus sensibles au sein de la communauté nationale. Pour cette raison et depuis un certain temps maintenant, Carabineros de Chile, la police en uniforme du Chili a adopté une série de mesures visant à améliorer et rendre plus effective la prévention de la criminalité pour les citoyens.

Une de ces mesures a été de décider d'incorporer l'analyse criminelle et sa méthodologie dans les grandes lignes directrices pour le traitement de l'information policière et la prise de décision aux niveaux stratégique, opérationnel et tactique de l'institution armée.

Parmi les nombreux développements que les Carabineros ont entrepris à cet égard, des plateformes technologiques ont été conçues pour appuyer ces mesures, ainsi que pour la diffusion claire et rapide de l'information aux Carabineros en patrouilles préventive sur le territoire. Ainsi, ces plateformes correspondent à des processus d'analyse de l'information sur les réseaux criminels, l'établissement de profils, ainsi que le géoréférencement des crimes parmi les domaines traités par ces outils numériques.

Vers un modèle prédictif

Un des moyens choisis par les institutions de police pour prévenir la commission de délits est la répartition de leurs effectifs dans des lieux précis. Ainsi, la prévention est plus susceptible de fonctionner lorsque les fonctionnaires sont placés efficacement dans des espaces où les criminels ont décidé d'agir à cause d'un manque de présence policière pouvant inhiber ou décourager leurs actions.

Être capable de répartir ses effectifs précisément dans ces lieux est un des principaux défis de la police.

Pour y parvenir, les domaines de recherche consacrés aux questions de prévention de la criminalité partout dans le monde ont développé au fil des ans diverses formules qui, bien qu'elles aient été mises en application avec plus ou moins de succès, ont donné lieu à une base de connaissances sur le sujet.

Dans ce contexte, les Carabineros et le Centre d'analyse et de modélisation de politiques en sécurité (CEAMOS) de l'Université du Chili, ont signé un partenariat de coopération académique et professionnel, dans le but de développer un outil technologique utile pour la planification des services de prévention de la police en uniforme, en fonction des secteurs avec une plus grande probabilité que surviennent certains actes criminels.

C'est ainsi qu'ils sont parvenus à créer un modèle prédictif de la criminalité, qui est actuellement utilisé dans 37 unités opérationnelles de Carabineros de Chile (postes de police) dans la ville de Santiago (capitale nationale) et 22 autres unités réparties dans les grandes villes du reste du pays.

Intégration de trois modèles

Ce modèle consiste en un algorithme développé à partir des trois modèles probabilistes complexes suivants, qui permettent de générer des zones de risque de survenance de crimes sur le territoire, et ainsi faire une prédiction.

- Modèle de prévision Multikernel : il calcule le risque de criminalité par le biais de fonctions spatio-temporelles appelées Kernel dans le but d'identifier quelles sont les périodes de temps qui présentent une plus grande représentativité des signaux étudiés. Pour ce faire, cet algorithme traite deux ensembles de données qui englobent les tendances historiques (données a priori) et les dernières tendances (données a posteriori) de l'activité criminelle.
- Modèle de prospection : il tire son origine du logiciel développé par Kate Bowers, Shane Johnson et Ken Pease de l'University College of London appelé Promap. Il génère une zone de risque sur une base temporelle.
- Modèle Dempster et Shafer ou expert : il se fonde sur la théorie de Dempster-Shafer et la théorie des fonctions de croyances pour calculer les probabilités et obtenir ainsi une zone de risque de crime.

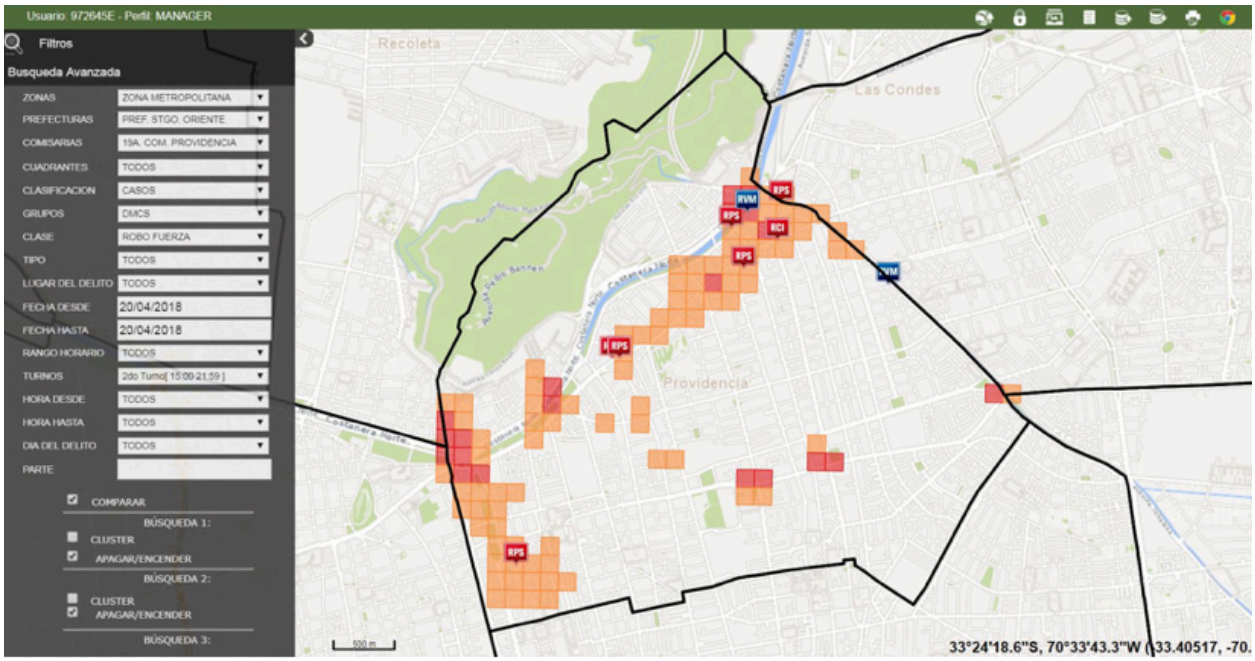
Mises en œuvre

Le développement de ce nouveau modèle a donné lieu à la création d'un logiciel complexe, capable d'indiquer, bien à l'avance, les zones de forte concentration de risque de criminalité pour que le personnel des bureaux d'opérations de chaque poste (responsables de définir les services opérationnels et de répartir les ressources humaines et logistiques) puisse planifier adéquatement les patrouilles préventives.

Ces zones de risque sont classées dans un ensemble de grilles de 150 x 150 mètres, sous les crimes regroupés dans les catégories de « vol avec violence » et « vol à main armée » pour les 5 prochains tours qui seront effectués (tous les matins).

Ce logiciel a été intégré en tant que module au système d'ana-

Figure 1.1. **Capture d'écran du système d'analyse de l'information territoriale SAIT 2.0**



lyse de l'information territoriale SAIT 2.0 qui est la plateforme de géoréférencement et d'analyse de l'information territoriale de Carabineros, pour être utilisé lors du processus de planification des services de prévention et d'identification des priorités pour les patrouilles dans les secteurs où le risque de survenance de certains actes criminels est très élevé.

De plus, ce système de prévision a également été incorporé au sein du système de surveillance et de contrôle des Carabineros SIMCCAR, une plateforme de consultation mobile par le biais d'un assistant numérique personnel (dispositif portable) qui permet au Carabineros sur le terrain d'accéder aux bases de données en ligne des institutions impliquées dans la sécurité, le repérage et la justice, l'information hautement utile pour la réalisation de contrôles préventifs par leurs effectifs.

Parmi les options offertes par ces dispositifs, il y en a une (Applications/Carte) qui permet de visualiser les prédictions sur une carte, en fonction du besoin, de l'emplacement géographique (municipalité) et du type de service recherché par l'usager, pour qui il également possible de voir son propre emplacement sur la carte et de vérifier s'il correspond ou non aux grilles de risque accru.

Enfin, il convient d'ajouter que l'utilisation conjointe des modules SAIT 2.0 de prévision de la criminalité et de contrôle Simccar, permet de surveiller le déplacement des dispositifs dans le territoire, et donc par conséquent d'effectuer des patrouilles et des contrôles préventifs dans les secteurs présentant le plus grand risque de criminalité.

Jusqu'à présent, la mise en application de ce modèle a permis d'atteindre un taux de précision moyen variant de 35 à 40 %.

Figure 1.2. **Plateforme de consultation mobile SIMCCAR**

Contribution

Acteurs émergents de la sécurité et baisse tendancielle des taux d'homicides en Afrique de l'Ouest : cas du Burkina Faso, de la Côte d'Ivoire, du Niger et du Sénégal

Nabi Youla Doumbia
Ph. D en Criminologie, Université de Montréal
Coordonnateur de recherche du projet Homicides en Afrique, Canada

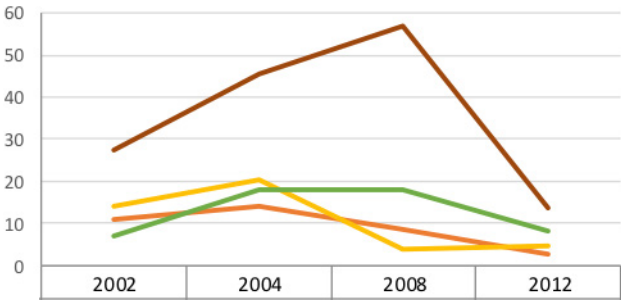
Les homicides ne sont pas une catégorie monolithique. La notion renferme une pluralité de sous-types obéissant à des mobiles différents. En Afrique de l'Ouest francophone, on en dénombre plus d'une dizaine. Les principaux types d'homicides de cette région sont semblables à ceux qu'on retrouve sur les autres continents, à savoir les homicides familiaux, infanticides et meurtre de conjoints; les homicides querelleurs, rixes qui opposent souvent pour des broutilles des amis; et les homicides consécutifs à un autre crime, généralement le vol à main armée et le viol. Ces trois types d'homicides représentent plus de 80 % des cas (Cusson, Doumbia et Yebouet, 2017). L'étude des homicides constitue un angle stratégique d'analyse des problèmes de violence dans une société. En effet, étudier les homicides consiste à étudier toutes les situations-problèmes dont ils constituent le dénouement extrême et tragique ; les prévenir revient donc à empêcher ou perturber le déroulement de ces situations-problèmes : les vols à main armés, la violence conjugale et les bagarres. De plus, les données sur les homicides sont meilleures à celles disponibles sur les autres crimes (Van Dijk, 2008). L'Organisation des Nations unies contre la drogue et le crime (ONUDC) fournit sur la base des causes de mortalité de l'Organisation mondiale de la santé (OMS) des statistiques sur les homicides dans le monde qui permettent d'effectuer des comparaisons entre pays. L'analyse de ces données laisse entrevoir une baisse tendancielle des taux d'homicides dans les quatre pays d'Afrique de l'Ouest analysés ici.

La baisse tendancielle des taux d'homicides

La figure 1 suivante illustre l'évolution du taux d'homicides au Burkina Faso, en Côte d'Ivoire, au Niger et au Sénégal. Les données proviennent de deux sources : Petrini (2010) et ONUDC (2014) pour les données de 2002 et l'ONUDC (2011, 2014) pour les années subséquentes. L'observation du taux d'homicides sur une période de dix ans montre une tendance générale à la baisse dans les quatre pays. Les involutions les plus importantes se sont produites entre 2008 et 2012, sauf pour le Niger où elles ont eu lieu plus tôt entre 2004 et 2008. La baisse la plus spectaculaire se trouve en Côte d'Ivoire. Le taux d'homicide y est passé de 56, 9 pour cent mille habitants à 13,6 pour cent mille habitants, soit une baisse de 43,3 points. La situation de ce pays reste singulière. Entre 2002 et 2011, la Côte d'Ivoire a traversé une situation de guerre civile matérialisée par la partition du pays. La perte de l'autorité de l'État dans les zones rebelles et la désorganisation de l'administration dans les zones sous contrôle gouvernementales ont pu favoriser la résolution violente des conflits privés. L'absence d'organe de justice fonctionnelle a ainsi poussé les individus à se rendre justice eux-mêmes (Doumbia 2018).

Sous réserve de la fiabilité des données, la baisse générale des taux d'homicides dans ces quatre pays révèle l'existence d'une tendance lourde. On peut l'expliquer en partant de la perspective criminologique de l'activité de routine (Cohen & Felson, 1979). Selon cette perspective, un homicide se produit lorsque convergence en un lieu et un moment donné une personne motivée à tuer (tueur) et une personne visée (rival) dans un contexte où il n'y a pas de pacificateur compétent (gardien). Il suffit qu'une de ces trois conditions manque pour empêcher le crime, soit l'absence de motivation à tuer ou l'absence de rivaux ou encore la présence de gardiens compétents. Les raisons qui poussent à tuer diffèrent peu selon les pays. La recherche de la gloire, du pouvoir, des femmes et de l'honneur reste aujourd'hui comme hier les principales raisons de tuer à travers le monde (Cusson, 2015). Les conflits étant consubstantiels à l'espèce humaine une vie sans rivaux est improbable. Sur ces deux coutures on ne peut postuler de différences

Figure 1. **Tendances des homicides en Afrique de l'Ouest**



	2002	2004	2008	2012
Sénégal	11	14,2	8,7	2,8
Niger	14,2	20,2	3,8	4,7
Burkina Faso	7	18,1	18	8
Côte d'Ivoire	27,4	45,7	56,9	13,6

notables entre ces pays. Reste l'absence de gardien, qui correspond à la faiblesse des contrôles sociaux.

C'est évident pour la Côte d'Ivoire, les taux d'homicides exorbitants de ce pays sont liés à la crise politique. La sortie de crise a permis d'améliorer la situation grâce notamment à l'extension du maillage policier et administratif sur l'ensemble du territoire national, concomitamment à la collecte des armes à feu à travers le processus de démobilisation, désarmement et réinsertion (DDR) des anciens combattants. Pour l'ensemble des quatre pays, les inflexions des taux d'homicides peuvent être attribuées en partie à la croissance exponentielle et constante du secteur de la sécurité privée depuis le début des années 2000 (Bryden, 2016). Selon les données de l'observatoire de la sécurité privée, les effectifs du secteur dépassent ceux des forces de sécurité publique. Ils sont par exemple plus de 70 000 en Côte d'Ivoire et plus de 30 000 au Burkina Faso (Observatoire de la gouvernance de la sécurité privée, 2018). À côté de ces acteurs formels, subsistent également des acteurs informels, chasseurs traditionnels, organisations ethniques, parentèle, etc. qui assurent la sécurité (Baker, 2008). Bref, les gardiens peuvent dissuader et empêcher des personnes de voler ou de se bagarrer et partant prévenir les homicides liés à ces faits. Leurs interventions précoces peuvent arrêter l'escalade de la violence entre conjoints, si une prise en charge adéquate du problème suit. Enfin, dernier argument et non le moindre, en étant un des premiers pourvoyeurs d'emplois, la sécurité privée constitue en soi une mesure de prévention sociale. Dans un contexte de crise endémique de l'emploi, ce secteur réussit à arracher de nombreux jeunes à une précarité dont les liens avec la violence sont bien documentés. Toutefois, les taux d'homicides des quatre pays demeurent relativement élevés, supérieurs à ceux des pays européens (1,5 pour 100 mille habitants). Pour les réduire davantage, de nombreux défis existent.

Les défis

Les homicides ne sont pas une fatalité et certaines mesures peuvent réduire sa prévalence. Sur le plan structurel, la lutte contre la pauvreté et les inégalités s'avère incontournable. Il existe en effet une forte corrélation entre ces deux variables et le taux d'homicides (Ouimet, 2012 ; Van Djk, 2008). Pourtant, les indicateurs sociaux ne sont pas reluisants dans ces quatre pays. Le niveau de pauvreté est affligeant dans l'ensemble. La meilleure performance du quatuor est détenue par le Sénégal, qui occupe la 163e place sur 188 pays à l'indice de développement humain (PNUD, 2014). Les inégalités restent élevées : l'indice de Gini varie entre 0,31, le score le plus bas (Niger) et 0,43, le score le plus élevé (Côte d'Ivoire). La perspective prochaine de l'émergence économique de ces pays devrait fournir l'occasion et les moyens d'une plus grande justice distributive.

La recherche de la stabilité politique régionale est plus qu'une urgence, sur le plan conjoncturel. Comme le démontre l'exemple de la Côte d'Ivoire, les conflits politiques ont pour effet d'instaurer une situation d'anarchie qui favorise la privatisation de la justice et la prolifération des facilitateurs des homicides que sont les armes à feu et les stupéfiants. Lorsque l'État s'effondre, la souveraineté et la règle du droit s'éclipsent (Zartman, 1995 ; Rotberg, 2004). De ce point de vue, la zone sahélienne mitoyenne au Sénégal, au Niger et au Burkina Faso est devenue un hub du crime organisé où les terroristes d'Almourabitoun et leurs associés s'adonnent à des trafics de tous genres (ONUDC, 2013 ; Zeïni, 2014). Le contrôle des armes et de la drogue dans les pays de l'Afrique de l'Ouest passe par la pacification des zones aux mains des terroristes.

Sur le plan organisationnel, la prolifération des acteurs de la sécurité privée, formelle et informelle ne va pas sans poser quelques problèmes en regard du respect des droits de l'homme et des prérogatives de la puissance publique. Une meilleure gouvernance de la sécurité basée sur un plan stratégique de prévention incluant les acteurs privés et publics et ordonnant leurs actions autour de quelques objectifs communs pourrait améliorer les rapports entre ces différentes entités et accroître collectivement leur efficacité (CIPC, 2016). De même, l'utilisation des nouvelles technologies de l'information, téléphones portables, Facebook, etc. offre des opportunités pour sensibiliser et éduquer à la non-violence, détecter et signaler les crimes. L'utilisation du portefeuille électronique prive les agresseurs de gains potentiels. Ces outils technologiques ont un potentiel énorme qui n'a pas encore été suffisamment exploité.

Enfin un défi épistémologique. Des études évaluatives sont nécessaires pour améliorer les pratiques (Bowles, Akpokodje, Tigere, 2005 ; World Health Organization, 2014). Tandis qu'émergent de nouveaux acteurs de la sécurité et de nouvelles pratiques dans la région, c'est le cas des Kolweogo, un groupe de vigilance, au Burkina Faso ; ou encore l'Agence d'assistance à la sécurité de proximité (ASP), une agence paraétatique de sécurité privée au Sénégal ; ou encore, la vidéo surveillance du Plateau, le quartier des affaires d'Abidjan en Côte d'Ivoire, peu d'études indépendantes ont été consacrées à l'évaluation de ces différentes initiatives. Pourtant, les meilleures recettes sécuritaires sont celles qui portent la marque des particularismes locaux (Crawford, 2009 ; ONUDC, 2016). Les contextes des États de l'Afrique de l'Ouest ayant de nombreuses similitudes, il serait plus raisonnable de généraliser à l'ensemble de la région des recettes qui ont fait la preuve de leur efficacité dans un de ces pays.

Notes

1 https://issafrica.org/crimehub/facts-and-figures/national-crime

2 https://www.motherjones.com/politics/2012/12/mass-shootings-mother-jones-full-data/

3 La relation entre le taux d'homicide par pays et le pourcentage de femmes victimes d'homicides a une distribution logistique (à partir de données de 2015), c'est-à-dire qu'elle représente une courbe inverse dont la régression explique plus du 40 % de la variance (R^2 = 0,403; f= 29,688; p < 0;05). Ceci permet de conclure qu'il existe une relation inversement proportionnelle entre le TH et le pourcentage de femmes victimes. Plus le TH augmente moins le pourcentage de femmes victimes est important (r= -0.42; p<0,05).

4 Il manquait un nombre important de données qui ont été estimées à partir d'une méthode économétrique d'imputation multiple. Ces conclusions sont le résultat de cette estimation.

5 Cette revue de littérature s'est basée sur deux mots clés («crime prevention» et «community safety») entre janvier 2015 et octobre 2017. Deux moteurs de recherche ont été utilisés : ProQuest et Google Scholar. Après la révision de titres nous avons répertorié 233 documents. Enfin, après la révision des textes, nous avons retenu 65 documents scientifiques.

6 Le nombre total est de 121 plusieurs documents ayant été classifiés sur plusieurs catégories.

7 Selon l'étude, « la territorialité renvoie au sentiment de propriété ou d'appropriation des usagers légitimes qui réduit les occasions de commettre des infractions en décourageant les utilisateurs illégitimes » [Territoriality refers to the legitimate users' sense of ownership or appropriation which reduces the opportunities for offending by discouraging illegitimate users] (Montoya, Junger, & Ongena, 2016, p. 519).

8 « Significatif » veut dire que l'effet a été statistiquement significatif en acceptant un 5 % d'erreur. En revanche la force ou la faiblesse de l'effet est déterminée par la taille de cet effet sur la variable à expliquer. L'effet peut ainsi être parfaitement significatif et faible.

Références

Chapitre 1 : Tendances en matière de criminalité et de prévention de la criminalité

Andresen, M. A., Curman, A. S., & Linning, S. J. (2017). The trajectories of crime at places: Understanding the patterns of disaggregated crime types. Journal of Quantitative Criminology, 33(3), 427–449.

APSA. (2016). APSA Roadmap 2016 - 2020. Addis-Abeba: African Peace and Security Architecture. Consulté à l'adresse http://www.peaceau.org/uploads/2015-en-apsa-roadmap-final.pdf

Aqil, N. (2016). Call for democratic policing: An alternative perspective on crime control in urban neighborhoods of Lahore, Pakistan. Journal of Research in Architecture and Planning, 21(2), 29-39.

Asamblea General, OEA. (2015). Actas y documentos volumen I (No. AG/DEC. 80 (XLV-O/15) AG/RES. 2872 (XLV-O/15) a AG/RES. 2879 (XLV-O/15)). Washington, D.C.: Organización de Estados Americanos.

Asamblea General, OEA. (2016). Actas y documentos volumen I (No. AG/DEC. 81 (XLVI-O/16) a AG/DEC. 94 (XLVI-O/16) AG/RES. 2880 (XLVI-O/16) a AG/RES. 2897 (XLVI-O/16)). Santo Domingo: Organización de Estados Americanos.

Asamblea General, OEA. (2017). Actas y documentos volumen I (No. AG/DEC. 95 (XLVII-O/17) AG/RES. 2898 (XLVII-O/17) a AG/RES. 2914 (XLVII-O/17)). Cancun: Organización de Estados Americanos.

Asian-Barometer. (2008). Asian-Barometer. Wave 2. Taipei. Consulté à l'adresse http://www.jdsurvey.net/jds/jdsurveyAnalisis.jsp?ES_COL=101&Idioma=E&SeccionCol=05&ESID=503

Azrael, D., Hepburn, L., Hemenway, D., & Miller, M. (2017). The Stock and Flow of U.S. Firearms: Results from the 2015 National Firearms Survey. RSF, 3(5), 38-57. https://doi.org/10.7758/RSF.2017.3.5.02

Banco interamericano de desarrollo. (2017). Los costos del crimen y de la violencia: nueva evidencia y hallazgos en América Latina y el Caribe. Washington, D.C.

Banco Interamericano de Desarrollo, & Ministerio del Interior de la República Oriental del Uruguay. (2018). ¿Cómo evitar el delito urbano? El Programa de Alta Dedicación Operativa en la nueva Policía uruguaya. Montevideo: Banco Interamericano de Desarrollo.

Barreras, F., Dıaz, C., Riascos, A., & Ribero, M. (2016). Comparison of different crime prediction models in Bogotá. Bogota: Universidad de los Andes.

Blatter, J. (s. d.). Glocalization. In Encyclopedia Britannica. Consulté à l'adresse https://www.britannica.com/topic/glocalization

Bonilla, M. E. (2016). Community participation in matters of public safety in Bucaramanga and its Metropolitan Area. Présenté à XXIV IPSA World Congress of Political Science, Poznań.

Braga, A. A., Papachristos, A., & Hureau, D. (2012). The effects of hot spots policing on crime. The Campbell Collaboration. https://doi.org/10.4073/csr.2012.8

Braga, A. A., & Welsh, B. C. (2016). Broken Windows Policing to Reduce Crime: A Systematic Review. The Campbell Collaboration.

Braga, A. A., Welsh, B. C., & Schnell, C. (2015). Can Policing Disorder Reduce Crime? A Systematic Review and Meta-analysis. Journal of Research in Crime and Delinquency, 52(4), 567-588. https://doi.org/10.1177/0022427815576576

Campie, P., Petrosino, A., Fronius, T., Read, N., Research (AIR), A. I. for, & America, U. S. of. (2017). Community-Based Violence Prevention Study of the Safe and Successful Youth Initiative: An Intervention To Prevent Urban Gun Violence. Consulté à l'adresse Consulté à l'adresse https://www.ncjrs.gov/pdffiles1/ojjdp/grants/250771.pdf

Caplan, J. M., Kennedy, L. W., & Miller, J. (2011). Risk terrain modeling: brokering criminological theory and GIS methods for crime forecasting. Justice Quarterly, 28(2), 360–381.

CCSPJP. (2018). Metodología del ranking (2017) de las 50 ciudades más violentas del mundo (Seguridad, Justicia y Paz). Mexico D.F.: Consejo Ciudadano para la seguridad publica y la justicia penal. Consulté à l'adresse http://www.seguridadjusticiaypaz.org.mx/biblioteca/prensa/send/6-prensa/242-las-50-ciudades-mas-violentas-del-mundo-2017-metodologia

Chicoine, L. E. (2017). Homicides in Mexico and the expiration of the U.S. federal assault weapons ban: A difference-in-discontinuities approach. Journal of Economic Geography, 17(4), 825-856. https://doi.org/10.1093/jeg/lbw031

CIPC. (2016a). 5e Rapport international sur la prévention de la criminalité et la sécurité quotidienne: les villes et le Nouvel Agenda Urbain. Montréal : Centre International pour la prévention de la Criminalité. Consulté à l'adresse http://www.crime-prevention-intl.org/fr/publications/report/report/article/4e-rapport-international-sur-la-prevention-de-la-criminalite-et-la-securite-quotidienne.html

CIPC. (2016b). La sécurité dans les transports publics terrestres. Montréal : Centre International pour la prévention de la Criminalité. Consulté à l'adresse http://www.crime-prevention-intl.org/uploads/media/Rapport_sur_la_securite_dans_les_transports_publics_FINAL_01.pdf

CIPC. (2017). Stratégies nationales de prévention de la violence chez les jeunes. Une étude comparative internationale. Mon-

tréal: Centre International pour la prévention de la Criminalité. Consulté à l'adresse http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/2017/Strategies_nationales_de_prevention_de_la_violence_Jeunes_Final.pdf

Conférence des États parties à la Convention des Nations Unies contre la corruption. (2017). Rapport de la Conférence des États parties à la Convention des Nations Unies contre la corruption sur les travaux de sa septième session, tenue à Vienne du 6 au 10 novembre 2017 (No. CAC/COSP/2017/14). Vienne. Consulté à l'adresse https://www.unodc.org/documents/treaties/UNCAC/COSP/session7/V1708296f.pdf

Conseil économique et social des Nations Unies. (2017). Tendances et nouveaux problèmes en matière de criminalité dans le monde et mesures de prévention du crime et de justice pénale visant à y faire face (Commission pour la prévention du crime et la justice pénale Vingt-sixième session No. E/CN.15/2017/10). Vienne: Conseil économique et social des Nations unies.

Corporación Latinobarómetro. (2017). Informe 2017. Santiago de Chile: Corporación Latinobarómetro.

Cullen, F. T., Jonson, C. L., & Nagin, D. S. (2011). Prisons Do Not Reduce Recidivism: The High Cost of Ignoring Science. The Prison Journal, 91(3), 48S-65S. https://doi.org/10.1177/0032885511415224

Cusson, M., Doumbia, N. Y., & Yebouet, H. B. (2017). Mille homicides en Afrique de l'Ouest: Burkina Faso, Côte d'Ivoire, Niger et Sénégal. Montréal: Presses universitaires de Montréal.

de Vries, S. L. A., Hoeve, M., Assink, M., Stams, G. J. J. M., & Asscher, J. J. (2015). Practitioner Review: Effective ingredients of prevention programs for youth at risk of persistent juvenile delinquency - recommendations for clinical practice. Journal of Child Psychology and Psychiatry, 56(2), 108-121. https://doi.org/10.1111/jcpp.12320

DuPont, R. L. (2018). The opioid epidemic is an historic opportunity to improve both prevention and treatment. Brain Research Bulletin, 138, 112-114. https://doi.org/10.1016/j.brainresbull.2017.06.008

Esbensen, F.-A., Osgood, D. W., Peterson, D., Taylor, T. J., & Carson, D. C. (2013). Short-and long-term outcome results from a multisite evaluation of the GREAT program. Criminology & Public Policy, 12(3), 375–411.

Escudero, J. A., & Ramírez, B. (2018). Risk terrain modeling for monitoring illicit drugs markets across Bogota, Colombia. Crime Science, 7(1), 3.

European Commission. (2015). The European Agenda on Security. Brussels: European Commission. Consulté à l'adresse https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

European Commission. (2016). Strategic Plan 2016-2020: European anti-fraud office (OLAF). Brussels: European Commission. Consulté à l'adresse https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

European Commission. (2017). Europeans' attitudes towards security (No. Special Eurobarometer 464b). Bruxelles: European Commission.

Fagan, J., & Richman, D. (2017). Understanding recent spikes and longer trends in American murders. Columbia law review, 117(5), 1235–1296.

Gill, C. E., Weisburd, D., Bennett, T., Telep, C. W., & Vitter, Z. (2011). Community-oriented policing to reduce crime, disorder, and fear and increase legitimacy and citizen satisfaction in neighborhoods. The Campbell Collaboration.

Giménez-Santana, A., Caplan, J. M., & Drawve, G. (2018). Risk Terrain Modeling and Socio-Economic Stratification: Identifying Risky Places for Violent Crime Victimization in Bogotá, Colombia. European Journal on Criminal Policy and Research, 1–15.

Global Initiative to End All Corporal Punishment of Children. (2018). Ending legalised violence against children by 2030: Progress towards prohibition and elimination of orporal punishment in Pathfinder countries. London: Global Initiative to End All Corporal Punishment of Children. Consulté à l'adresse http://endcorporalpunishment.org/assets/pdfs/reports-other/Pathfinders-report-2018-singles.pdf

Gouseti, I. (2017). A construal-level approach to the fear of crime. In M. Lee & G. Mythen (Éd.), The Routledge International Handbook on Fear of Crime. Routledge.

Harding, D. J., Morenoff, J. D., Nguyen, A. P., & Bushway, S. D. (2017). Short- and long-term effects of imprisonment on future felony convictions and prison admissions. Proceedings of the National Academy of Sciences, 114(42), 11103-11108. https://doi.org/10.1073/pnas.1701544114

Hassan, M. M., & Abdullah, A. (2017). Perceived effectiveness of community oriented policing implementation in Malaysia: a comparison of socio-demographic factors. International Journal of Engineering Sciences & Research TechnologySilencing the Guns by 2020, 9(6), 15-27.

Hobbs, D. (1998). Going Down the Glocal: The Local Context of Organised Crime. The Howard Journal of Criminal Justice, 37(4), 407-422. https://doi.org/10.1111/1468-2311.00109

Homel, P., & Masson, N. (2016). Partnerships for Urban Safety in Fragile Contexts: The Intersection of Community Crime Prevention and Security Sector Reform. Geneva: Geneva Peacebuilding Platform.

Huey, S. J., Lewine, G., & Rubenson, M. (2016). A Brief Review and Meta-Analysis of Gang Intervention Trials in North America. In C. Maxson & F.-A. Esbensen (Éd.), Gang Transitions and Transformations in an International Context (p. 217-233). Springer, Cham. https://doi.org/10.1007/978-3-319-29602-9_12

ICPC. (2015). Prevention of drug-related crime report. Montreal: International Centre for the Prevention of Crime. Consulté à l'adresse http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/2015/Rapport_FINAL_ENG_2015.pdf

ICPC. (2016). Crime prevention and community safety cities and the new urban agenda: 5th international report. Montreal: International Centre for the Prevention of Crime. Consulté à l'adresse http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/International_Report/CIPC_5th-IR_EN_17oct_Final.pdf

Ijimakinwa, S. O., Arijeniwa, A., Osakede, K., Adesanya, T., Ojo, A., & Abubakar, K. (2016). Community policing and insecurity in Nigeria: a study of coaster community in Ikorodu and Badagry local government area of Lagos state. Review of Public Administration and Management, 5(10), 112-122.

Ishak, S. (2016). Perceptions of People on Police Efficiency and Crime Prevention in Urban Areas in Malaysia. Economics, 4(5), 243–248.

ISS. (2018, mars 14). Silencing the Guns by 2020 – Ambitious but essential. Consulté 24 avril 2018, à l'adresse https://issafrica.org/iss-today/silencing-the-guns-by-2020-ambitious-but-essential

Jackson, J., & Gouseti, I. (2014). Fear of Crime. In J. M. Miller (Éd.), The Encyclopedia of Theoretical Criminology (p. 1-5). Chichester, UK: John Wiley & Sons, Ltd. https://doi.org/10.1002/9781118517390.wbetc130

Jennings, W. G., Gonzalez, J. R., Piquero, A. R., Bird, H., Canino, G., & Maldonado-Molina, M. (2016). The nature and relevance of risk and protective factors for violence among Hispanic children and adolescents: Results from the Boricua Youth Study. Journal of Criminal Justice, 45, 41-47.

Johnson, R. R. (2016). Reducing fear of crime and increasing citizen support for police. Retrieved from Dolan Consulting Group website: http://dolanconsultinggroup. com/wpcontent/uploads/2016/07/Research_Brief_Reducing-Fear-of-Crime-and-Increasing-Citizen-Support_July262. pdf.

Katz, C. M., Hedberg, E. C., & Amaya, L. E. (2016). Gang truce for violence prevention, El Salvador. Bulletin of the World Health Organization, 94(9), 660-666.

Khosa, P., Dube, N., & Nkomo, T. S. (2017). Investigating the Implementation of the Ke-Moja Substance Abuse Prevention Programme in South Africa's Gauteng Province. Social Sciences, 5, 70–82.

Koper, C. S., Woods, D. J., & Roth, J. (2004). An Updated Assessment of the Federal Assault Weapons Ban: Impacts on Gun Markets and Gun Violence, 1994-2003. Philadelphia: National Institute of Justice, United States Department of Justice. Consulté à l'adresse https://www.ncjrs.gov/pdffiles1/nij/grants/204431.pdf

Kreuzer, P. (2016). « If they resist, kill them all »: police vigilantism in the Philippines. Frankfurt am Main: Peace Research Institute Frankfurt.

Levan, K. (2013). Guns and Crime: crime facilitation versus crime prevention. In D. A. Mackey & K. Levan (Éd.), Crime prevention. Burlington, Mass: Jones & Bartlett Learning.

Lewis, D. A., & Salem, G. (2016). Fear of crime: incivility and the production of a social problem. Consulté à l'adresse http://ebookcentral.proquest.com/lib/AUT/detail.action?docID=4540115

Loeffler, C. E. (2013). DOES IMPRISONMENT ALTER THE LIFE COURSE? EVIDENCE ON CRIME AND EMPLOYMENT FROM A NATURAL EXPERIMENT: DOES IMPRISONMENT ALTER THE LIFE COURSE. Criminology, 51(1), 137-166. https://doi.org/10.1111/1745-9125.12000

Lopez, B. (2017). U.S. DOJ Violence Reduction Network Shows Promise in Early Stages. Consulté 23 avril 2018, à l'adresse https://www.nij.gov:443/topics/crime/violent/Pages/violence-reduction-network-evaluation.aspx

Lyndon, N., Selvadurai, S. S., Sum, S. M., & Abidin, N. Z. (2017). The Impact of Crime Prevention Innovation Project Towards a Residential Area: An Analysis from Abductive Research Strategy. Présenté à The 6th International Conference on Social Sciences and Humanities, Malasya.

Ministère de la sécurité publique, Canada. (2017a). Plan d'action national de lutte contre la traite de personnes - Rapport annuel sur le progrès 2015-2016. Ottawa: Ministère de la sécurité publique, Canada. Consulté à l'adresse https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-ctn-pln-cmbt-prgrss-2016/index-fr.aspx

Ministère de la sécurité publique, Canada. (2017b). Violence liée aux armes à feu et aux gangs. Consulté 23 avril 2018, à l'adresse https://www.securitepublique.gc.ca/cnt/cntrng-crm/gn-crm-fr-rms/index-fr.aspx

Montoya, L., Junger, M., & Ongena, Y. (2016). The Relation Between Residential Property and Its Surroundings and Day- and Night-Time Residential Burglary. Environment and Behavior, 48(4), 515.

Nakamura, H., & Murae, F. (2017). Significant education factors in creating local safety maps. Safer Communities, 16(1), 20-31.

OEA. (s. d.). Red Interamericana de Prevención de la Violencia y el Delito. Consulté 23 avril 2018, à l'adresse http://www.oas.org/ext/es/seguridad/red-prevencion-crimen/La-Red

Ohyama, T., & Amemiya, M. (2018). Applying Crime Prediction Techniques to Japan: A Comparison Between Risk Terrain Modeling and Other Methods. European Journal on Criminal Policy and Research, 1–19.

Ojebuyi, B. R., Onyechi, N. J., Oladapo, O., Oyedele, O. J., & Fadipe, I. A. (2016). Explaining the effectiveness of community-based crime prevention practices. A case study from Nigeria. Brighton, UK.

ONUDC. (2015a). Classification internationale des infractions à des fins statistiques. Vienne: Office des nations unies contre la drogue et le crime. Consulté à l'adresse http://www.unodc.org/documents/data-and-analysis/statistics/crime/ICCS/ICCS_French_2016_web.pdf

ONUDC. (2015b). Déclaration de Doha sur l'intégration de la prévention de la criminalité et de la justice pénale dans le programme d'action plus large de l'Organisation des Nations Unies visant à faire face aux problèmes sociaux et économiques et à promouvoir l'état de droit aux niveaux national et international et la participation du public. Doha: Office de Nations unies contre la drogue et le crime. Consulté à l'adresse https://www.unodc.org/documents/congress/Declaration/V1504152_French.pdf

ONUDC. (2016). Promotion de l'Etat de droit et de la sécurite humaine en Afrique de l'Est: Programme Régional 2016-2021. Nairobi: Office de Nations unies contre la drogue et le crime.

Organisation des Nations Unies. (s. d.). Par une Déclaration politique, l'Assemblée générale réaffirme le Plan d'action mondial de l'ONU pour la lutte contre la traite des personnes. Consulté 20 avril 2018, à l'adresse https://www.un.org/press/fr/2017/ag11955.doc.htm

Organisation Mondiale de la Santé. (2017). Campagne mondiale pour la prévention de la violence. Consulté 20 avril 2018, à l'adresse http://www.who.int/violence_injury_prevention/violence/global_campaign/fr/

Pantoja, R. (2015). Multisystemic therapy in Chile: A public sector innovation case study. Psychosocial Intervention, 24(2), 97–103.

Ribeiro, L., Oliveira, V. N., & Diniz, A. M. A. (2016). Los significados de « policía comunitaria » para la Policía Militar Brasileña / The meanings of « community policing » for the Brazilian Military Police. Estudios Sociológicos, 34(102), 603-637.

Roeder, O. K., Eisen, L.-B., Bowling, J., Stiglitz, J. E., & Chettiar, I. M. (2015). What Caused the Crime Decline? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2566965

Sharkey, J. D., Stifel, S., & Mayworm, A. (2017). How to help me get out of a gang: youth recommendations to family, school, community, and law enforcement systems. Journal of juvenile justice, 64-83.

Sherman, L. W., & Weisburd, D. (1995). General deterrent effects of police patrol in crime "hot spots": A randomized, controlled trial. Justice quarterly, 12(4), 625–648.

Shiva Kumar, A. K., & Stern, V. (2017). Ending Violence in Childhood. Global Report 2017. New Delhi: Know Violence in Childhood. Consulté à l'adresse https://www.unicef.org/jamaica/Overview_Report_(High-Res).compressed.pdf

Small arms survey. (2007). Guns and the city. Cambridge: Cambridge Univ. Press. Consulté à l'adresse http://www.smallarmssurvey.org/fileadmin/docs/A-Yearbook/2007/en/full/Small-Arms-Survey-2007-Chapter-05-EN.pdf

Smith, T., & Scott, J. (2013). Policing and crime prevention. In D. A. Mackey & K. Levan (Éd.), Crime prevention. Burlington, Mass: Jones & Bartlett Learning.

Souverein, F. A., Ward, C. L., Visser, I., & Burton, P. (2016). Serious, Violent Young Offenders in South Africa: Are They Life-Course Persistent Offenders? Journal of Interpersonal Violence, 31(10), 1859-1882.

Suh, D.-H., & Song, J.-H. (2016). Establishing Crime Prevention Systems based on Internet of Things and Associated Spatial Urban Factors. Advanced Science and Technology Letters, (139), 45-50.

The Republic of the Union of Myanmar Committee for Drug Abuse Control. (2018). National Drug Control Policy. Naipyidó: Central Committee for Drug Abuse Control.

Union Africaine - Département Paix et Sécurité. (2016). Programme on Women, Gender, Peace and Security. Consulté 24 avril 2018, à l'adresse http://www.peaceau.org/fr/page/80-women-gender-peace-and-security

United Nations Commission on narcotic drugs. (s. d.). Session 61 of the Commission on Narcotic Drugs. Consulté 20 avril 2018, à l'adresse http://www.unodc.org/unodc/en/commissions/CND/session/61_Session_2018/session-61-of-the-commission-on-narcotic-drugs.html

UNODC. (2014). Protecting the Future: Improving the Response to Child Sex Offending in Southeast Asia. Vienna: United Nations Office on Drugs and Crime. Consulté à l'adresse https://www.unodc.org/documents/southeastasiaandpacific/Publications/2015/childhood/2014.08.28.Protecting_the_Future-Responding_to_CSO.pdf

UNODC. (2017a). Improving cross-border criminal justice cooperation in the ASEAN region: conference outcome report and recommendations. Bankok: United Nations Office on Drugs and Crime. Consulté à l'adresse https://www.unodc.org/documents/southeastasiaandpacific//Publications/2017/Summary_Report_of_ILA_Conference.pdf

UNODC. (2017b). World drug report 2017. Vienne: United Nations Office on Drugs and Crime.

UNODC. (2018). New regional network to address wildlife and timber trafficking. Consulté 24 avril 2018, à l'adresse https://www.unodc.org/southeastasiaandpacific/en/2018/03/wildlife-somtc/story.html

UNODC. (s. d.). Session 26 of the CCPCJ. Consulté 20 avril 2018, à l'adresse http://www.unodc.org/unodc/en/commissions/CCPCJ/session/26_Session_2017/session-26-of-the-ccpcj.html

Weisburd, D., Braga, A. A., Groff, E. R., & Wooditch, A. (2017). Can Hot Spots Policing Reduce Crime in Urban Areas? An agent-based simulation. Criminology, 55(1), 137-173. https://doi.org/10.1111/1745-9125.12131

Weisburd, D., Farrington, D. P., & Gill, C. (Éd.). (2016). What Works in Crime Prevention and Rehabilitation: Lessons from Systematic Reviews. New York: Springer.

Weisburd, D., Farrington, D. P., & Gill, C. (2017). What Works in Crime Prevention and Rehabilitation. Criminology & Public Policy, 16(2), 415-449. https://doi.org/10.1111/1745-9133.12298

Weisburd, D., Wooditch, A., Weisburd, S., & Yang, S.-M. (2016). Do Stop, Question, and Frisk Practices Deter Crime? Evidence at Microunits of Space and Time. Criminology & Public Policy, 15(1), 31-56. https://doi.org/10.1111/1745-9133.12172

Weisburd, S. (2016). Police Presence, Rapid Response Rates, and Crime Prevention. Unpublished Working Paper.

Welsh, B., & Farrington, D. P. (2007). Closed-circuit television surveillance and crime prevention: A systematic review. The Swedish National Council for Crime Prevention.

WHO. (2017). Global plan of action to strengthen the role of the health system within a national multisectoral response to address interpersonal violence, in particular against women and girls, and against children. Geneva: World Health Organization, United Nations Office on Drugs and Crime and United Nations Development Programme.

Wilson, J. Q., & Kelling, G. L. (1982). Broken windows. Atlantic monthly, 249(3), 29–38.

Contribution

Acteurs émergents de la sécurité et baisse tendancielle des taux d'homicides en Afrique de l'Ouest...

Baker, B. (2008). Multi-choice policing in Africa. Stockholm: Elanders Gotab AB.

Bowles, R., Akpokodje, J., & Tigere, E. (2005). Evidence-based approaches to crime prevention in developping countries. European Journal on Criminal Policy and Research, 347-377.

Bryden, A. (2016). La privatisation de la sécurité en Afrique. Défis et enseignements de la Côte d'Ivoire, du Mali et du Sénégal. Genève: DCAF.

Centre International pour la Prévention de la Criminalité (CIPC). (2016). 5e rapport international sur la prévention de la criminalité et la sécurité quotidienne: les villes et le nouveau agenda urbain. Montréal: CIPC.

Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 588-608.

Crawford, A. (2009). Crime Prevention Policies in Comparative Perspective. Cullompton: Willan Publisher.

Cusson, M. (2015). Les homicides. Criminologie historique de la violence et de la non-violence. Montréal: Hurtubise.

Cusson, M., Doumbia, N. Y., & Yebouet, H. (Dir. 2017). Mille homicides en Afrique de l'Ouest : Burkina Faso, Côte d'Ivoire, Niger et Sénégal. Montréal: Presses de l'Université de Montréal.

Dijk, V. (2008). The World of Crime. Breaking the Silence on Problems of Security, Justice and Development Across the World. London: Sage Publication.

Observatoire de la gouvernance de la sécurité privée. (2018, Avril 24). http://observatoire-securite-privee.org/fr/content/recherche-données. Récupéré sur http://observatoire-securite-privee.org/fr/

Office des Nations Unies contre la Drogue et le Crime (ONUDC). (2016). Recueil des règles et normes de l'organisation des Nations Unies en matière de prévention du crime et de justice pénale. Vienne: ONUDC.

ONUDC. (2011). Global study on homicide 2011. Vienne: ONUDC.

ONUDC. (2013). Criminalité transnationale organisée en Afrique de l'Ouest. Évaluation des menaces. Vienne.

ONUDC. (2014). Global Study on Homicide, 2013. Vienne: ONUDC.

Ouimet, M. (2012). A World of Homicides: the Effects of Economic Development, Income Inequality and Excess Infant Mortality on the Homicide Rate for 165 Countries in 2010. Homicide Studies, 238-258.

Paré, P.-P. (2013). la police et l'homicide : une comparaison internationale. Dans M. Cusson, S. Guay, J. Proulx, & F. Cortoni, Traité des violences criminelles (pp. 721-740). Montréal: Hurtubise.

Petrini, B. (2010). Homicide Rate Dataset 1995-2008. Washington, D.C.: World Bank.

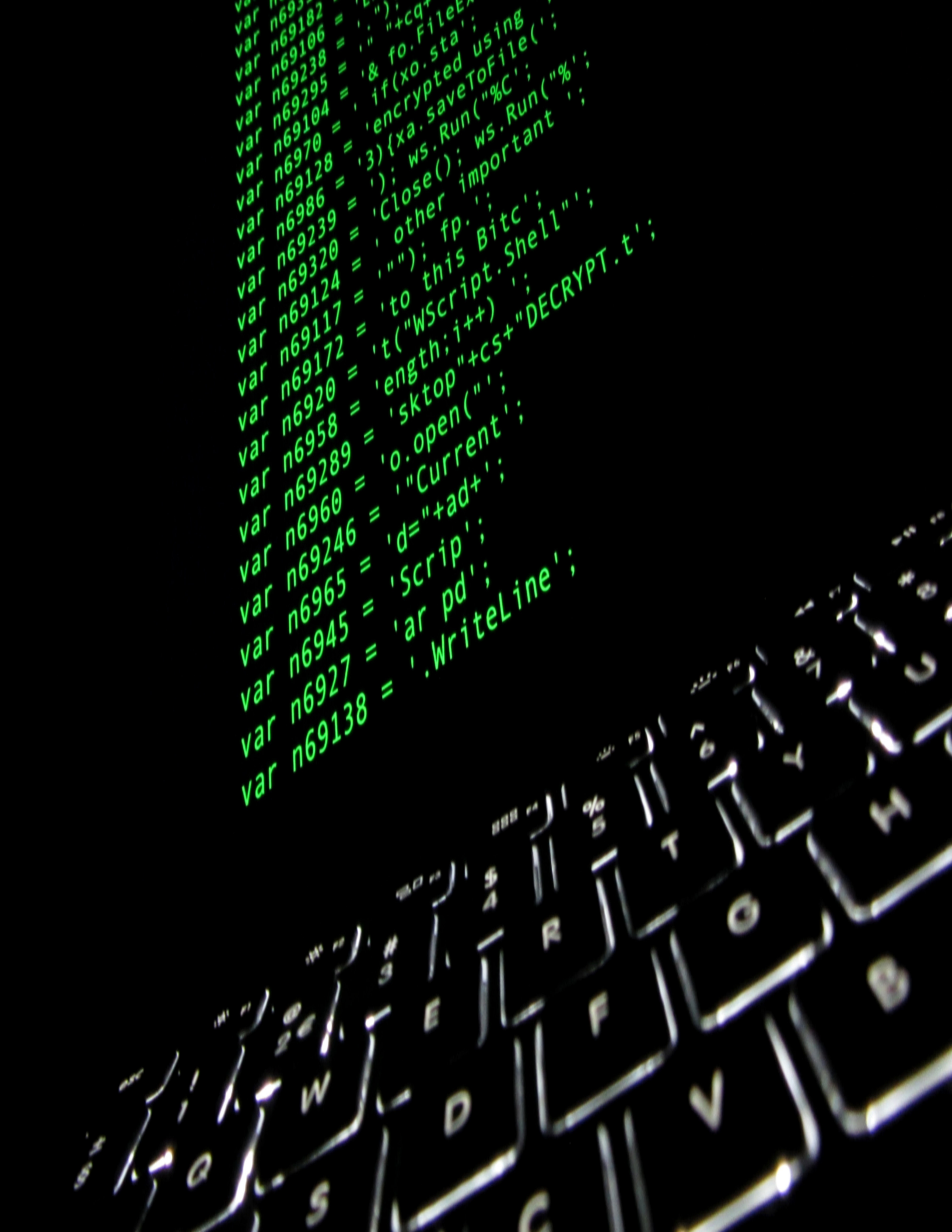
PNUD. (2014). Rapport sur le developpement humain 2014. Genève.

Rotberg, R. (. (2004). When States fails: Causes and consequences. Princeton: Princeton University Press.

World Health Organization (WHO). (2014). Global Status Report on Violence Prevention. Geneve: WHO.

Zartman, W. I. (1995). Introduction : Posing the problem of collapsed states. Dans W. I. Zartman, Collapsed states (pp. 1-11). London: Lienne Rienner Publisher.

Zeïni, M. (2014). La problématique de la criminalité transnationale et le contrôle démocratique du secteur de la sécurité. Bamako: Friedrich-Ebert-Stiftung.


var n69182 = ' : ");
var n69106 = ' " "+cq+
var n69238 = ' & fo.FileEx
var n69295 = ' if(xo.sta';
var n69104 = 'encrypted using
var n6970 = '3){xa.saveToFile(';
var n69128 = '); ws.Run("%C';
var n6986 = 'Close(); ws.Run("%';
var n69239 = ' other important ';
var n69320 = '""); fp.';
var n69124 = 'to this Bitc';
var n69117 = 't("WScript.Shell"';
var n69172 = 'ength;i++) ';
var n6920 = 'sktop"+cs+"DECRYPT.t';
var n6958 = 'o.open("';
var n69289 = '"Current';
var n69960 = 'd="+ad+';
var n69246 = 'Scrip';
var n6965 = 'ar pd';
var n6945 = '.WriteLine';
var n6927
var n69138

CHAPITRE 2

LES CRIMES DANS UN MONDE NUMÉRIQUE

Ce second chapitre tente une problématisation de notre approche des phénomènes de cybercriminalité et se divise en trois volets. Le premier volet ouvre la réflexion autour de la cybercriminalité en s'intéressant à l'environnement spécifique au sein duquel elle s'inscrit, le cyberespace : notamment les dimensions de gouvernance et de facteurs d'inégalités y sont examinées. Le second volet se penche quant à lui sur les difficultés de mesurer la cybercriminalité, des difficultés d'ordre structurel, méthodologique et conceptuel. Enfin, le troisième volet tente, à travers une revue des données et des informations disponibles, d'établir un panorama mondial de la cybercriminalité.

Introduction

En 2017, le géant américain des cotes de crédit personnelles, Equifax, subit un piratage via sa plateforme web : 147,9 millions de personnes aux États-Unis, mais aussi au Canada et en Grande Bretagne, voient ainsi leurs dates de naissance, numéros d'assurance sociale, de permis de conduire ou de cartes de crédit compromis (Sweet, 2018) et potentiellement disponibles sur le Dark Web, la portion du cyberespace non-régulée. Ce sont ainsi 147,9 millions de victimes potentielles de fraude et d'usurpation d'identité qui ont été créées par plusieurs bris de sécurité survenus au courant de l'année 2017, ce qui constitue le plus important vol d'informations personnelles aussi sensibles de l'Histoire. En effet, il s'agit d'un scénario particulièrement sombre, souligne Avivah Litan, spécialiste en cybersécurité interrogée par le journal britannique The Independant : « Sur une échelle de un à dix, c'est un 10 en termes d'usurpations d'identité possibles » (Griffin, 2017). Très médiatisée, cette affaire permet d'identifier plusieurs enjeux majeurs qui illustrent parfaitement la manière dont les activités cybercriminelles nous poussent à remettre en question nos conceptions, nos modes de gouvernance et nos pratiques, sur Internet et dans le monde dit « réel ».

Tout d'abord, le crime : nous ne disposons, à ce jour, que de peu d'informations sur ce qui s'est réellement passé. Et pour cause: l'enquête menée pour déterminer les causes et les modalités de cet événement a été réalisée par Mandiant, une firme de cybersécurité privée, à la demande d'Equifax. Ainsi, l'information disponible au public est très partielle. Nous savons néanmoins que le piratage a été permis par une faille de sécurité du portail informatique, découverte en mars par le département américain de la sécurité intérieure (Department of Homeland Security) et immédiatement signalée à la compagnie, qui assure avoir développé des efforts pour sécuriser la faille (Wattles & Larson, 2017).

Deux observations peuvent être ici faites. D'une part, l'affaire éclaire de manière brutale la vulnérabilité des acteurs (publics ou privés) qui collectent, stockent et utilisent des données personnelles : cette vulnérabilité face au piratage se traduit par une vulnérabilisation des personnes dont les données sont volées. « Equifax, vous aviez une tâche », assène un éditorialiste du New York Times. « Votre seul objectif, comme entreprise, la raison pour laquelle vous avez été créés et qui demeure une préoccupation constante, c'est de collecter et de maintenir les données financières les plus privées des personnes » (Manjoo, 2017). D'autre part, il est nécessaire de souligner que l'enquête a été menée en interne, par une firme privée : ainsi, les autorités publiques sont écartées d'un rôle qui leur revient traditionnellement (faire la lumière sur un crime) et les informations concernant l'événement, dont le nombre de victimes potentielles s'élève tout de même à presque 150 millions de personnes, demeurent gérées par la compagnie impliquée, sous un angle de communications corporatives.

Deuxièmement, l'après-crime et la gestion de la crise : d'après les déclarations d'Equifax suivant l'enquête menée par Mandiant, une série de piratages ont été commis entre mai et juillet 2017, et furent découverts le 29 juillet. Ce n'est pourtant que le 7 septembre qu'Equifax annonce le piratage, ainsi que l'étendue des victimes potentielles, c'est-à-dire plus d'un mois après leur découverte, ce qui pose un problème en soi. Aux potentielles victimes, la compagnie a offert un an de contrôle de leur crédit, mais il revenait aux individus d'effectuer l'ensemble des démarches nécessaires pour sécuriser leur crédit auprès des quatre autres bureaux de crédits les plus importants. Enfin, Equifax conditionnait la divulgation d'informations sur le risque individuel d'exposition au piratage à un abandon, par les victimes potentielles, de tout recours individuel ou collectif contre la compagnie.

Les implications de cette crise et de sa gestion sont nombreuses. Mais soulignons un constat central dès lors qu'on se place dans une perspective de prévention : l'abandon des victimes potentielles et l'absence de responsabilités clairement établies du collecteur de donnée en cas d'incident de sécurité de ce genre. Pour nombre de critiques, cette situation ubuesque est permise par l'indigence des cadres de régulation entourant les incidents de piratage (Turner, 2017).

Troisièmement, les implications pour le futur : elles sont de plusieurs types. La première de ces conséquences concerne la valeur même des types de données : ainsi, une information aussi vulnérable et relativement facile à obtenir ne peut plus constituer un moyen de vérification de l'identité d'une personne. Comme Nathaniel Gleicher, Directeur des Politiques de Cybersécurité de l'administration Obama, soulignait dans un communiqué quelques jours après l'annonce de l'incident : « ce piratage pourrait bien porter le coup de grâce à l'idée que nous pouvons utiliser les identifiants personnels comme les numéros de sécurité sociale comme des facteurs de sécurité » (Pierson, 2017). La seconde de ces implications est juridique : en effet, et de manière plutôt prévisible, plusieurs procédures juridiques sont en cours qui réfutent la clause, très décriée, conditionnant l'accès des potentielles victimes à l'information concernant leur vulnérabilité dans le piratage à un abandon de tout recours possible contre Equifax. Ces poursuites se manifestent notamment par des actions collectives au Canada (Meckbach, 2018) et aux États-Unis

(Harney, 2017), mais aussi à travers d'autres méthodes, comme le recours aux tribunaux de petites créances (Murphy, 2018). Ainsi, il est à attendre que ces procédures permettent d'établir des précédents autour des questions de responsabilités, sur le terrain juridique. Enfin, sur le terrain politique, des évolutions aux États-Unis sont possibles, notamment à travers l'engagement d'élus comme la sénatrice Elizabeth Warren, qui entend utiliser cet événement pour promouvoir un encadrement législatif plus strict des responsabilités liées aux données personnelles collectées par les grandes entreprises. Interrogée par Vox, la sénatrice précisait en février 2018 : « durant des années, Equifax et les autres bureaux de crédit ont pu générer du profit en utilisant les informations privées des gens, et ce, sans leur permission explicite. Nous avons besoin de véritables conséquences lorsqu'ils commettent des fautes » (Stewart, 2018). Parallèlement, Equifax a dû répondre de leur gestion des données personnelles devant le comité du Sénat sur le secteur bancaire, et doivent aujourd'hui collaborer avec plusieurs instances américaines, fédérales et provinciales, afin d'éclaircir non seulement les détails de l'événement de 2017, mais aussi de justifier leurs actions subséquentes. En outre, une proposition de loi, portée par les sénateurs démocrates Warren et Warner, vise à : 1) clarifier les responsabilités de ces géants de la donnée ; 2) établir des sanctions en cas d'incidents dus à des défauts de sécurité ; 3) créer un organisme fédéral de supervision de la cybersécurité en charge, notamment, de surveiller les pratiques des bureaux de crédit et ; 4) encourager l'investissement du secteur privé dans la cybersécurité (Stewart, 2018).

Cette affaire Equifax illustre donc très bien l'ensemble des grands enjeux qui entourent aujourd'hui la manière dont nous faisons face à la cybercriminalité. Notre **vulnérabilité** en tant qu'individus ou en tant qu'organisations de très grande envergure, publiques ou privées. La **pauvreté des cadres de compréhension, de régulation et de gestion** qui entourent les pratiques développées dans le cyberespace, y compris les pratiques impliquant des informations extrêmement sensibles. Le manque de clarté des responsabilités respectives des acteurs. La **gouvernance polycentrique**, où les autorités publiques ne jouent plus le rôle de garant, d'arbitre et de protecteur des individus et des organisations. Enfin, la nécessité de développer des approches innovantes pour gouverner le cyberespace, prévenir la cybercriminalité et protéger les victimes, potentielles ou avérées.

Ce premier chapitre s'attachera donc à effectuer un tour d'horizon de « ce que l'on sait » de la situation actuelle du cybercrime. Tout d'abord, nous reviendrons sur le cyberespace comme environnement très singulier et tenterons d'identifier celles de ses caractéristiques qui influent le plus sur la manière dont la cybercriminalité et la cybervictimisation vont s'y développer : notamment, nous nous attarderons sur les questions d'inégalités d'accès, de compétences et d'usages. Ensuite, nous prendrons une vue d'ensemble géographique de la cybercriminalité qui, faute de données pertinentes, consistera plus en un panorama des informations disponibles. Enfin, nous examinerons plus en détail les implications principales et les enjeux majeurs, dans une perspective de prévention.

Le cyberespace : gouvernance, inégalités et implications pour la criminalité

Le cyberespace est un système formé des interactions entre des objets connectés, des interactions qui peuvent prendre la forme de transferts de données ou d'informations : il est ainsi à la fois virtuel et physique (Malecki, 2017). L'essor d'Internet dans l'ensemble des sphères de la vie moderne constitue l'un des aspects du processus de globalisation des échanges et de l'avènement de ce que le sociologue Manuel Castells nomme « l'âge de l'information » (Castells, 2002). Plusieurs accélérations ont été observables dans la croissance du cyberespace : la démocratisation des accès à Internet, l'essor de l'accessibilité mobile à travers les téléphones intelligents et, plus récemment, la multiplication des objets connectés.

Ce cyberespace constitue bien plus qu'un support ou une extension du monde dit « réel » : il forme un environnement propre, aux caractéristiques spécifiques. Selon la chercheure Wanda Capeller (2001) ce changement d'environnement implique que les activités déviantes et criminelles qui s'y développent le font à la fois en continuité avec le monde réel (les activités illégales investissent le cyberespace et s'y adaptent) ou bien en discontinuité (des activités criminelles naissent des opportunités présentées par ce nouvel environnement). En conséquence, une des clés pour comprendre la cybercriminalité est de comprendre le fonctionnement du cyberespace et de ses caractéristiques, au premier rang desquelles sa gouvernance, c'est-à-dire le système des acteurs et des modalités qui conditionnent sa régulation. Celle-ci gravite autour de trois types d'acteurs essentiels : ceux qui développent, exploitent et administrent les infrastructures physiques permettant la connexion des appareils et le stockage des données connectées, ceux qui fournissent les accès au cyberespace et ceux qui offrent les services en permettant les usages les plus importants (stockage de donnée, réseaux sociaux, plateformes de contenu, cybersécurité).

Cette gouvernance remet directement en cause le paradigme westphalien de la centralité de l'État, ainsi que les concepts et notions clés qui lui sont traditionnellement attachés, tels que l'État de droit, la sécurité, les frontières, les droits humains et la souveraineté, une situation encore complexifiée par les rapides avancées technologiques et leurs conséquences sur l'accès, les usages et la gouvernance du cyberespace : conséquemment, les institutions étatiques peinent à s'adapter et à offrir des solutions efficaces (Liaropoulos, 2017).

En ce sens, le cyberespace se prêterait plutôt à une gouvernance, qui transcenderait les États westphaliens et les frontières traditionnelles, pour se placer dans l'optique d'une gouvernance globale au sens d'un modèle de prise de décision coopératif où acteurs étatiques et non étatiques doivent s'associer pour faire face à des défis qui débordent le cadre de leurs actions individuelles (Finkelstein, 1995). Au cœur de ce modèle, le cyberespace doit alors retrouver les acteurs centraux précédemment cités et qui relèvent, pour la plupart, du secteur privé.

C'est ce point, tout particulièrement, qui recèle pour la prévention de la cybercriminalité des implications cruciales. En effet, le cyberespace a été formé, dès ses débuts, à la fois comme une réalité d'échanges et comme un projet politique libertaire, exprimé en 1996 dans la Déclaration d'Indépendance du Cyberespace et qui rejette toute intervention ou contrôle étatique (Electronic Frontier Foundation, 1996). Cette utopie libertaire fonde nombre des représentations à la base même des nombreux débats actuels sur la gouvernance du cyberespace, où l'idée de régulation par les pouvoirs publics se voit opposer une conception fondée sur la notion de bien commun.

Pourtant, avec la démocratisation des accès et des usages, ce sont les grands acteurs privés qui ont, par leur capacité à offrir ces accès et les outils permettant ces usages, concentrés l'essentiel de la prise de décision et de la gouvernance : l'utopie libertaire est devenue une réalité capitaliste. En outre, ces acteurs privés sont localisés, ainsi que leurs infrastructures, au sein d'États et, ainsi soumis, dans une certaine mesure, à leur juridiction. Par conséquent, le projet d'une gouvernance multi-acteurs au sein de laquelle la représentation, les intérêts et l'importance de l'ensemble des usagers et des parties prenantes seraient équitablement répartis demeure un défi majeur, encore loin de faire consensus, et moins encore de constituer une réalité (Liaropoulos, 2017; Pereira, 2016).

Cette gouvernance concentrée par un groupe d'acteurs restreint implique alors plusieurs enjeux majeurs en termes de cybercriminalité et de cybersécurité :

- Comment les acteurs privés, centraux dans la gouvernance du cyberespace, y envisagent-ils la sécurité de tous, notamment celle des plus vulnérables (particuliers, groupes vulnérables, victimes) ?
- Comment les priorités en matière de lutte contre la cybercriminalité sont-elles déterminées, notamment entre les crimes relevant de l'atteinte aux intérêts des acteurs privés et ceux relevant de l'atteinte aux personnes, surtout les plus vulnérables (pédopornographie, violences faites aux femmes, crimes haineux, etc.) ?
- Comment intervenir dans les cyberespaces non régulés par les principaux acteurs privés ou publics (aussi communément appelé Dark Web) ?
- Comment adapter la politique publique et la régulation législative, deux outils essentiels pour la lutte contre la criminalité et la prise en charge des victimes, aux réalités du cyberespace et de ses acteurs ?
- Comment développer des partenariats entre les secteurs étatiques et privés afin de garantir la sécurité de tous et toutes, de manière équitable et dans un objectif collectif ?
- Comment enfin garantir les droits essentiels, individuels et collectifs, tels que la liberté d'expression et les libertés politiques ?

Afin de mieux comprendre les liens entre cyberespace et criminalité, il convient donc de se pencher d'abord sur cette transition entre mondes réel et virtuel : comment s'opère-t-elle et quelles en sont les conséquences dans les phénomènes criminels? De nombreuses pistes s'offrent pour tenter de répondre à cette question. Nous choisirons ici de prendre une perspective de prévention, qui cherche ainsi à déterminer des relations entre les activités criminelles et un ensemble de facteurs les favorisant, au premier rang desquels les questions d'inégalités.

Cyberespace et inégalités

Loin de l'idéal d'accessibilité et de démocratisation qu'incarne Internet, le cyberespace est en effet un lieu d'inégalités, parmi lesquelles on soulignera les questions d'accès, de compétences et de sécurité. Ces trois facteurs sont essentiels lorsqu'on s'intéresse à la cybercriminalité, tant du point de vue de ses auteurs que de celui de ses victimes.

Stansbury (2003) distingue quatre inégalités principales : l'inégalité d'accès, l'inégalité de compétences, l'inégalité des opportunités économiques et l'inégalité de participation démocratique, qui influent alors, selon l'auteure, la manière dont les individus utiliseront le cyberespace. D'autres auteurs préfèrent une typologie ancrée dans la théorie de l'appropriation des ressources technologiques, qui distingue quatre dimensions configurant les types d'accessibilité : la motivation, l'accès physique et matériel, les compétences et les usages (Dijk, 2012). Ces inégalités sont aussi appelées « fractures numériques », un terme mis au pluriel pour en souligner l'aspect multiforme et multifactoriel. Au départ de ce terme, la première fracture numérique se forme autour des questions d'accès (Warschauer, 2004), la seconde autour de celles de compétences (Hargittai, 2011) et la troisième autour des usages (van Dijk & Hacker, 2003).

L'état actuel des connaissances et le corpus de littérature sur ces questions est, comme tout ce qui touche aux questions liées au cyberespace, encore embryonnaire et en cours de développement. Pour autant, la question des fractures numériques et de leurs liens avec les facteurs d'inégalités du monde dit « réel » fait l'objet d'une recherche très dynamique. Afin d'en illustrer les grandes avenues, nous avons choisi ici de nous pencher plus particulièrement sur la première fracture numérique, soit la plus documentée. La deuxième et la troisième ne seront ainsi décrites que très brièvement, avant d'analyser la relation existant entre l'ensemble de ces fractures et la cybercriminalité.

La première fracture numérique : l'accès au cyberespace

Tout d'abord, soulignons que l'accès même au cyberespace est profondément inégalitaire, en tout premier lieu pour des raisons technologiques : sans infrastructures de réseau et sans appareil pour se connecter, le cyberespace demeure hors de portée. Ainsi, les différents types d'accès, depuis la ligne à haut-débit jusqu'aux données mobiles, en passant par les cyber-cafés ou les accès publics, comme l'école, forment

un ensemble hétérogène d'accessibilité différenciée : cette « fracture numérique » n'est donc pas tranchée entre ceux qui ont accès et ceux qui ne l'ont pas, mais regroupe un ensemble complexe de situations d'accès plus ou moins aisé (Warschauer, 2004).

Ainsi définie comme les conditions plus ou moins aisées d'accès au cyberespace, cette fracture numérique reflète la plupart des facteurs d'inégalité classiques que l'on retrouve dans le monde dit « réel ». Le niveau de développement, la condition sociale et économique individuelle, l'âge, le genre, la place dans l'espace public, l'accès aux services, le niveau d'éducation, sont autant d'indicateurs intéressants à considérer dans l'accessibilité au cyberespace.

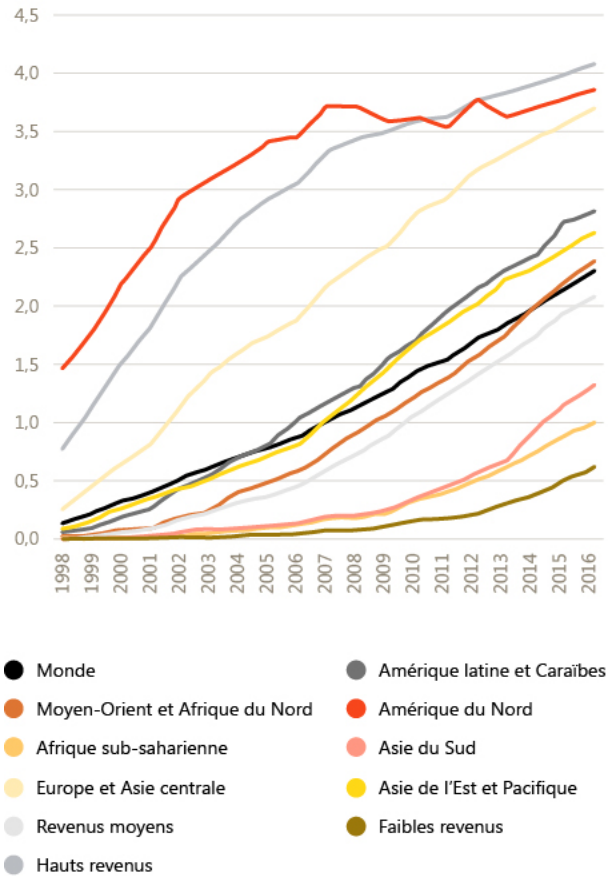
En outre, ces facteurs sont aussi déterminants dans les processus délictueux « classiques », aussi bien pour les auteurs que pour les victimes (CIPC, 2005, 2010, 2011, 2012a, 2012b). Aussi, il est capital, afin d'aborder la prévention de la cybercriminalité, d'envisager les facteurs d'inégalité caractéristiques du cyberespace.

1. Fracture numérique et inégalités de développement

Les inégalités macro-économiques ont très largement conditionné la manière dont l'accès au cyberespace s'est développé à travers les pays. Dimension constituante du phénomène de mondialisation, Internet en suit les grandes dynamiques, notamment dans la différentiation de son développement. Ainsi, Internet est né et s'est développé d'abord dans le monde occidental et les pays les plus riches, suivant ensuite les grands canaux de la mondialisation : l'urbanisation et le développement économique, le second point étant illustré par le graphique ci-dessous.

Plusieurs constats peuvent être tirés de la lecture du graphique précédent. Tout d'abord, l'essor de l'accès au cyberespace, au tournant des années 2000, loin de combler les inégalités qui existaient entre pays aux différents niveaux de développement économique, les a renforcées : les pays les moins avancés économiquement, notamment en Afrique subsaharienne et en Asie du Sud, sont demeurés à l'écart de cette révolution technologique. En effet, si l'on observe une croissance plus récente de

Graphique 2.1. **Évolution du taux de pénétration d'Internet par agrégats de pays géographiques et économiques**



Source: Banque Mondiale (2017)

leur accès à Internet, notamment due à l'essor des accessibilités mobiles, leur taux de pénétration accuse un retard significatif. Ainsi, selon l'Union Internationale des Télécommunications, 17,5 % des habitants des pays les moins avancés avaient accès à Internet en 2017, contre 6 % en 2012 (International Telecommunication Union, 2017c).

Un second constat intéressant à poser est celui de l'ancienneté : ainsi, les internautes des pays occidentaux et des pays les plus riches ont une pratique plus longue du cyberespace, qui a donc été développé et modelé par eux et pour eux. Ceci est particulièrement important vis-à-vis de la seconde vague d'accessibilité, qui a ouvert le cyberespace au monde émergent, c'est-à-dire aux classes moyennes des économies émergentes à forte croissance et, dans une moindre mesure des pays les plus pauvres.

Ainsi, si l'on revient à la question des conditions et des caractéristiques posées par ce nouvel environnement « cyber », cette première fracture numérique pose non seulement la question de l'accès, mais indirectement aussi, à travers les différentes temporalités de celui-ci, celle de l'appropriation, des usages et des compétences, c'est-à-dire qu'elle conditionne directement la seconde fracture numérique.

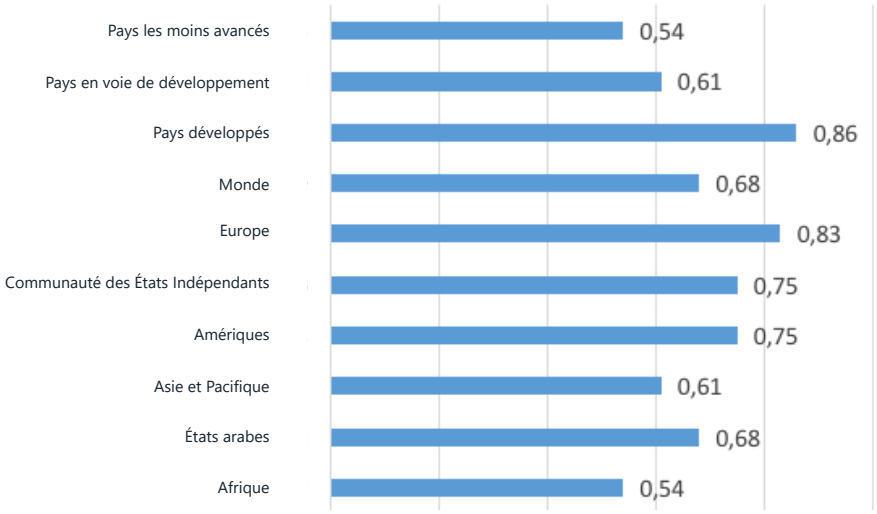
2. Fracture numérique et inégalités sociales et économiques

Alors que les inégalités d'accès s'observent de manière flagrante au niveau international, ce constat ne doit pas, cependant, masquer celles à l'œuvre au sein même des sociétés et des pays. Si les inégalités socio-économiques constituent des dimensions absolument centrales dans les approches criminologique et sociologique classiques, il est très intéressant de constater que la littérature scientifique qui s'intéresse à leurs expressions dans le cyberespace tendent à montrer qu'elles influencent de manière beaucoup plus complexe et indirecte les accès, compétences et usages (van Deursen & van Dijk, 2013).

Ainsi, on peut souligner que plusieurs études menées dans des pays occidentaux riches concordent à suggérer que les classes économiques les moins favorisées ont un usage plus intensif d'Internet (Fuchs, 2009). Notamment, les enfants et les jeunes issus de milieux moins favorisés ont un usage plus soutenu d'Internet que les autres, ainsi qu'une supervision moins présente, ce qui renforce des inégalités préexistantes, notamment dans leurs chances de succès scolaire (Camerini, Schulz, & Jeannet, 2017). Ceci est particulièrement crucial pour comprendre les liens entre facteurs socio-économiques et cybercriminalité, car un milieu défavorisé économiquement, un manque de supervision des temps libres et un risque accru d'échec scolaire pourrait indiquer un renforcement des facteurs de risque de criminalité.

Il faut toutefois nuancer ce constat, car il dérive surtout d'études appliquées aux pays les plus riches et où les questions d'accès se posent avec moins d'acuité. Dans les pays du monde émergent et de ceux les moins avancés économiquement, le poids des déterminants économiques et sociaux demeure encore important dans l'accès, les compétences et les usages du cyberespace (Fuchs & Horak, 2008). On notera de même l'importance capitale de la distinction urbain/rural dans ces questions (Alzouma, 2013), qui rappelle le point précédemment évoqué : la mondiali-

Graphique 2.2. **Rapport entre le taux de pénétration d'Internet chez les 15-24 ans et leur part dans la population totale**



Source : International Telecommunication Union (2017c)

sation et ses caractéristiques, dont l'accès démocratisé au cyberespace fait partie, s'exprime dans le monde en développement d'abord et avant tout dans les territoires urbains.

3. Fracture numérique et attributs sociodémographiques

Si les facteurs économiques constituent des conditions importantes dans la formation des fractures numériques, d'autres types de facteurs y jouent un rôle non moins important, parmi lesquels les questions générationnelles, le genre, l'éducation, le handicap, l'appartenance à une minorité, etc. Nous nous pencherons ici sur quelques-unes de ces dimensions : 1) la relation entre les jeunes et l'essor du cyberespace, notamment dans les pays émergents ; 2) le facteur du genre dans l'accès à Internet et ; 3) les liens complexes entre niveau d'éducation, compétences et usages du cyberespace, et vulnérabilité.

La révolution numérique et l'avènement du cyberespace sont souvent perçus comme une question générationnelle entre les « natifs » technologiques et leurs aînés : les dynamiques à l'œuvre sont en fait plus complexes et font intervenir un éventail de facteurs en interrelation (Helsper Ellen Johanna & Eynon Rebecca, 2013). Une de ces nuances à apporter réside, par exemple, en une différenciation des contextes, notamment en termes de développement économique. La figure ci-dessous vise à mettre en lumière l'importance des jeunes générations dans le cyberespace en fonction du niveau de développement économique.

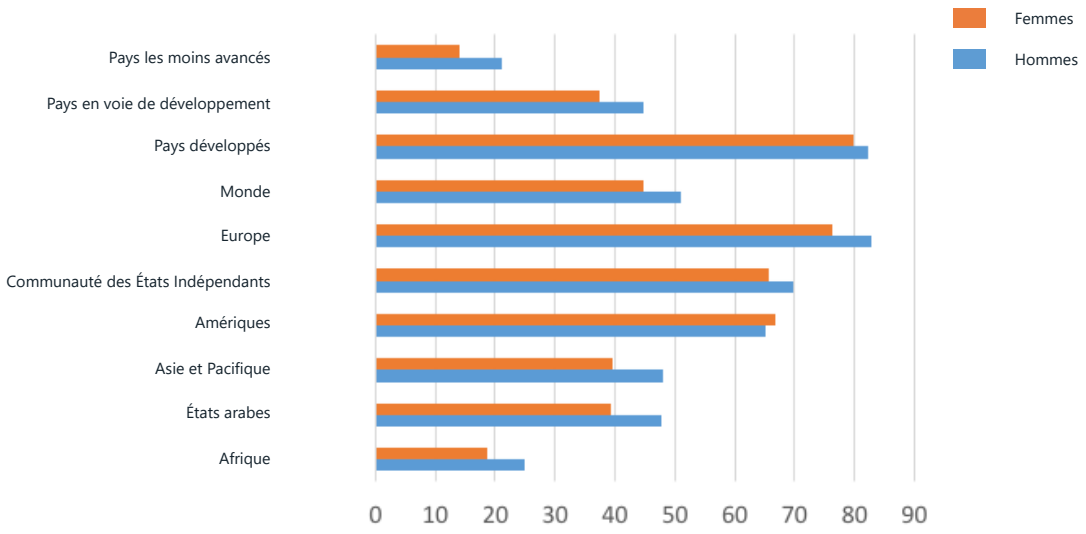
On s'aperçoit alors qu'au sein du monde en développement, ce sont les plus jeunes qui ont investi, en majorité, le cyberespace, alors que cet écart générationnel est moins marqué dans les pays les plus riches et les plus connectés. On remarque que les pays les moins avancés, notamment dans les continents africain et asiatique, ont une proportion d'usagers d'internet particulièrement jeune.

Pour autant, l'essor de l'accès au cyberespace chez les jeunes, notamment dans le monde en développement, demeure lui aussi profondément inégalitaire : 94 % des 15-24 ans des pays développés sont des usagers d'Internet, contre 67 % dans le monde en développement et seulement 30 % au sein des pays les moins développés (International Telecommunication Union, 2017b). La perception souvent véhiculée d'une « génération M » ultraconnectée ne concerne-t-elle donc que les jeunes des pays les plus riches, leurs homologues du monde émergent faisant encore face à un accès inégal et inégalitaire.

En outre, si les jeunes constituent le cœur de la révolution apportée par le cyberespace, ce changement de paradigme défavorise les plus âgés : pour les pays de l'OCDE, le taux de pénétration d'Internet est de 95 % pour les 16-24 ans, pour seulement 63 % des 55-74 ans (OCDE, 2017). Cependant, les plus grandes inégalités générationnelles ne s'observent pas entre cette génération M occidentale et leurs aînés, mais bien dans le monde émergent.

Ces facteurs générationnels doivent être compris en association avec une autre grande dimension des inégalités, celle du genre.

Graphique 2.3 **Taux de pénétration d'internet par genre et par pays**



Source : International Telecommunication Union (2017)

La figure ci-dessous montre l'accès différentié entre femmes et hommes en fonction des grandes régions mondiales et des niveaux de développement.

Encore ici, le constat s'impose d'une répercussion dans le cyberespace des inégalités de genre observées dans le monde dit réel, à l'exception notable du continent américain. Les différences les plus marquées se retrouvent également, comme dans les questions générationnelles, au sein du monde émergent et des pays économiquement moins avancés. Ce constat confirme le précédent et indique que les inégalités réelles ont un impact plus significatif dans ces régions où la fracture numérique s'exprime avec le plus d'acuité.

La seconde et la troisième fracture numérique : inégalités de compétences et d'usage

Ces inégalités réelles se retrouvent également autour des dimensions de compétences et d'usages : autrement dit, à accès équivalent, les internautes font face à des facteurs d'inégalité quant à leurs capacités de compréhension et de maîtrise des outils technologiques, ainsi qu'à la manière dont ils naviguent au sein du cyberespace, des activités qu'ils y développent et des outils qu'ils y emploient (van Dijk & Hacker, 2003). Au sein de chacune de ces formes de fracture numérique, les facteurs d'inégalité précédemment évoqués (développement économique, inégalités sociales et économiques individuelles, éducation, genre, âge) s'expriment aussi, un sujet qui a fait l'objet de plusieurs études récentes.

Par exemple, van Deursen et van Dijk (2010) ont mis en lumière l'importance déterminante du niveau d'éducation dans l'acquisition des compétences nécessaires à tirer pleinement bénéfice des opportunités offertes par l'accès à Internet. De leur côté, Blank et Lutz (2016) tentent de dépasser la question des inégalités d'accès aux bénéfices pour inclure celle de l'exposition aux dommages (harm) : de manière intéressante, leur étude montre une plus grande exposition aux dommages pour les internautes les plus éduqués et ceux qui se préoccupent le plus des questions de privauté dans le cyberespace que pour les autres catégories, notamment les internautes moins technologiquement avancés. Cette corrélation entre un niveau de connaissances et d'usages plus élevé et une plus grande vulnérabilité au cybercrime est non seulement observée pour les individus, mais aussi pour les organisations et les États : en effet, souligne Speer (2000), les États qui s'appuient le plus sur les technologies de l'information et de la communication pour leur fonctionnement sont aussi ceux qui sont le plus exposés aux risques de cybervictimisation.

Cyberespace, inégalités et cybercriminalité

Aussi, comme le souligne Majid Yar,

> « Internet ne doit pas être vu comme un simple élément technologique, une sorte de « page blanche » qui existerait en dehors des personnes qui l'utilisent. Il est plutôt nécessaire de le considérer comme un ensemble de pratiques sociales : Internet prend une forme particulière parce que des personnes en font des usages particuliers, pour des raisons spécifiques » (Yar, 2006, p. 6).

Aussi, on observe que le cyberespace constitue une réalité propre, aux caractéristiques spécifiques. Les caractéristiques du monde réel ont une influence sur la manière dont les usagers investissent le cyberespace, et, par conséquent sur les facteurs influençant cybercriminalité et cybervictimisation. Pour autant, cette influence est indirecte, et il est ainsi nécessaire de reconstruire l'approche d'analyse et de compréhension des phénomènes cybercriminels en prenant en compte cet environnement spécifique qu'est le cyberespace.

La question se pose alors de savoir comment ces fractures numériques et ces facteurs d'inégalités s'expriment dans les phénomènes cybercriminels : autrement dit, les facteurs sociaux, culturels, économiques et politiques à la base des inégalités d'accès, de connaissance et d'usage du cyberespace ont-ils une influence déterminante sur les trajectoires des auteurs et des victimes de cyberdélinquance? Par exemple, les jeunes, qui investissent massivement le cyberespace, sont particulièrement vulnérables face à la cybercriminalité. Or, l'on sait que, concernant la criminalité dans le monde réel, victimisation et perpétration sont des processus intimement liés, surtout chez les jeune: ainsi, la victimisation et l'exposition à des activités criminelles et violentes constitue un facteur de risque important dans le développement de tels comportements (Margaret Shaw, 2001; WHO, 2015). Une hypothèse qui émerge donc est celle d'un lien entre une accessibilité au cyberespace accrue chez les jeunes et un risque supérieur face à des processus de victimisation/perpétration.

Bert-Jaap Koops (2010) propose une perspective sur les facteurs de risques centrée, quant à elle, sur les opportunités produites par les caractéristiques intrinsèques du cyberespace : autrement dit, il cherche non plus à répondre à la question de savoir comment les facteurs du monde « réel » influencent le développement d'activités criminelles dans le cyberespace, mais plutôt comment le cyberespace fournit les opportunités à de telles activités. De cette réflexion, le chercheur introduit alors douze facteurs de risque : la globalité, la déterritorialisation, la flexibilité des réseaux, l'anonymat, l'interaction à distance, la possibilité de manipulation des données, l'automatisation des processus, les effets d'échelles, l'agrégation et la multiplication de petits larcins, l'économie de l'information, les limitations structurelles aux garde-fous classiques (contrôle social, surveillance), ainsi que la rapidité des cycles d'innovation.

Il est ici important de souligner que la recherche demeure encore embryonnaire autour des relations entre inégalités du monde dit « réel », inégalités dans le cyberespace (les fractures précédemment évoquées) et phénomènes de cybercriminalité

(Kigerl, 2012, 2016) et cybervictimisation (Halder & Jaishankar, 2016 ; Jaishankar, 2011 ; Jaishankar & Halder, 2011), notamment en ce qui concerne les cyber-violences et la victimisation des groupes les plus vulnérables (Nicola Henry & Anastasia Powell, 2016).

Cette question, centrale dans l'approche criminologique actuelle, demeure aujourd'hui une zone « frontière » des chercheurs, ce qui, tant du point de vue de la connaissance comme de celui de l'action pour prévenir la cybercriminalité, constitue l'enjeu majeur auquel sont confrontés les preneurs de décision, une problématique sur laquelle se penchent plus en détail les troisième et quatrième chapitres.

Définir et mesurer la criminalité à l'heure du cyberespace

La définition même de la cybercriminalité est aujourd'hui un débat essentiel de la science criminologique (Yar, 2006). Globalement, deux approches sont proposées, qui proposent chacune une perspective épistémologique radicalement différente sur la nature même de la criminalité dans le cyberespace : la première soutient que cet espace virtuel constitue un miroir du monde physique, permettant ainsi une adaptation des grandes théories criminologiques, tandis que la seconde plaide pour une approche nouvelle de la cybercriminalité, alors considérée comme un phénomène singulier (Stratton, Powell, & Cameron, 2017). Les débats et les explorations dont fait l'objet la cybercriminalité dans le champ de la science criminologique forment un aspect sur lequel se penche le troisième chapitre du présent rapport.

Pour autant, et si la science criminologique se trouve encore confrontée aux défis fondamentaux de définition qu'impliquent un champs d'étude totalement nouveau, l'urgence et l'importance des phénomènes criminels cristallisés autour du cyberespace exigent que les pouvoirs publics prennent les devants et définissent les cadres de leur réponse. Tout particulièrement, l'une des implications majeures des phénomènes cybercriminels réside en une redéfinition radicale des notions de lieu et de la relation entre l'auteur et la victime. Ainsi, dans le cyberespace, un acte illicite commis par une personne physique, résidant à un endroit donné du monde réel, peut être dirigé envers une (ou des) victime(s) se trouvant dans un lieu totalement différent. En termes d'enquête et de procédure juridique, ceci signifie que plusieurs juridictions se trouvent de facto impliquées et doivent, pour permettre une réponse efficace, se coordonner de plusieurs manières : 1) par la coopération de leurs services de police et de justice et 2) par l'harmonisation de leurs cadres juridiques (Grabosky, 2004).

Face à cette urgence, les institutions internationales jouent un rôle fondamental dans la constitution d'une définition communément acceptée et qui puisse soutenir aussi bien le développement des cadres nationaux que celui d'une souhaitable réponse internationale. L'Office des Nations-Unies contre la Drogue et le Crime (UNODC) souligne que la notion de cybercriminalité regroupe un ensemble d'actes disparates plus qu'elle ne décrit un type précis d'offenses. Deux grandes approches se présentent alors pour l'acteur public : 1) une définition restrictive axée sur l'objet (actes visant l'ordinateur et son contenu) et 2) une définition inclusive axée sur le modus operandi (actes impliquant, dans leur totalité ou partiellement, l'utilisation d'objets électroniques connectés). Dans son rapport de 2013, l'UNODC recommande, à des fins de lutte contre la cybercriminalité, d'en adopter une définition inclusive afin de permettre une adaptation aisée des cadres législatifs et juridiques aux rapides évolutions technologiques qui la caractérisent (UNODC, 2013). Cette problématique ne sera pas envisagée dans ce chapitre, mais abordée en profondeur dans le chapitre suivant. Il convient pour l'heure de se concentrer sur les données, autre enjeu majeur en ce domaine.

Mesurer la cybercriminalité : une mission impossible ?

La première difficulté à mesurer la cybercriminalité est double : tout d'abord, l'activité et les acteurs formant le cyberespace constituent un système hypercomplexe lui-même impossible à mesurer objectivement. Ensuite, l'activité cybercriminelle elle-même est souvent difficilement détectable, même par les victimes d'actes délictueux (Cobb, 2015).

La seconde difficulté pour la mesure de la cybercriminalité tient à la gouvernance même du cyberespace : multipolaire, atomisée et en grande partie a-structurée. Ceci entraîne plusieurs implications majeures : 1) la prédominance des acteurs privés dans la production de données sur la cybercriminalité, 2) la place périphérique des pouvoirs publics dans la collecte et la production de ces données et 3) l'ampleur des chiffres noirs et des occurrences non signalées.

Globalement, deux grands types de sources sont disponibles pour faire un état des tendances observées au niveau mondial. La première catégorie regroupe les acteurs privés, majoritairement les grandes entreprises et bureaux de conseils œuvrant dans le domaine de la cybersécurité (Norton, Symantec, PwC, Ponemon, McAfee entre autres). Ceci oriente leur contenu vers : 1) les problématiques rencontrées par leur clientèle-cible, notamment le secteur privé et 2) des types de crimes spécifiques visés par leurs activités de cybersécurité, comme le vol de données, les différents types de piratage et d'intrusion, ainsi que la fraude. Plusieurs auteurs soulèvent toutefois des doutes sur l'exactitude des données collectées et sur la transparence des motivations de ces grandes firmes de cybersécurité dans la production de ce genre de rapports (Levi, 2017). La seconde catégorie de sources est constituée des agences gouvernementales (par exemple, le FBI américain), multigouvernementales (comme Europol) ou internationales (UNODC, entre autres). Ces études, bien que généralement plus ciblées géographiquement et moins nombreuses que les précédentes, sont précieuses car elles couvrent un plus grand éventail

d'activités délictueuses, parmi lesquelles l'exploitation sexuelle, la cyberviolence, le crime organisé, le cyberterrorisme ou les cyberviolences. Il est intéressant de noter que ces deux catégories d'études accordent une place grandissante aux enquêtes de victimisation et aux sondages sur les usages et le sentiment de sécurité dans le cyberespace.

La problématique principale qui s'impose dans la mesure de la cybercriminalité est que le cybercrime est massivement sous-rapporté et sous-comptabilisé, ce qui implique une prédominance des « chiffres noirs », c'est-à-dire que la grande majorité des actes délictueux et criminels commis dans le cyberespace n'entrent dans aucun type de mesure (Yar, 2006). Comme le souligne Freyssinet,

> « aucune étude statistique fiable ne permet aujourd'hui de mesurer l'ampleur des phénomènes cybercriminels, que ce soit à cause des problèmes de définition (…) ou de la faible propension des victimes à porter plainte (…) Ainsi, la progression éventuelle des statistiques officielles (…) ne saurait être interprétée comme une augmentation significative du nombre de ces faits, mais plutôt comme une meilleure prise en compte collective de ces problèmes» (Freyssinet, 2010, p.28)

En outre, plusieurs obstacles se posent au signalement des actes de cybercriminalité, notamment auprès des institutions gouvernementales. En ce sens, la question du vol de données, souvent sous forme de quantités massives d'informations personnelles recueillies par les acteurs privés sur les usagers de leurs services, constitue l'un des points épineux du signalement de cybercrimes. Une des raisons en réside dans le fait que la collecte de telles données, ainsi que les responsabilités des entreprises sur les questions de sécurité liées auxdites données, restent encore peu encadrées. Ainsi, les entreprises auront tendance à ne pas divulguer ces informations, d'une part pour préserver leur réputation et, de l'autre, pour se protéger contre d'éventuels recours de clients indirectement lésés par le vol de données les concernant (Pereira, 2016). À l'heure actuelle, ces délits sont très difficiles à évaluer : on estime par exemple que 80 à 90 % des cyberattaques menant à des vols de données ne sont pas signalés (Medina & Molist, 2017).

Jusqu'ici, rares sont les pays ayant adopté des législations obligeant les acteurs privés à signaler des actes de piratage et de vol de données dont ils sont victimes. Les États-Unis et l'Union européenne ont adopté des textes dans ce sens, obligeant notamment à signaler l'occurrence d'incidents de ce type aux individus dont les données sont susceptibles d'avoir été compromises. Le Canada, pour sa part, devrait voir ce genre d'obligation entrer en vigueur au cours de l'année 2018 (Connolly, 2018).

Pour d'autres types de cybercrimes, notamment ceux visant les usagers individuels (tels que, par exemple, la fraude par hameçonnage[9] et rançongiciel[10]), on note un manque de mécanismes facilitant le signalement par les particuliers, notamment sous forme de ligne d'appel ou de mécanisme en ligne. En outre, la classification même des actes signalés prête à confusion, puisqu'il n'existe pas de classification harmonisée des actes relevant de la cybercriminalité : ainsi, chaque pays aura sa propre typologie et souvent, à l'intérieur même d'un pays donné, l'enregistrement d'un délit relevant de la cybercriminalité sera attribué à une autre catégorie dite « traditionnelle » comme la fraude (UNODC, 2013).

Outre la mesure des incidents et les enquêtes de victimisation, une dernière approche pour mesurer la cybercriminalité est de tenter d'en évaluer le coût économique. L'avantage principal de ce choix réside en sa capacité à rendre compte, même de manière approximative, de l'impact de ces activités dans le monde réel. Pour autant, les difficultés méthodologiques et opérationnelles de ce genre de mesure sont telles qu'il semble impossible de se fier aujourd'hui à l'une de ces évaluations (Gañán, Ciere, & van Eeten, 2017). En effet, l'hypercomplexité des activités cybercriminelles et de leurs impacts sur les économies impliquent des limites majeures : 1) l'identification et la circonscription des effets à mesurer (notamment la prise en compte ou non des coûts liés à la sécurité), 2) la collecte de données fiables et 3) les méthodes d'analyse. Une étude récente menée par une équipe de recherche de la fondation RAND montre bien les considérables variations des estimations en fonction des différentes approches envisagées (Dreyer et al., 2018). En 2014, le Centre pour les études stratégiques et internationales estimait le coût total de la cybercriminalité entre 375 et 575 milliards de dollars (Center for Strategic and International Studies, 2014). Microsoft avance, pour 2017, le chiffre de 500 milliards de dollars et la firme de cybersécurité McAfee celui de 600 milliards pour 2018 (Chalfant, 2018).

Une tentative de typologie des tendances de la cybercriminalité

En termes de cybercriminalité, les tendances annuelles sont d'abord et avant tout renseignées par les rapports produits par les grandes firmes de cybersécurité, et concernent donc les activités délictueuses qui affectent, en premier lieu, le secteur privé. Les types d'activités couverts par ces rapports sont essentiellement liés à l'évolution des technologies et des modus operandi. Ainsi, les activités délictueuses en expansion en 2017 et qui, selon toute vraisemblance, seront très dynamiques en 2018 incluent les techniques de piratage (d'appareils, de données et de comptes), les logiciels malveillants, les rançongiciels, les différents types de fraude et d'usurpation d'identité, ainsi que, notamment depuis 2017-2018, l'essor des fausses nouvelles et du microciblage (Deutsche Telekom, 2017).

Ce constat est corroboré du côté des usagers individuels par l'enquête menée annuellement par la firme Norton, qui relevait, en 2017, que, parmi les 44% de leurs clients individuels interrogés ayant été victimes d'activités délictueuses au cours de

l'année précédente, les activités criminelles et délictueuses les plus fréquemment rapportées étaient, en ordre d'importance : l'infection d'un appareil connecté par un virus (53 %), la fraude bancaire (38 %), le piratage d'un compte (34 %), la fraude commerciale (33 %) et la fraude par courriel (32%), incluant le hameçonnage et l'infection par pourriel (Norton - Symantec, 2017).

Pour ce qui est des tendances technologiques en cybercriminalité, trois familles d'activités se dégagent : 1) les logiciels malveillants, notamment en croissance pour les objets connectés; 2) les attaques par hameçonnage, tout particulièrement à des fins d'usurpation d'identité et; 3) les attaques contre l'accessibilité des données, que ce soit par le refus de service ou DDoS ou par le rançonnage (Medina & Molist, 2017).

L'essor de la téléphonie mobile s'accompagne d'un essor de la cybercriminalité visant les téléphones intelligents, et affecte tout particulièrement les pays émergents où ce mode de communication est un vecteur essentiel de développement. Le monde émergent est également particulièrement touché par d'autres formes de cybercriminalité, notamment la fraude. Par exemple, les trois principaux pays victimes de hameçonnage sont, dans l'ordre, la Chine, le Brésil et l'Algérie (Forcepoint, 2016). De son côté, la firme Symantec fait état d'une croissance rapide des activités cybercriminelles visant la téléphonie mobile, avec une augmentation de 105% entre 2015 et 2016 des virus identifiés spécifiquement développés pour les téléphones intelligents (Norton - Symantec, 2016).

Il convient de souligner la corrélation entre la diminution observée des crimes dits traditionnels dans le monde économiquement développé, notamment des crimes contre la propriété, avec la croissance de la criminalité en ligne. Si les liens de causalité ne sont pas encore clairement établis, cette corrélation suggère que la progression de la cybercriminalité serait liée, du moins en partie, à un glissement des activités délictueuses du monde réel vers le cyberespace (Weulen Kranenbarg, Holt, & van Gelder, 2017)

Il est intéressant de voir que ce genre d'activités criminelles peut être mesuré de deux manières. Une option est d'en mesurer l'intensité : par exemple, on peut mesurer l'évolution du nombre de rançongiciels identifiés par une firme de cybersécurité (une mesure assez aisément productible et publiée par les différents rapports mentionnés plus haut). Une autre option est de mesurer le volume d'utilisation de ces logiciels : les résultats peuvent être très différents. Par exemple, dans le cas des rançongiciels, on observe une stabilisation de leur nombre (tout du moins, de ceux détectés) et du nombre de leurs familles entre 2015 et 2016; cependant, l'estimation du nombre d'attaques déjouées indique une forte augmentation, de 0,4 Millions en 2015, 1,6 Millions en 2016 à 3 Millions en 2017 (Symantec, 2018). Ceci montre que si la technologie se stabilise, l'intensité de ce genre d'activités, elle, est en augmentation.

Une seconde catégorie de tendances concerne les activités dirigées contre la personne, comme les cyberviolences, le cyberharcèlement, ainsi que les discours haineux. Ces crimes et délits, s'ils existent dans le monde dit réel, ont pris une ampleur, une forme et des conséquences toutes particulières lorsqu'ils se sont développés dans la cybersphère (un aspect sur lequel revient le chapitre 3). L'anonymat et dépersonnalisation qui caractérisent les interactions en ligne ont notamment contribué à une désinhibition des comportements de violences dans le cyberespace (Zweig, Dank, Lachman, & Yahner, 2013).

Les groupes victimisés dans le cyberespace par ces violences reflètent la diversité de ceux victimisés dans le monde physique et regroupent, notamment, les femmes et l'ensemble des minorités sexuelles, ethniques et religieuses (Peterson & Densley, 2017). Deux groupes se distinguent sur le terrain de la cyberviolence : les violences faites aux femmes et aux filles, qui trouvent dans le cyberespace un terrain particulièrement propice (Pasricha, 2016), ainsi que le cyberharcèlement et les cyberviolences, notamment amoureuses, chez les adolescents, les réseaux sociaux constituant aujourd'hui « un nouveau vecteur de violence chez les jeunes » (Patton et al., 2014).

De la même manière, les formes de cyberviolences diffèrent, ainsi que leur expression en fonction des contextes géographiques, sociaux et culturels. Si la cyberviolence dans les pays non occidentaux demeure encore sous-étudiée, il convient de noter plusieurs exceptions, par exemple dans le cas de l'Inde, où plusieurs recherches ont été publiées ces dernières années sur le sujet, notamment sur les violences faites aux femmes dans le cyberespace (Halder & Jaishankar, 2016; Jaishankar & Halder, 2011; Pasricha, 2016). Cependant, on déplore une très faible production scientifique sur la prévalence ou l'étiologie des différentes formes de cyberviolence (Diamond & Bachman, 2015). Plusieurs formes de cyberviolences font toutefois l'objet d'une littérature bourgeonnante, notamment concernant les populations adolescentes et la question du cyberharcèlement, l'investissement des réseaux sociaux par les gangs, la forte présence des groupes haineux, ainsi que la propagande et le recrutement terroriste (Peterson & Densley, 2017).

Ensuite, les cadres juridiques et la criminalisation de ce genre d'activités diffèrent beaucoup d'un pays à l'autre (UNODC, 2013). Ceci constitue un frein majeur à la production de données harmonisées au niveau mondial. Enfin, ces violences font l'objet de taux de signalement très faibles, ce que montre, entre autres, une étude du Pew Research Center menée aux États-Unis. Les résultats de cette enquête indiquent que, si 41% des répondants adultes déclarent avoir été victimes de harcèlement en ligne, seuls 48 % d'entre eux ont opposé une action telle que le signalement à la plateforme de contenu, l'ajustement de leurs paramètres de navigation ou la modification de leurs usages (Pew Research Centre, 2014).

Auteurs et victimes : qui sont-ils ?

Pour se pencher sur la question des auteurs des actes délictueux, criminels ou déviants dans le cyberespace, une réalité s'impose: aujourd'hui, la commission d'une vaste portion de ce genre d'actes ne requière pas de compétences ou de connaissances

technologiques poussées (UNODC, 2013). Aussi, tout individu lambda jouissant d'une connexion à Internet peut développer une activité criminelle ou délictueuse. L'étendue des possibles devient alors extrêmement large. Bien que toute estimation des activités cybercriminelles soit limitée par des contraintes inhérentes majeures, l'UNODC estimait, en 2013, que 80 % des actes cybercriminels relevaient, d'une manière ou d'une autre, d'une forme de criminalité organisée (UNODC, 2013). Aussi, le cyberespace a-t-il été investi par des formes organisées de criminalité, que ce soit par glissement de leurs activités vers le monde virtuel ou par l'émergence de nouvelles opportunités offertes dans le cyberespace.

De leur côté, qui sont les victimes de la cybercriminalité ? La réponse la plus fréquemment apportée est que tout usager d'un appareil connecté est une victime potentielle. Pour autant, si, face à la multiplicité des crimes et des modus operandi présents dans le cyberespace, l'établissement d'un profil type de victimes s'avère impossible, il est intéressant de souligner ici certaines caractéristiques.

Dans son enquête annuelle, la firme Norton a estimé à 978 millions le nombre d'individus ayant été victimes d'une forme de cybercriminalité en 2017, sur une population d'internautes d'1,8 milliard : le plus souvent, cette victimisation se fait sous la forme d'infection par un virus, de fraude bancaire, de piratage de compte courriel ou de réseau social, de fraude commerciale ou de hameçonnage (Norton - Symantec, 2017). Pour autant, il convient de souligner que, si le vecteur technologique de ces activités criminelles comporte majoritairement une composante technologique, l'erreur humaine en est un déterminant clé : ainsi, les dernières statistiques de l'agence européenne en charge de la sécurité des réseaux et de l'information (ENISA) montrent que 90 à 95 % des cyberattaques menées à terme dans le monde ont été permises par un hameçonnage réussi (European Union Agency For Network and Information Security, 2018). Toujours selon cette enquête, les usagers conservent une confiance élevée en la capacité du secteur privé à gérer de manière sécuritaire leurs informations personnelles (76 à 82 %), tandis que plus de 41 % déclarent une diminution de leur confiance en leur gouvernement pour cette même responsabilité.

Le Global Economic Crime Survey, produit par la firme Pricewaterhouse Coopers, consiste en une enquête menée à l'échelle mondiale auprès du secteur privé. Dans sa dernière édition, l'enquête a ainsi montré que la cybercriminalité est devenue le second crime économique rapporté par les entreprises avec une progression de 8 points entre 2014 et 2016, et que la cybercriminalité est une préoccupation grandissante pour le secteur privé. En contraste, il est intéressant de noter que seules 37 % des entreprises interrogées disposaient d'un plan de réaction au cybercrime. En outre, une moitié des répondants doutait de la capacité des pouvoirs publics à faire face aux événements de cybercriminalité les touchant (PwC, 2016). La vulnérabilité face à la cybercriminalité touche, au sein du secteur privé, surtout les petites et moyennes entreprises (Ponemon Institute LLC, 2016).

Concernant par exemple les fraudes dites BEC (en anglais, Business Email Compromise), une évolution des fameuses arnaques « nigérianes »[11] adaptées au secteur privé, ce sont les petites et moyennes entreprises qui en constituent la cible principale, comptant pour 38 % du volume total des entreprises ciblées (Symantec, 2016).

Si l'on considère l'ensemble des activités délictueuses commises dans le cyberespace, les taux de cybervictimisation sont supérieurs à ceux concernant les crimes dits « traditionnels » (UNODC, 2013). Ce constat est confirmé par les différents rapports sur la cybersécurité, qui font état de niveaux de criminalité et de victimisation en augmentation rapide (International Telecommunication Union, 2017a ; Norton - Symantec, 2016, 2017 ; Ponemon Institute, 2017 ; PwC, 2016, 2018 ; RSA, 2016 ; Symantec, 2018). Pour autant, il faut nuancer cette conclusion, notamment en ceci qu'elle englobe des activités telles que l'infection d'un appareil par un virus ou la réception de courriels frauduleux, des incidents très courants et qui, dans une majorité de cas, sont neutralisés par des systèmes de protection ou par le jugement de l'utilisateur.

Une revue systématique des enquêtes de cybervictimisation effectuées en Europe a montré que les offenses graves et les crimes commis dans le cyberespace formaient un volume bien moindre que la « cybercriminalité » prise comme un tout homogène englobant sans distinction l'ensemble des incivilités, délits et crimes. Ainsi, il apparaît que seuls 0,6 à 3,5 % des usagers rapportaient avoir été victimes de fraude commerciale en ligne, 0,4 à 2,2 % pour la fraude bancaire 0,4 % pour les autres types de fraude (incluant la fraude amoureuse et celle à avance de frais), 3% pour les formes les plus sérieuses de cyberharcèlement, et 1,3 à 5,8 % pour le piratage (Reep-van der Berg & Junger, 2018).

Un élément, également très intéressant du point de vue de la cybervictimologie, est que les incidences de revictimisation varient énormément en fonction du type de cybercrime considéré. Par exemple, une enquête de victimisation menée en Angleterre et au Pays de Galles par l'Office national de Statistiques (Office of National Statistics) et le Ministère de l'Intérieur (Home Office) a montré qu'en moyenne, seules 16% des victimes de fraudes avaient été re-victimisées (Levi, 2017). À l'inverse, les victimes de revenge porn[12] vivent, quant à elle, un processus de revictimisation répétitif affectant toutes les sphères de leur vie (Bates, 2015). Enfin, rappelons ce qui a été précédemment mentionné, à savoir que les taux de cybervictimisation sont plus élevés dans les pays à niveau de développement moins élevé (UNODC, 2013), ainsi que chez les usagers les plus fréquents et qui possèdent un niveau de connaissance et d'usage du cyberespace plus développé.

Cependant, l'ensemble de ces grandes tendances doit être lu à la lumière de notre méconnaissance et notre incapacité à mesurer, même grossièrement, l'ampleur des phénomènes cybercriminels. À cet égard, une étude de Jardine (2015) tentant une normalisation de plusieurs mesures absolues d'actes cybercriminels, montre bien la lecture faussée que ces tendances chif-

frées induisent souvent. L'auteur dégage alors plusieurs facteurs qui mettent à mal la lisibilité et la fiabilité de ces mesures : 1) la complexité du cyberespace et de ses acteurs entraîne une grande difficulté à mesurer Internet, et donc établir un « tout » quantifiable servant de base pour la normalisation, 2) les rapides évolutions des caractéristiques et de l'ampleur du cyberespace, qui rendent toute tendance non normalisée absolument illisible dans le temps, du fait même des changements intrinsèques du contexte cyberspatial, 3) l'absence de système de collecte de données sur le cybercrime fiable et harmonisé, qui fait que les études doivent se baser sur des données à la qualité et la représentativité très médiocre. Ainsi, sur les 13 tendances étudiées : 6 normalisations montrent une amélioration de la situation en dépit de tendances indiquant une aggravation; 6 normalisations montrent une amélioration plus grande de la situation que ce que les tendances absolues indiquent et; une seule normalisation confirme l'indication fournie par la tendance absolue mesurée.

Distribution géographique de la cybercriminalité

Il est très difficile de procéder à une analyse géographique de la cybercriminalité, notamment car : 1) les tendances évoluent rapidement, 2) les activités cybercriminelles sont très variées et 3) leur répartition géographique varie en fonction du type considéré. Cependant, et de manière très indicative, soulignons ici la tentative de la firme Symantec à effectuer un classement annuel des pays les plus « producteurs » d'activité cybercriminelle. Ainsi, en 2016, les dix premiers étaient : les États-Unis (23,96%), la Chine (9,63 %), le Brésil (5,84 %), l'Inde (5,11 %), l'Allemagne (3,35 %), la Russie (3,07 %), le Royaume-Uni (2,61%), la France (2,35 %), le Japon (2,25 %) et le Vietnam (2,16 %), en termes de volume d'activité cybercriminelle (Symantec, 2018). Notons que cette évaluation se concentre sur un nombre restreint d'activités et rappelons que les méthodologies à la base de ce genre d'études comportent trop de limitations pour être considérées comme absolument fiables. Il est en outre important de souligner qu'il existe une forte corrélation entre les pays les plus producteurs de cybercriminalité et ceux qui en sont le plus victimes. Dans un rapport de 2015, la firme de gestion des risques Red24 identifiait les pays les plus affectés par la cybercriminalité (États-Unis, Russie, Chine, Hong Kong, Inde, Brésil, Royaume-Uni, Pays-Bas, Allemagne et Norvège) et ceux à l'origine des cyberattaques (Russie, Chine, Europe de l'Est, Roumanie, Brésil, Nigéria, Vietnam, Indonésie, Corée du Sud et États-Unis) : on observe ainsi que les pays les plus producteurs de cybercriminalité sont aussi ceux qui en subissent les principaux dommages (Red24, 2015).

La distribution géographique de la cybercriminalité peut être mesurée de deux manières : ou bien l'on se base sur la localisation physique de l'auteur, ou bien l'on choisit celle de la victime (Kigerl, 2012). Selon la nature de l'activité délictueuse envisagée, l'une ou l'autre de ces approches peut s'avérer plus pertinente. Par exemple, pour des domaines comme le hameçonnage, l'envoi de pourriels ou l'usage de botnets[13], le pays d'origine de ces activités s'avère le plus utile, tandis que dans le cas de cybervio-

lences, une mesure centrée sur la victime peut se révéler plus pertinente.

En outre, la distribution géographique des auteurs, des victimes et des types d'activités délictueuses est très liée aux fractures numériques et aux inégalités caractérisant le cyberespace, dont nous avons parlé en début de chapitre. Dans cette perspective, Alex Kigerl (2016) propose une typologie intéressante de ce qu'il nomme les « nations du cybercrime ». En se basant sur les données fournies par pays, notamment celles offertes par les rapports des grandes firmes internationales de cybersécurité, l'auteur a identifié des profils de pays en fonction de : 1) leur niveau de participation à certains types de cybercriminalité, 2) types de cybercriminalité et 3) des facteurs macro tels que le revenu net par habitant. Ainsi, il a pu identifier 4 grands groupes de pays.

- **Groupe 1 :** des pays à faible participation à la cybercriminalité, qui concerne essentiellement les pays les plus affectés par la fracture numérique, notamment l'accès au cyberespace. On y retrouve en majorité les pays au niveau de développement économique plus faible.
- **Groupe 2 :** les « spécialistes de la fraude par avance de frais », qui regroupe les pays dont l'activité cybercriminelle gravite autour des fraudes les moins sophistiquées technologiquement parlant. Il concerne un ensemble très hétérogène de pays (on y retrouve notamment des pays comme l'Islande et le Nigéria) : l'auteur analyse ces résultats en se concentrant sur l'aspect non technologique de ces crimes, qui permettent à des individus aux compétences limitées de développer des activités criminelles très rémunératrices (on pense, entre autres, au célèbre modèle de l'arnaque nigériane, dite 419, analysés dans le chapitre 3).
- **Groupe 3 :** les pays caractérisés par des formes moins graves de cybercriminalité, comme les pourriels non frauduleux ou infectés, le piratage ou les atteintes à la propriété intellectuelle. Ce groupe est constitué des pays les plus développés économiquement et les plus connectés (ceux qui se trouvent « du bon côté » des fractures numériques).
- **Groupe 4 :** les « spécialistes du hameçonnage », regroupant en fait 40% de l'ensemble des pays considérés et qui se distingue par une grande activité cybercriminelle dans l'ensemble des types de crimes envisagés, surtout en termes de fraude (incluant des niveaux équivalents au groupe 2 pour la fraude sur avance de frais), de courriels infectés et frauduleux et de hameçonnage.

Cette étude est particulièrement intéressante en ceci qu'elle tente de construire un premier cadre permettant d'évaluer des corrélations entre des macro-facteurs et les activités cybercriminelles.

Dans ce qui suit, nous tentons d'identifier des dynamiques propres et des problématiques clés pour chacune des grandes régions du globe. Il convient ici de souligner l'aspect très disparate des informations disponibles à ce sujet, ce qui rend difficile la comparaison géographique.

a) Afrique

Le continent africain offre des conditions particulièrement favorables au développement d'un secteur cybercriminel dynamique, notamment par la forte progression des technologies de l'information et de la communication, de la faiblesse des infrastructures technologiques et de l'insuffisance des cadres juridiques et des capacités de sécurité nationales (Mark Shaw, 2018). On soulignera toutefois un manque crucial de données sur les phénomènes cybercriminels dans le continent africain.

En 2014, la Commission Économique des Nations-Unis pour l'Afrique soulignait que les activités cybercriminelles progressaient plus rapidement dans ce continent que partout ailleurs (United Nations Economic Commission for Africa, 2014). Toutefois, la part africaine dans le paysage global est encore restreinte : en termes d'activités malveillantes (cyberattaque, logiciels malveillants, courriels frauduleux, hameçonnage, bots et centres de commande et contrôle), l'Afrique n'est à l'origine que de moins de 3 % du volume mondial (Symantec, 2016). La fraude par ruse demeure une problématique très présente en Afrique : particulièrement, le Nigéria et l'Afrique du Sud sont par exemple à l'origine de 55 % du volume mondial des courriels de type BEC (Symantec, 2016). On observe néanmoins une complexification des types de fraude, avec une orientation vers des scénarii de fraude plus élaborés, notamment en direction des entreprises (Trend Micro & Interpol, 2017).

Le piratage est également, dans le continent africain comme au Moyen-Orient, une source de cybercriminalité. Notamment, il convient de noter que 57 % des logiciels utilisés dans ces régions sont des copies piratées, contre 38 % pour la moyenne mondiale (Business Software Alliance, 2016). Ces logiciels corrompus constituent des vecteurs privilégiés de logiciels malveillants et représentent une part très importante de l'infrastructure informatique, notamment dans les économies les plus dynamiques du continent : 84 % en Algérie, 81 % en Côte d'Ivoire, 78 % au Kenya et au Sénégal, 74 % en Tunisie et 66 % au Maroc (Business Software Alliance, 2012).

L'Afrique du Sud, le Nigéria et la région nord-africaine se distinguent des autres pays africains par leur dynamisme en matière de cybercriminalité. Globalement, on observe que le poids relatif des pays dans l'activité cybercriminelle africaine correspond au taux de pénétration d'Internet dans ces pays, lui-même très lié au niveau de développement économique national. En outre, les africains eux-mêmes sont particulièrement touchés par la cybervictimisation. En Afrique du Sud, 67 % des adultes interrogés dans le cadre de l'enquête annuelle menée par la firme Norton en 2016 ont rapporté avoir été victime de cybercriminalité au cours de l'année précédente, contre une moyenne mondiale de 48 % (Norton - Symantec, 2016).

En 2013, 47 % des usagers de téléphones intelligents sud-africains rapportaient avoir été victimes d'une forme d'activité cybercriminelle visant leur appareil mobile (Norton - Symantec, 2013). Ceci est particulièrement problématique, car le continent africain est aussi celui où les téléphones intelligents sont le plus employés pour effectuer des transferts d'argent (Symantec, 2016). En outre, on estime que les usagers de téléphones mobiles devraient encore augmenter de manière rapide en Afrique, passant de 301 millions en 2013 à 504 millions en 2020 (GSMA, 2015). Ainsi, les individus, les entreprises et, plus largement, les économies africaines se trouvent fortement affectées par la cybercriminalité, qui coûte par exemple près de 500 Millions de dollars par an au Nigéria, la plus importante économique du continent avec un PIB de 521,8 Milliards de dollars (Shiloh & Fassassi, 2017).

b) Amérique latine

Le crime organisé latino-américain a massivement investi le cyberespace, que ce soit pour y développer de nouveaux champs d'activités comme la fraude en ligne, ou bien pour faciliter leurs activités traditionnelles, notamment en support de trafics et de blanchiment d'argent (Clavel, 2016). En effet, la force organisationnelle et opérationnelle du secteur du crime organisé latino-américain, associée à la faiblesse et la vulnérabilité des infrastructures et de la sécurité informatiques régionales, conduit à une situation particulièrement critique, où les organisations criminelles jouissent aujourd'hui de moyens et de compétences techniques égaux ou supérieurs à ceux des États et des agences de sécurité (Observatorio de la ciberseguridad en América latina y el Caribe, 2016). Ainsi, la lutte contre la cybercriminalité en Amérique latine est intrinsèquement liée à celle contre le crime organisé (Trend Micro - Organisation des États Américains, 2013).

Le Brésil est devenu au cours des dernières années un point chaud de la cybercriminalité au niveau mondial et se trouve « à l'épicentre d'une vague globale de cybercriminalité », tant du point de vue de la commission que de la victimisation (Muggah & Thompson, 2015). Le pays se situait en 2015 à la seconde place mondiale pour les logiciels malveillants et les fraudes visant les transactions bancaires (Kaspersky, 2015). Le Centre d'Études, de Réponses et de Traitement des Incidents de Sécurité du Brésil (CERT) a enregistré une augmentation de 197 % du nombre de signalements concernant des incidents cybercriminels durant l'année 2014, parmi lesquelles 40% concernant des tentatives de fraude (Diario do Comercio, 2015).

Selon le Département de Sécurité (Departamento de Segurança) brésilien, ce sont les petites et moyennes entreprises brésiliennes qui sont le plus visées par ces activités (65 % contre 30,8 % pour les grandes compagnies), notamment en raison de niveaux moins élevés de sécurité (Folha de S. Paolo, 2015). En outre, le Brésil occupe le premier rang mondial en termes d'infection par des logiciels malveillants de téléphones mobiles. Le second pays latino-américain, le Mexique, arrive en 4ème place de ce classement qui montre une vulnérabilité particulièrement marquée dans les pays du monde émergent (Malwarebytes, 2017).

Le Brésil a ainsi développé un milieu cybercriminel original, qui

opère moins au sein du Deep Web[14] que sur le cyberespace dit « de surface », à travers des plateformes comme les réseaux sociaux classiques : formée de cybercriminels particulièrement jeunes, cette mouvance brésilienne s'est cristallisée autour des fraudes et des logiciels malveillants tournés vers le secteur bancaire (Trend Micro, 2015).

c) Asie et Pacifique

Le continent asiatique constitue un point de très forte croissance pour le cyberespace et, par conséquent, le domaine cybercriminel. En effet, avec le taux de croissance économique le plus dynamique au Monde ainsi que la plus forte progression du taux de pénétration d'internet, les internautes asiatiques représentaient, en 2016, 55 % des usagers mondiaux selon le World Internet Statistics. Pour autant, les situations asiatiques sont loin d'être homogènes, notamment en termes de volume d'usagers, de taux de pénétration et de niveau de développement économique. À cet égard, on notera par exemple que la Chine et l'Inde concentrent à elles seules plus de la moitié de l'ensemble des internautes asiatiques, tandis que les taux de pénétration varient de manière très importante entre les pays les plus connectés comme le Japon, la Corée du Sud, l'Australie, la Nouvelle Zélande ou Taiwan, et des pays dont les niveaux de développement et l'importance des populations rurales marginalisées freinent la pénétration d'Internet, comme c'est le cas pour l'Inde, le Pakistan ou encore les pays de la péninsule indochinoise (Broadhurst & Chang, 2013).

Il est donc prévisible de voir l'ampleur de la cybercriminalité commise contre le secteur privé comme contre les individus, suivre et profiter de cette croissance : on estime ainsi que les organisations asiatiques, publiques comme privées présentent 80% de risque de plus que les autres d'être victimes de cyberattaques (Oliver Wyman, 2017). De fait, selon la firme de cybersécurité LogRythm, les entreprises asiatiques font face à une menace grandissante : leurs dernières enquêtes ont montré qu'en 2016, 90 % des entreprises asiatiques avaient été victime d'une forme de cybercriminalité, contre 76 % en 2015 et 66% l'année précédente (Lewis, Weinland, & Peel, 2016). En 2017, la firme ESET estimait que 54 % de ses clients parmi les petites et moyennes entreprises (situées à Singapour, Hong Kong, en Inde, en Thailande et au Japon) avaient été victimes d'un piratage de données dans les trois années précédentes : par ordre d'importance, c'est l'Inde (avec 73 %) et Hong Kong (avec 61 %) qui étaient les plus touchés, au contraire du Japon (29 %). En outre, la même enquête montrait que le risque d'attaque est corrélé à la taille de l'entreprise : 70 % des plus grandes entreprises de la catégorie avaient été victimes d'un piratage contre 37 % des plus petites (ESET, 2017).

En outre, les pays asiatiques émergents comme le Vietnam ou la Malaisie jouent un rôle de plus en plus important sur la scène cybercriminelle tant comme origine que comme cible de ces activités (Chang, 2017), et ce, pour plusieurs raisons : 1) l'émergence de leur connectivité au cyberespace, 2) leur croissance économique et 3) les enjeux géopolitiques régionaux comme les tensions en Mer de Chine du Sud (Boudreau & Chau, 2016).

d) États-Unis, Chine, Russie et la disparition des frontières entre cybercrime et cyberguerre

Bien que le focus de notre travail ne porte pas en soi sur les multiples dimensions géopolitiques du cyberespace, il convient ici d'identifier plusieurs pays pour lesquels la cybercriminalité est intrinsèquement liée à des questions de sécurité nationale et parmi lesquels les États-Unis, la Chine et la Russie se distinguent tout particulièrement. En effet, ces trois pays cumulent plusieurs caractéristiques : 1) ils sont des cyberpuissances, qui ont investi le cyberespace comme un champ géopolitique stratégique et ont bâti des capacités offensives et défensives particulièrement développées, 2) ils sont des foyers pour la cybercriminalité en ceci qu'une grande partie de l'activité cybercriminelle mondiale y prend racine et 3) ils sont des cibles privilégiées de cette cybercriminalité, qu'elle soit dirigée contre leurs institutions gouvernementales, leur secteur privé ou leurs citoyens. Il est intéressant de remarquer que les conceptions cristallisées autour de ces questions reprennent les logiques bloquistes propres à la Guerre Froide : par exemple, dans son rapport sur les cyber-attaques, l'équipe de recherche de la firme FireEye identifie 4 ensembles : l'Asie, l'ancien bloc soviétique, le Moyen-Orient et les États-Unis (Geers, Kindlund, Moran, & Rachwald, 2017).

Aux États-Unis, les activités cybercriminelles sont largement considérées comme une menace géopolitique, et ce, qu'elles soient dirigées vers le secteur privé comme public, et quels que soient leurs motivations. James Comey, alors directeur du FBI, exprimait bien cette confusion en 2017 : « il y a deux sortes de grandes compagnies aux États-Unis. Il y a celles qui ont été piratée par les Chinois et celles qui ne savent pas qu'elles ont été piratées par les Chinois » (Cook, 2014, p.1). Le IC3 confirme cette tendance à la hausse des activités criminelles dirigées contre le secteur privé des États-Unis, enregistrant une hausse de 11% des plaintes reçues entre 2014 et 2016, pour des pertes déclarées passant de 80 000 $ à 1,33 millions de dollars en seulement deux ans (Insurance Information Institute, 2017).

Les États-Unis constituent une pièce absolument essentielle du paysage mondial de la cybercriminalité, et ce, sous trois aspects principaux : 1) en terme de criminalité, 2) en termes de victimisation et 3) en termes de réponses. Tout d'abord, les victimes individuelles américaines comptaient pour 143 des 978 millions de celles comptabilisées par la firme Norton dans son dernier rapport, totalisant 19,4 des 172 milliards de dollars de pertes estimés (Norton - Symantec, 2017). Les vols de données sont également une problématique en forte augmentation pour les entreprises américaines : entre 2016 et 2017, le centre de ressources en usurpation d'identité (Identity Theft Resource Center) a enregistré une hausse de 44,7 % des signalements (Insurance Information Institute, 2017). Grâce à l'obligation faite aux acteurs privés de

déclarer ce genre d'incident, on a ainsi, pour ce pays, une image plus fiable de la situation. Les principaux types de cybercriminalité rapportés par le IC3 (Internet Complaint Center, centre des plaintes relatives à Internet dépendant du FBI) sont: les différents types de fraude, le vol de données personnelles, les courriels frauduleux, le cyberharcèlement et les menaces (Federal Bureau of Investigation - Internet Crime Complaint Center, 2016). Selon le même rapport, les dommages financiers les plus importants sont causés par les différents types de fraudes et les vols de données personnelles.

Le cyberespace a émergé comme une nouvelle priorité stratégique pour la Russie post soviétique, qui a développé un système particulièrement abouti de convergence et de collaboration entre les milieux cybercriminels et le gouvernement. Au cours des dernières années, le milieu cybercriminel russe s'est considérablement structuré, hiérarchisé et étoffé (Stoyanov, 2015) et jouit aujourd'hui d'une grande complaisance de la part des autorités nationales (Cybersecurity Intelligence, 2015). La Russie compte aujourd'hui, selon les estimations, pour environ 35% des revenus totaux de la cybercriminalité (Lewins, 2017). Hautement spécialisée et technologiquement très avancée, la cybercriminalité russe se montre performante sur ses deux priorités : le profit des cybercriminels et l'avancée des intérêts stratégiques russes (Galeotti, 2011).

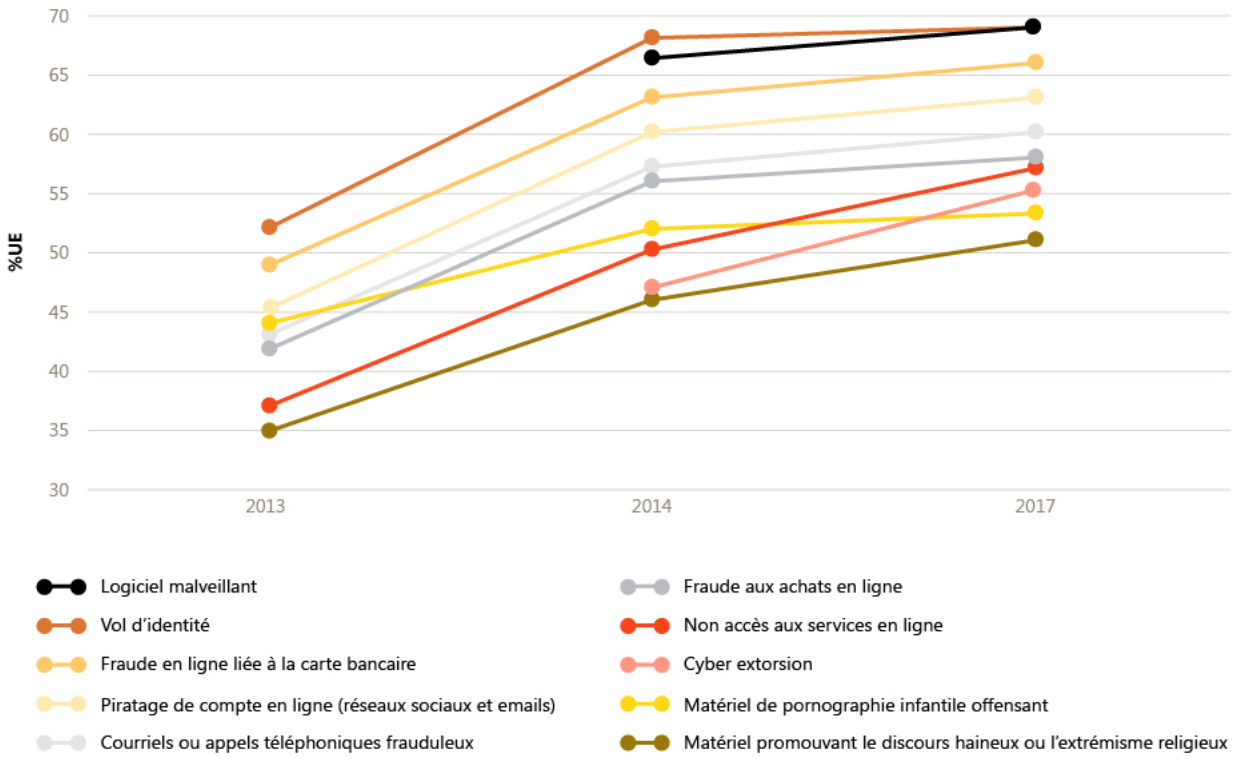
Enfin, la Chine constitue, dans le paysage asiatique, un point focal de la cybercriminalité, aussi bien comme origine d'activités illicites qu'en termes de victimisation (Microsoft, 2017). En effet, les internautes et les entreprises chinoises sont particulièrement vulnérables et les taux de victimisation sont élevés, notamment dans les provinces les plus développées du pays et qui cumulent des revenus, ainsi que des taux de pénétrations d'internet supérieurs à ceux du reste du pays (Cheng, 2017).

Cette catégorie de pays pour lesquels le cyberespace constitue un terrain stratégique de projection de puissance ne se résume pour autant pas aux trois nations précédemment évoquées. On soulignera que d'autres pays, notamment la Corée du Nord et l'Iran, se distinguent, eux aussi, par des conditions favorables à l'émergence d'un milieu cybercriminel vigoureux : accès aux compétences, faible répression et complaisance des pouvoirs publics (McAfee, 2018).

e) Europe occidentale et Canada

Le continent européen, tout particulièrement les pays de l'Union Européenne, fait l'objet d'une meilleure information et disponibilité de celle-ci, notamment en raison de plusieurs facteurs : 1) les mécanismes de signalement et l'obligation de signaler, 2) l'engagement de l'agence Europol pour la lutte contre la cyber-

Graphique 2.4. **Évolution de la perception du risque des usagers européens face à dix types de cybercrimes**



Source: Eurobaromètre (2017)

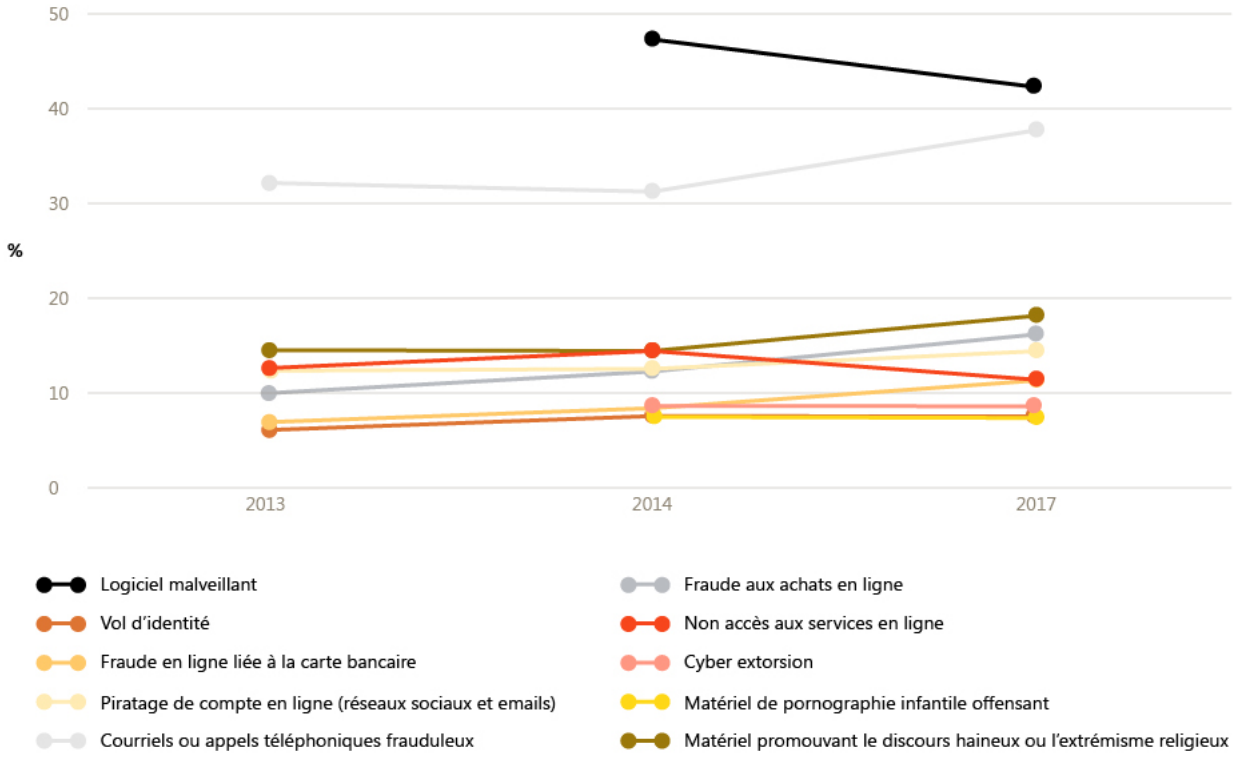
criminalité et son travail en termes d'analyse et de production de connaissance et 3) l'existence de solides enquêtes (Eurobaromètre) sur les usages, le sentiment d'insécurité et la victimisation dans le cyberespace. Les trois derniers baromètres sur le cybercrime ont été effectués en 2013, 2014 et 2017.

Les préoccupations face à la possibilité de victimisation dans le cyberespace ont très nettement augmenté depuis 2013, notamment pour la fraude et le vol d'identité. De manière très intéressante, la plus forte progression a été enregistrée entre 2013 et 2014 (des augmentations de l'ordre de 15 points), le niveau de préoccupation se stabilisant entre 2014 et 2017 (des augmentations de l'ordre de 2 à 3 points). Les plus fortes progressions des préoccupations des internautes européens entre 2014 et 2017 sont observables pour des crimes dont l'importance médiatique a émergé au cours de la même période : les rançongiciels (augmentation de 8 points) et les attaques dirigées contre les services bancaires en ligne (augmentation de 7 points). Il est intéressant de noter que les crimes de haine ou la promotion du terrorisme sur internet font l'objet d'une croissance soutenue des préoccupations : 35 % en 2013, 46 % en 2014 et 51 % en 2017.

La partie de l'Eurobaromètre portant sur la victimisation est particulièrement intéressante, notamment en ceci qu'elle montre une prévalence et une progression faible à modérées des crimes les plus fréquents comme la fraude commerciale ou bancaire, le hameçonnage, le piratage de comptes, le rançonnage ou le vol d'identité. Ces données sont tout particulièrement intéressantes quand elles sont comparées aux niveaux de préoccupation précédemment évoqués, ce qui montre bien comment, alors que l'inquiétude des internautes européens face à leur sécurité en ligne a fortement augmenté au cours des 5 dernières années, la prévalence de ces crimes demeure minoritaire et leur augmentation faible. Un phénomène observé dans le chapitre 1 dans le cadre de l'analyse du sentiment d'insécurité.

Enfin, les trois enquêtes successives montrent que les internautes s'en remettent prioritairement aux services de police pour apporter une réponse en cas de victimisation, notamment en cas de vol d'identité, de chantage ou rançonnage, de crimes sexuels ou de fraude bancaire. Les acteurs privés, tels que le site internet ou commerçant en ligne ou encore le fournisseur d'accès à Internet, sont également considérés comme des interlocuteurs, notamment en cas de fraude commerciale, de logiciels frauduleux ou de piratage (Eurobarometer, 2017).

Graphique 2.5. **Évolution du taux de victimisation des usagers européens pour dix types de cybercrimes**



Source: Eurobaromètre (2017)

Au Canada, les données policières confirment une tendance à la hausse, avec une croissance de 45 % dans les signalements d'incidents cybercriminels depuis 2014, et plus de la moitié des petites et moyennes entreprises ont été victimes d'activités cybercriminelles (McAfee, 2018). La Chambre du Commerce du Canada estimait en 2017 que la cybercriminalité captait 15 à 20 % des 3 milliards de dollars générés par la cyberéconomie (Canadian Chamber of Commerce, 2017). En moyenne pour l'année 2017, une entreprise canadienne a été confrontée à près de 10 cyberattaques, dont 20 % ont compromis des informations hautement stratégiques (Scalar, 2018). Il est toutefois intéressant de noter que la génération dite M, formée des moins de 35 ans, semble avoir moins tendance à être victime d'activités illégales sur Internet, avec un taux de 42% contre 60% mondialement, et 69 % aux États-Unis (Norton - Symantec, 2017).

Conclusion : quels enjeux pour la prévention de la cybercriminalité ?

De ce chapitre, que retenir ? Tout d'abord, que la cybercriminalité en soi ne constitue pas un champ homogène, mais bien plus un ensemble d'activités délictueuses commises dans le cyberespace. Ainsi, il est très difficile d'en tirer quelque conclusion que ce soit, tant les enjeux, les acteurs et les dynamiques à l'œuvre sont diverses et hétéroclites. Ensuite, soulignons que, du point de vue de la prévention, cet ensemble sans cohérence ne peut être conçu comme un objet d'action. Tout d'abord, car nous ne connaissons rien ou pas grand-chose des processus et facteurs qui sous-tendent les activités cybercriminelles, une question épineuse et fondamentale sur laquelle se penche le prochain chapitre. Ensuite, car il est très complexe de mesurer et d'estimer de manière fiable et précise les différentes activités et leurs conséquences. Enfin, la conception que les grands acteurs, publics et privés, ainsi que les usagers, se font du cyberespace est essentiellement sécuritaire, plus que préventive, un aspect qui sera largement abordé dans les quatrième et cinquième chapitre.

Pour conclure, revenons néanmoins à un aspect clé qui, selon nous, doit constituer une trame de fond lorsque l'on se pose la question de savoir comment prévenir la cybercriminalité : la question des libertés, collectives et individuelles, des questions de privauté et de la nécessité de redéfinir les cadres qui les régissent à l'heure du cyberespace et de la surveillance de masse.

Dans leur ouvrage phare, Singer et Friedman (Singer & Friedman, 2014) soulignent qu'au cours de la dernière décennie, les États ont privilégié une conception sécuritaire du cyberespace : selon ces auteurs, la cybersécurité est donc aujourd'hui la priorité qui guide les relations entre gouvernements et acteurs privés dans le cyberespace, les premiers cherchant à développer des outils institutionnels et législatifs pour obliger les seconds à collaborer à leurs efforts (en termes d'enquêtes, de procédures juridiques, de surveillance et de contrôle). En terme de cybercriminalité, cette conception considère le cyberespace comme « ingouvernable, impossible à connaître, qui nous rend vulnérables, qui est toujours menaçant et qui est habité par un éventail d'acteurs hostiles et menaçants auxquels il confère de nombreux avantages » (David Barnard-Wills & Debi Ashenden, 2012, p. 116).

Un des enjeux principaux de la lutte contre la cybercriminalité réside aujourd'hui dans la définition de nouveaux équilibres entre les libertés individuelles et du droit à la privauté d'une part, et des nécessités de sécurité et de surveillance de l'autre. Au cœur de cette problématique, deux dimensions clé font tout particulièrement débat : 1) la question des données personnelles et de l'étendue des pouvoirs, notamment de la part des autorités publiques, en termes d'accès aux données collectées par des tiers privés et 2) l'encadrement des techniques d'encryptions.

Cette perspective sécuritaire est indissociable du contexte actuel, marqué, notamment, par trois phénomènes aux implications « cyber » majeures : le terrorisme, le « hacktivisme » et les cyberguerres. Elle est en outre très influencée par un manque de connaissances sur le cyberespace et ses dynamiques, souvent remarqué chez les preneurs de décisions gouvernementaux et les législateurs.

Enfin, il conviendra d'analyser dans le chapitre 4 l'approche aujourd'hui universellement privilégiée face aux enjeux de de la cybercriminalité, celle d'une gestion du risque plutôt que d'une prévention de l'acte : Wanda Capeller souligne ce glissement d'une société du risque (terme développé par le sociologue Ulrich Beck en 1986, à la suite de la catastrophe nucléaire de Tchernobyl) à une société du risque virtuel. Cette approche est déterminante dans la manière dont les preneurs de décision, publics, privés et individuels, agissent face à la cybercriminalité, notamment car la gestion du risque implique, comme réponse, une responsabilisation essentielle de la victime potentielle. Ce sont alors aux internautes, aux usagers, aux entreprises, de prendre les mesures pour se protéger, ce qui est diamétralement opposé à une vision intégrale de la prévention de la criminalité.

Cette différence absolument fondamentale recèle plusieurs implications importantes. Pour les auteurs tout d'abord, les efforts de prévention ne sont plus alors axés sur la nécessité de comprendre et mitiger les facteurs sociaux, environnementaux et personnels menant au développement de trajectoires criminelles et à la commission d'actes déviants et délictueux. Pour les victimes, notamment les groupes les plus vulnérables tels que les enfants, les femmes ou les minorités sexuelles, religieuses ou ethniques, l'essentiel des efforts de prévention vise à modifier leurs pratiques et usages d'Internet de manière à minimiser les risques de victimisation. Ce qui constitue, d'un point de vue éthique, une approche pouvant être, sur plusieurs points, une entrave à la liberté de ces acteurs. Il est intéressant de souligner que de telles approches, dans le monde « réel », seraient à juste titre l'objet de critiques, notamment si elles ne s'accompagnent pas d'un travail préventif agissant sur les auteurs potentiels de crimes.

Cependant, les récentes évolutions observées montrent une prise en charge plus multidimensionnelle de la sécurité dans le cyberespace, qui intègre de plus en plus des aspects de prévention et d'éducation (Malecki, 2017). Cependant, la situation dans laquelle nous nous trouvons aujourd'hui ne permet pas encore, en large mesure, de construire une approche basée sur des données probantes, celles-ci étant encore rares, succinctes et sujettes à des rapides évolutions. Par conséquent, le domaine de l'action publique en réponse à la cybercriminalité doit bâtir les moyens de cette approche de la politique publique basée sur des données probantes afin de construire une véritable approche préventive.

Contribution

Mettre fin au processus de l'émergence de la cybercriminalité: des délinquants motivés aux cyberattaques

Alex Kigerl
Ph. D, Chercheur et professeur adjoint en justice pénale et criminologie
Washington State University, États-Unis

Il faut passer par tout un processus d'étapes avant de tomber victime du piège de la cybercriminalité. Le délinquant potentiel doit être motivé à commettre un crime, il doit être techniquement capable d'entreprendre une cyberattaque, cette attaque doit réussir à atteindre sa cible sans être bloquée par les technologies de protection (filtres de pourriels, logiciels antivirus) et dans la plupart des cas, il y a le facteur humain qui nécessite qu'une personne arrive à tomber dans le piège de cette cyberattaque. Tout au long de ce processus, chaque étape présente une occasion de développer une ou plusieurs stratégies de prévention de la cybercriminalité.

Il existe des conditions structurelles et sociétales qui semblent liées à la cybercriminalité, tout comme des environnements propices à la commission de cybercrimes (chômage, internet par habitant). Une fois qu'un délinquant est suffisamment motivé et capable de commettre un délit, ce sont les efforts de dissuasion juridique et technologique qui réussiront à le persuader de renoncer ou réduire l'ampleur des attaques, ou encore d'aller les commettre ailleurs. Ces attaques en soi peuvent également être déjouées par le biais de technologies de prévention ou la sensibilisation des internautes à la sécurité informatique. Enfin, dans ce processus, les cybercriminels confirmés peuvent être poursuivis ou neutralisés, ce qui contribuera à prévenir des attaques futures jusqu'à ce que le vide laissé par le délinquant puni soit comblé par de nouveaux délinquants très zélés.

Bien évidemment, la meilleure solution serait de multiplier les efforts de prévention dès la première étape, en essayant de neutraliser dès le départ l'émergence des délinquants motivés, par le biais de changements structurels, d'incitations et d'opportunités. Malheureusement, la recherche à ce stade est très peu développée, la plupart des efforts d'intervention étant dirigées vers les technologies de protection, notamment la conception de logiciels de sécurité pour détecter toutes intrusions dans le réseau, repérer et mettre en quarantaine tout logiciel malveillant, empêcher des pourriels malveillants d'atteindre des millions de destinataires et signaler les noms de domaines Internet sur liste noire.

Le deuxième type d'effort couramment mis en œuvre pour lutter contre la cybercriminalité intervient dans la dernière étape de prévention : la neutralisation par le biais de mesures juridiques punitives. Les moyens légaux pour lutter contre la cybercriminalité sont plus complexes que ceux utilisés pour lutter contre les formes traditionnelles de criminalité dans la rue, car la cybercriminalité ne respecte pas les frontières entre les pays, encore moins les frontières entre les différentes juridictions juridiques qu'une cyberattaque peut survoler. Il est souvent difficile de convaincre les forces de l'ordre du pays d'origine du cybercriminel d'aider à sa poursuite, car nombreuses sont les nations qui refusent de coopérer. Les contrevenants sont également plus difficiles à retracer, car ils sont capables de dissimuler leur identité et leur location grâce à une myriade de moyens technologiques. Recueillir des preuves nécessite également des outils technologiques plus sophistiqués pour les enquêteurs.

Cependant, la recherche appliquée à la première étape du processus a beaucoup progressé au cours des dernières années en explorant des variables au niveau macro qui semblent être connectées et prédire l'activité cybercriminelle. Pourtant, du point de vue de la prévention, il convient de noter l'incertitude entourant l'ordre de causalité entre l'environnement à l'échelle macro où réside le cyberdélinquant et la tendance de ce dernier à commettre par la suite des crimes sur le cyberespace. Est-ce l'environnement qui crée des criminels motivés ou ces derniers contribuent-ils à l'environnement ? Existe-t-il une troisième variable à l'origine des deux ou s'agit-il d'une combinaison de tous ces éléments ?

Une grande partie des explorations à l'échelle macro en matière de cybercriminalité se sont fondées sur les États-nations comme unité d'analyse. Une de ces applications utilise une approche de regroupement pour catégoriser les pays en fonction de leur profil d'activités cybercriminelles (Kigerl, 2016). Ainsi, quatre catégories de pays ont été identifiées : les pays avec une faible cybercriminalité, les pays où sévit la fraude par avancement de frais, les pays où sévissent les attaques par hameçonnage et les pays où sont commis des actes de cybercriminalité sans gravité. Les pays avec une faible cybercriminalité sont en effet les moins actifs en termes de taux de cybercriminalité, mais ont aussi tendance à avoir les taux de PIB et de connexion Internet les plus bas. Les pays où sévit la fraude par avancement de frais, qui se spécialisent dans les demandes frauduleuses par courriel telles que la fraude nigériane pour convaincre à son insu une victime d'« avancer des fonds » en échange d'une offre intéressante, possèdent des taux de PIB et de connexion Internet très peu élevés. La fraude par avancement des frais ne nécessite que très peu de technique sophistiquée, car elle dépend principalement de la manipulation sociale plutôt que de logiciels malveillants ou autres attaques automatisées. Le Nigeria fait partie de ces pays classés dans les nations où sévit la fraude par avancement de frais.

Les nations spécialisées dans l'hameçonnage, dont le but est de tenter de frauder une victime en se faisant passer pour sa banque, afin de lui voler des informations d'identification confidentielles telles que ses coordonnées bancaires, sont généralement des nations plus riches avec une connexion Internet plus rapide. Techniquement plus sophistiquées, les escroqueries par hameçonnage utilisent des sites internet clones conçus pour être autant que possible identiques au site internet original qu'il cherche à repro-

duire afin d'enregistrer les touches frappées sur le clavier par les internautes ou l'information saisie dans les formulaires remplis par les victimes. Parmi ces nations, on peut citer notamment la Russie. Enfin, les nations spécialisées dans les actes de cybercriminalité sans gravité ont principalement recours aux pourriels ou au piratage numérique, et présentent les taux de PIB les plus élevés et le plus grand nombre d'internautes. Parmi ces nations, on retrouve les États-Unis et la Chine qui comptent une importante population et un grand nombre d'ordinateurs déjà connectés.

Cependant, il est tout aussi possible que cette dernière catégorie de pays où se produisent des actes de cybercriminalité sans gravité soit la cible d'activités cybercriminelles en raison du grand nombre d'appareils connectés à Internet et d'internautes, ce qui pourrait encourager les fraudeurs à passer l'action. Les pourriels sont généralement envoyés à partir de robots (botnets), soit des ordinateurs infectés par des logiciels malveillants capables d'envoyer des pourriels en masse au nom du spammeur, ce dernier ayant souvent le contrôle de milliers de machines infectées. Avec plus d'ordinateurs connectés, les nations les plus riches ont tendance à être les cibles les plus idéales pour ce type d'attaque. De plus, les nations avec des infrastructures technologiques plus performantes et plus de libertés politiques sont plus susceptibles de signaler des infections causées par des logiciels malveillants (Holt, Burruss, & Bossler, 2016). De même, au niveau fédéral aux États-Unis, l'utilisation d'Internet à la maison est associée à une plus grande fréquence de vols d'identité (Song, Lynch et Cochran, 2016).

Le nombre d'internautes par habitant dans un pays influence grandement les taux de cybercriminalité de cette nation, que l'activité cybercriminelle en question soit l'objet d'actes commis par des délinquants résidant au sein du pays ou qui utilisent simplement cette nation comme un canal pour commettre leurs attaques. Toutefois, la richesse et la prospérité économique jouent un rôle plus complexe en ce qui a trait à la cybercriminalité. En effet, les pourriels peuvent être classés entre des messages marketing ayant pour objectif de vendre des produits, des courriels frauduleux ou malveillants destinés à infecter les courriels des destinataires par le biais de logiciels malveillants. Les pourriels marketing sont plus courants dans les pays avec un PIB élevé, les pourriels frauduleux quant à eux sévissent plus souvent dans les pays avec un PIB plus faible et les pourriels malveillants peuvent être utilisés dans n'importe quel pays, peu importe le PIB (Kigerl, 2018). Une fois de plus, nous constatons que de nombreuses stratégies utilisées pour la fraude s'appuient sur la manipulation sociale, et sont moins coûteuses, car elles ne nécessitent pas de technologie chère ou d'équipements informatiques de haut niveau. Il est vraiment facile d'avoir recours à la fraude par courriel, c'est pour cette raison que les nations pauvres semblent privilégier le plus cette forme de cybercriminalité.

Le chômage peut également avoir une influence sur le nombre d'internautes. En soi, si le chômage tend à réduire le niveau de cybercriminalité d'une nation, une connexion facile à Internet tend à augmenter les attaques en la matière (Kigerl, 2012). Cependant, ces deux variables sont étroitement liées: les pays ayant un taux de chômage très élevé ont également tendance à avoir moins d'internautes. Si l'on considère les exceptions, l'impact sur l'activité cybercriminelle peut être différent. Par exemple, dans toutes les nations avec une connexion Internet plus facile, le chômage a une influence positive sur la cybercriminalité. Ainsi, un taux de chômage élevé peut être associé à des taux élevés de cybercriminalité uniquement si la connexion Internet est également facile. De toute évidence, les cybercriminels doivent pouvoir avoir accès à Internet et être suffisamment qualifiés technologiquement pour commettre des actes de cybercriminalité. Lorsqu'une nation compte de nombreux internautes, mais présente un fort taux de chômage, il est possible que cela encourage des délinquants ou des personnes avec de bonnes compétences technologiques à passer à l'action parce qu'ils n'arrivent pas à se générer des sources de revenus de manière légitime. Ils peuvent donc se tourner vers le cybercrime comme une source alternative aux revenus légaux.

L'identification des plus grands délinquants au niveau national en matière de cybercriminalité peut également dépendre si on mesure la cybercriminalité en termes absolus ou comme un taux dépendant de la taille de la population au sein d'un pays. Lorsque l'on mesure le piratage numérique et la contrefaçon de logiciels en fonction de la taille de la population d'un pays, les pays plus petits, pauvres et moins développés d'un point de vue technologique présentent des taux de piratage numérique plus élevés, mais une activité de piratage plus faible en termes absolus (Kigerl, 2013). Lorsque le piratage était mesuré en fonction du nombre absolu d'incidents dans le pays, les nations les plus riches avec un grand nombre d'internautes enregistraient la majorité des crimes. Cela suggère qu'un plus grand pourcentage de la population est impliqué dans des activités de piratage numérique dans les pays plus petits et moins riches, mais dans l'ensemble, la majorité des activités de piratage proviennent des pays plus riches et avec une connexion Internet plus facile. Les nations les plus pauvres comptent moins d'internautes, toutefois les internautes y résidant sont plus susceptibles d'avoir recours au piratage étant donné qu'ils n'ont pas les moyens de se payer des logiciels ou des films de manière légale. Cependant, dans les nations plus riches, le grand volume d'internautes implique en termes absolus qu'il y aura plus d'activités de piratage simplement parce qu'il y a plus d'utilisateurs Internet.

La recherche dans ce domaine est encore jeune, mais toutefois porteuse aujourd'hui de quelques idées sur les prochaines étapes de la recherche future et des interventions possibles qui pourraient déjà être mises en place pour prévenir la cybercriminalité en ciblant certaines de ces variables associées au niveau macro. La prévention de la cybercriminalité peut être ciblée à tout moment du processus d'émergence de la cybercriminalité. Jusqu'à présent, la majorité des efforts se sont concentrés autour de la dernière étape du processus, bien après que certains dommages aient déjà été causés. Il serait également judicieux de mobiliser des efforts de prévention additionnels pendant les premières étapes de survenance de la cybercriminalité.

Contribution

Les statistiques tronquées de la cybercriminalité

Benoît Dupont et Anne-Marie Côté
Professeur titulaire
Directeur scientifique du Réseau intégré sur la cybersecurité (SERENE-RISC)
Titulaire de la Chaire de recherche du Canada en sécurité, identité et technologie
Canada

La cybercriminalité occupe dorénavant une place prépondérante dans les médias et génère un flot continu d'inquiétudes au sein de la population, qui prend conscience de l'émergence de risques numériques associés aux nombreux services en ligne qui agrémentent sa vie quotidienne. À ce titre, la cybercriminalité représente certainement l'idéal-type de la délinquance du 21e siècle. Les gouvernements, les entreprises et les consommateurs du monde entier sont préoccupés par les nombreuses menaces qui pèsent sur les informations personnelles, le carburant de l'économie numérique (Côté et al., 2016). Il est toutefois surprenant de constater le décalage qui existe entre les messages alarmistes diffusés par les autorités et les entreprises sur la cybercriminalité, traduisant l'importance objective de ce phénomène, et le manque de fiabilité et de robustesse des statistiques mobilisées pour quantifier les préjudices subis et motiver l'urgence d'agir.

Le terme de « cybercriminalité » qui est rentré dans l'usage courant contribue indirectement à cette « quantophrénie » (Sorokin, 1959). Son ambiguïté sémantique, qui recouvre des comportements extrêmement variés allant de la distribution de pédopornographie au piratage informatique en passant par la fraude en ligne et de multiples formes d'attaques rendant les sites internet indisponibles, engendre en effet de nombreux questionnements et incertitudes quant à sa signification réelle (UNODC, 2013). Ceux-ci sont amplifiés par la complexité technique inhérente aux différentes formes de délinquance en ligne, qui exige une expertise encore peu répandue pour en comprendre les rouages internes. Il en résulte que le discours public sur la cybercriminalité s'appuie principalement sur le recours intensif à des statistiques dont la nature, la provenance et la qualité s'avèrent extrêmement problématiques (Côté et al., 2016 ; Flôrencio et Herley, 2013). La prolifération de statistiques sur la cybercriminalité doit alors s'accompagner d'un examen critique de leur origine et de leur validité.

Parmi les principales objections soulevées, citons l'emprise des acteurs privés de la cybersécurité produisant des chiffres selon des méthodologies opaques destinés à susciter un sentiment d'insécurité propice à la commercialisation de leurs produits et services (Dupont, 2016), le recours fréquent à des sondages d'opinion auprès d'échantillons réduits de répondants pour quantifier la prévalence d'un phénomène inégalement distribué (Furnell, Emm et Papadaki, 2015), le manque de comparabilité des statistiques collectées par les divers acteurs qui mobilisent des méthodologies d'analyse extrêmement diversifiées, la fréquence irrégulière de collecte des données empêchant l'analyse rigoureuse de l'évolution des phénomènes étudiés (Reep-van den Bergh et Junger, 2018), la difficulté de prendre en compte les comportements criminels qui comprennent à la fois des composantes en ligne et hors-ligne (Levi, 2017), ou encore le phénomène de sous-déclaration systématique des cybercrimes par leurs victimes aux organisations policières (Caneppele et Aebi, 2017).

Par ailleurs, la critique des statistiques de la cybercriminalité et de leurs modes de production s'est aussi penchée sur les effets indirects qu'une mesure imprécise de ce phénomène produit sur la quantification du volume global de la délinquance. Certains auteurs ont ainsi émis l'hypothèse que la baisse marquée de la criminalité traditionnelle enregistrée depuis la moitié des années 1990 dans les pays occidentaux devait être analysée comme le résultat d'une interaction avec les formes émergentes de délinquance numérique (Tcherni et al., 2016). Sans apporter de preuve définitive du déplacement de la délinquance de ses sphères d'activités traditionnelles vers les cybercrimes, il est indéniable que le volume actuel de ces derniers, qui représente selon les pays du tiers à la moitié de l'ensemble des crimes, remet sérieusement en question le récit criminologique dominant d'une chute drastique de la criminalité depuis une vingtaine d'années (Caneppele et Aebi, 2017). Autrement dit, le déficit de statistiques fiables sur la cybercriminalité nous aurait induit à tirer des conclusions erronées de l'évolution de la délinquance globale depuis deux décennies.

L'effort fait par le Bureau national de la statistique britannique afin de redresser la situation est à cet égard éloquent de l'approximation qui a frappé les chiffres de la cybercriminalité jusqu'à une période relativement récente. La nouvelle méthodologie qui fut adoptée pour l'édition 2015 de l'Enquête nationale de victimisation révéla ainsi qu'aux 6,5 millions de crimes traditionnels attendus venaient s'ajouter 7,6 millions de cybercrimes et d'incidents frauduleux à composante numérique, ce qui doubla sans préavis le volume annuel des chiffres de la criminalité dans ce pays (TNS, 2015). Rien ne semble indiquer que cette situation soit propre à la Grande Bretagne, et la disponibilité croissante de statistiques plus robustes pointe au contraire vers une tendance assez semblable dans la majorité des pays occidentaux (Reep-van den Bergh et Junger, 2018).

Les critiques méthodologiques adressées par la communauté scientifique à l'endroit des statistiques sur cybercriminalité ne relèvent pas uniquement d'un débat d'experts. À l'heure où les

gouvernements du monde entier se dotent de stratégies de cybersécurité ambitieuses incluant souvent des dispositions juridiques et réglementaires de prévention et de contrôle de la cybercriminalité, et que les budgets alloués à la mise en œuvre de ces politiques publiques et de ces programmes atteignent des centaines de millions, voire des milliards de dollars, les répercussions de l'utilisation de statistiques erronées sur la prise de décision sont loin d'être triviales (Anderson et al., 2012 ; Dupont, 2016). Les organismes publics, parapublics et privés, incluant les compagnies d'assurance, ainsi que les médias, sont dans l'impossibilité de présenter aux décideurs politiques et économiques, et à l'opinion publique, un tableau suffisamment précis des divers problèmes recensés pour motiver des interventions basées sur des données probantes.

Deux exemples serviront à préciser ce constat. Le premier est celui de l'impact de la cybercriminalité, qui doit être distingué de sa simple comptabilisation. En effet, si les enquêtes de victimisation menées récemment nous permettent de mesurer le nombre de personnes et d'organisations affectées par les diverses formes de cybercriminalité avec une précision satisfaisante, l'ampleur des pertes financières subies par celles-ci et les coûts associés à la restauration des systèmes et données compromis restent très difficiles à déterminer. Anderson et al. (2013) distinguent ainsi le volume de la cybercriminalité de l'impact de cette dernière, qui est mesuré à travers les revenus criminels générés par les délinquants, les pertes directes assumées par les victimes, les pertes indirectes qui incombent aux opérateurs des systèmes techniques exploités par les attaquants, et les coûts induits par les investissements requis afin de protéger les infrastructures numériques contre de futures attaques. Comme le soulignent les auteurs dans leur tentative d'évaluer aussi rigoureusement que possible les coûts de la cybercriminalité, les études disponibles ne permettent pas encore de calculer ces quatre dimensions. Il en découle que les stratégies de lutte contre la cybercriminalité sont élaborées sur la base d'intuitions et de données assez superficielles plutôt que sur des modélisations permettant de maximiser l'impact des interventions qui sont privilégiées.

Notre second exemple illustre comment des collaborations fructueuses peuvent être établies entre chercheurs universitaires issus de disciplines multiples et analystes provenant du secteur privé afin de produire des statistiques de la cybercriminalité qui éclairent le débat plus qu'elles ne l'obscurcissent. La collaboration d'informaticiens autrichiens, de criminologues canadiens, d'une association internationale dédiée à la lutte contre l'hameçonnage (l'Anti-Phishing Working Group) et d'une entreprise canadienne de cybersécurité (Go Secure) a ainsi permis de mesurer les flux financiers convergeant vers les cyberdélinquants qui exploitent des rançongiciels[15] (Paquet-Clouston et al., 2018). Nous avons ainsi pu établir que les 35 familles de rançongiciels les plus actives avaient reçu au cours de la période 2013-2017 un peu plus de 12 millions de dollars en rançons payées en bitcoins, et que les trois groupes de cybercriminels les plus performants avaient capté 88 % des profits. Ces données démontrent que le problème des rançongiciels, qui a reçu en 2017 et 2018 une couverture médiatique très intense, est probablement moins catastrophique qu'annoncé. Elles suggèrent également aux autorités publiques chargées de la prévention et des enquêtes en matière de cybercrime des pistes d'intervention se focalisant sur une poignée d'acteurs criminels clairement identifiés responsables de l'immense majorité des préjudices subis, qu'ils soient directs ou indirects.

Ces deux exemples démontrent à quel point il devient nécessaire d'associer les entreprises qui possèdent et commercialisent des produits et des services de cybersécurité aux efforts de mesure de la cybercriminalité déployés par les organismes statistiques gouvernementaux. Si nous avons souligné l'instrumentalisation que les entreprises de cybersécurité font parfois des chiffres qu'elles publient, force est d'admettre qu'elles disposent d'outils d'observation et d'analyse uniques leur permettant de mesurer les tendances de la cybercriminalité à l'échelle internationale. Combinés aux données provenant des enquêtes de victimisation plus classiques et des statistiques policières, ces chiffres pourraient être mobilisés de manière désintéressée afin de produire une mesure fiable de la cybercriminalité qui favoriserait des interventions préventives et répressives plus sélectives et efficaces.

Notes

9 L'hameçonnage est un terme général utilisé pour décrire l'envoi, par des criminels, de courriels, de messages textes et de sites Web qui sont conçus pour avoir l'air de provenir d'entreprises, d'institutions financières et d'organismes gouvernementaux légitimes bien connus et qui visent à tromper le destinataire afin de lui soutirer des renseignements personnels, financiers ou de nature délicate (GRC, 2018).

10 Les rançongiciels (ransomware) sont des logiciels malveillants qui prennent en otage les données d'un utilisateur en bloquant son accès à cette information sur son ordinateur ou sur son appareil mobile jusqu'à ce qu'il utilisateur ait versé une rançon.

11 Une définition de ce type de crime est donnée dans la section dédiée à la fraude dans le chapitre 3.

12 Le terme de revenge porn désigne la diffusion en ligne, sans le consentement de la personne y apparaissant, de matériel pornographique produit dans un cadre privé. Typiquement, il s'agit d'images ou de vidéos intimes, et les victimes sont, dans leur très grande majorité, des femmes ou des jeunes filles.

13 Botnet est un terme qui fait référence à un ensemble ou un réseau de robots informatiques ou bots, exécutés de manière automatique et dont le créateur peut contrôler tous les ordinateurs / serveurs infectés à distance.

14 Le Deep Web est formé de l'ensemble des pages non indexées et constitue la majeure partie du cyberespace. Si une majorité de ces pages ne supportent aucune activité frauduleuse, une partie peut en héberger : on fera alors plutôt appel au terme Dark Web, qui désigne les pages hébergeant du contenu hors de toute régulation.

15 Il s'agit d'applications malveillantes qui encryptent les données de leurs victimes et exigent le paiement d'une rançon en échange de la clé de déchiffrement.

Références

Chapitre 2 : Les crimes dans un monde numérique

Alexander van Deursen, & Jan van Dijk. (2010). Internet skills and the digital divide. New Media & Society, 13(6), 893-911. https://doi.org/10.1177/1461444810386774

Alzouma, G. (2013). Dimensions of the mobile divide in Niger. In M. Ragnedda & G. Muschert (Éd.), The Digital Divide. The Internet and social inequality in international perspective. Routledge.

Banque Mondiale. (2017). Indicateurs de développement dans le Monde.

Bates, S. (2015). "Stripped": An Analysis of Revenge Porn Victims' Lives after Victimization (Masters Degree). Simon Fraser University, Burnaby, Canada.

Boudreau, J., & Chau, M. N. (2016, août 10). Spyware Deluge Hits Vietnam Sites Amid South China Sea Spat. Bloomberg.

Broadhurst, R., & Chang, L. (2013). Cybercrime in Asia: Trends and Challenges. In Handbook of Asian Criminology.

Business Software Alliance. (2012). Shadow Market. 2011 BSA global software piracy study.

Business Software Alliance. (2016). BSA Global Software Survey 2016.

Camerini, A.-L., Schulz, P. J., & Jeannet, A.-M. (2017). The social inequalities of Internet access, its use, and the impact on children's academic performance: Evidence from a longitudinal study in Switzerland. New Media & Society,

Canadian Chamber of Commerce. (2017). Cyber Security in Canada.

Castells, M. (2002). The Internet Galaxy: Reflections on the Internet. Oxford: Oxford University Press.

Center for Strategic and International Studies. (2014). Net Losses: Estimating the Global Cost of Cybercrime.

Chalfant, M. (2018, février 21). Cyber crime costs global economy $600B annually, experts estimate. The Hill.

Chang, L. (2017). Cybercrime and Cyber Security in ASEAN. In Comparative Criminology in Asia. Springer International Publishing.

Cheng, R. (2017, mars 28). Cybercrime in China: Online Fraud. Forbes.

CIPC. (2005). Prévenir la Délinquance en Milieu Urbain et Auprês des Jeunes. Montreal.

CIPC. (2010). Prevención de la criminalidad y seguridad cotidiana: tendencias perspectivas. Montréal, QC, Canada. Consulté à l'adresse http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/prevencion_de_la_criminalidad_y_la_seguridad_cotidiana_ESP_01.pdf

CIPC. (2011). Practical Approaches to Urban Crime Prevention. Montreal, QC, Canadá. Consulté à l'adresse https://www.unodc.org/pdf/criminal_justice/Practical_Approaches_to_Urban_Crime_Prevention.pdf

CIPC. (2012a). Recueil international d'expériences en prévention de la violence et la criminalité chez les jeunes: Pratiques de pays occidentaux (p. 1-52). Montréal, Canada: CIPC - Centre International sur la Prévention de la Criminalité. Consulté à l'adresse http://www.crime-prevention-intl.org/uploads/media/Recueil_de_pratiques_MSP_-_version_finale.pdf

CIPC. (2012b). Recueil international d'expériences en prévention de la violence et la criminalité chez les jeunes: Pratiques de pays occidentaux (p. 1-52). Montréal, Canada: CIPC - Centre International sur la Prévention de la Criminalité. Consulté à l'adresse http://www.crime-prevention-intl.org/uploads/media/Recueil_de_pratiques_MSP_-_version_finale.pdf

Clavel, T. (2016, septembre 26). Can Latin American Governments Keep Up with Cyber Criminals?

Cobb, S. (2015). Sizing Cybercrime: Incidents and Accidents, Hints and Allegations. In Virus Bulletin Conference.

Connolly, A. (2018, avril 4). Companies will now have to tell Canadian consumers when their privacy is breached — and do it quickly. Global News.

Cybersecurity Intelligence. (2015, septembre 22). The Shocking State of Cybercrime in Russia.

David Barnard-Wills, & Debi Ashenden. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. Space and Culture, 15(2), 110-123. https://doi.org/10.1177/1206331211430016

Deutsche Telekom. (2017). Cybercrime: What to expect in 2018.

Diamond, B., & Bachman, M. (2015). Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology. International Journal of Cyber Criminology, 9(1).

Diario do Comercio. (2015, juillet 28). Numero de notificacoes incidentes de seguranca ciberneticos cresceu 197%.

Dijk, J. (2012). The Evolution of the Digital Divide. The Digital Divide turns to Inequality of Skills and Usage. Digital Enlightment Yearbook 2012, p. 57-75.

Dimaggio, P., Hargittai, E., Celeste, C., & Shafer, S. (2004). Digital inequality: From unequal access to differentiated use. In Social Inequality. Russell Sage Foundation.

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., William Welburn, J., & Winkelman, Z. (2018). Estimating the Global Cost of Cyber Risk. Methodology and Examples. RAND.

Electronic Frontier Foundation. (1996). A Declaration of the Independence of Cyberspace.

ESET. (2017). State of Cybersecurity in APAC: Small Businesses, Big Threats.

European Union Agency For Network and Information Security. (2018). ENISA Threat Landscape Report 2017.

Federal Bureau of Investigation - Internet Crime Complaint Center. (2016). 2016 Internet Crime Report.

Finkelstein, L. S. (1995). What Is Global Governance? Global Governance, 1(3), 367-372.

Folha de S. Paolo. (2015). Pequenas e médias empresas são os maiores alvos de ataques cibernéticos; saiba como se prevenir.

Forcepoint. (2016). 2016 Global Threat Report.

Fuchs, C. (2009). The Role of Income Inequality in a Multivariate Cross-National Analysis of the Digital Divide. Social Science Computer Review, 27(1), 41-58.

Fuchs, C., & Horak, E. (2008). Africa and the digital divide. Telematics and Informatics, 25(2), 99-116. https://doi.org/10.1016/j.tele.2006.06.004

Galeotti, M. (2011, novembre 21). Why are Russians excellent cybercriminals? the Moscow News.

Gañán, C., Ciere, M., & van Eeten, M. (2017). Beyond the pretty penny: the Economic Impact of Cybercrime. In NSPW 2017.

Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2017). World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks. FireEye.

Grabosky, P. (2004). The Global Dimension of Cybercrime. Global Crime, 6(1), 146-157.

Grant Blank, & Christoph Lutz. (2016). Benefits and harms from Internet use: A differentiated analysis of Great Britain. New Media & Society, 20(2), 618-640. https://doi.org/10.1177/1461444816667135

Griffin, A. (2017, septembre 8). Equifax Hack: huge scale of cyber attack means that many people will have had personal details stolen without knowing. The Independent. Consulté à l'adresse http://www.independent.co.uk/life-style/gadgets-and-tech/news/equifax-hack-credit-card-safety-security-am-i-part-of-it-in-what-to-do-latest-millions-a7935831.html

GSMA. (2015). The Mobile Economy. Sub-Saharian Africa.

Halder, D., & Jaishankar, K. (2016). Cyber Crimes against Women in India. New Dehli, Inde: SAGE Publishing.

Hargittai, E. (2011). Second-Level Digital Divide: Mapping Differences in People's Online Skills. Présenté à 29th TPRC COnference.

Harney, K. R. (2017, novembre 22). Data breach at Equifax prompts a national class-action suit. Washington Post. Consulté à l'adresse https://www.washingtonpost.com/realestate/data-breach-at-equifax-prompts-a-national-class-action-suit/2017/11/20/28654778-ce19-11e7-a1a3-0d1e45a6de3d_story.html

Helsper Ellen Johanna, & Eynon Rebecca. (2013). Digital natives: Where is the evidence? British Educational Research Journal, 36(3), 503-520. https://doi.org/10.1080/01411920902989227

Insurance Information Institute. (2017). Facts + Statistics: Identity theft and cybercrime.

International Telecommunication Union. (2017a). Global Cybersecurity Index (GCI) 2017.

International Telecommunication Union. (2017b). ICT Facts and Figures 2017. Genève, Suisse.

International Telecommunication Union. (2017c). ICT trends in the LDCs. Consulté à l'adresse https://www.itu.int/en/ITU-D/LDCs/Pages/ICT-Facts-and-Figures-2017.aspx

Jaishankar, K. (2011). Cyber criminology exploring Internet crimes and criminal behavior. Boca Raton, Fla. ; London: Boca Raton, Fla. ; London : CRC.

Jaishankar, K., & Halder, D. (2011). Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, USA: IGI Global.

Jardine, E. (2015). Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime. Global Commission on Internet Governance, No16.

Kaspersky. (2015). Financial Cyberthreats in 2014.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. Social Science Computer Review, 30(4), 470-486.

Kigerl, A. (2016). Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates. International Journal of Cyber Criminology, 10(2), 147-169.

Koops, B.-J. (2010). The Internet and its Opportunities for Cybercrime (SSRN Scholarly Paper No. ID 1738223). Rochester, NY: Social Science Research Network. Consulté à l'adresse https://papers.ssrn.com/abstract=1738223

Levi, M. (2017). Assessing the trends, scale and nature of eco-

nomic cybercrimes: overview and Issues. Crime, Law and Social Change, 67(1), 3-20. https://doi.org/10.1007/s10611-016-9645-3

Lewins, D. (2017, avril 7). Cybercrime: The Spark Which Started Russia's Cyber Crusade.

Lewis, L., Weinland, D., & Peel, M. (2016, septembre 19). Asia hacking: Cashing in on cyber crime. Financial Times.

Liaropoulos, A. N. (2017). Cyberspace Governance and State Sovereignty. In G. C. Bitros & N. C. Kyriazis (Éd.), Democracy and an Open-Economy World Order (p. 25-35). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-52168-8_2

Malecki, E. J. (2017). Real people, virtual places, and the spaces in between. Digital Support Tools for Smart Cities, 58, 3-12. https://doi.org/10.1016/j.seps.2016.10.008

Malwarebytes. (2017). 2017-State of Malware Report.

Manjoo, F. (2017, septembre 8). Seriously, Equifax? This Is a Breach No One Should Get Away With. The New York Times. Consulté à l'adresse https://www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html

McAfee. (2018). Economic Impact of Cybercrime – No Slowing Down.

Meckbach, G. (2018, février 1). Invasion of privacy class-action against Equifax proceeds in Ontario. Consulté 24 avril 2018, à l'adresse https://www.canadianunderwriter.ca/legal/invasion-privacy-class-action-equifax-proceeds-ontario-1004126839/

Medina, M., & Molist, M. (2017). Ciberseguridad: tendencias 2017. Valence, Espagne: Universidad Internacional de Valencia.

Microsoft. (2017). Microsoft Security Intelligence Report: China.

Muggah, R., & Thompson, N. (2015, septembre 17). Brazil's Cybercrime Problem. Foreign Affairs.

Murphy, B. (2018, mars 13). People Are Suing Equifax in Small-Claims Court and It's Totally Brilliant. Here's Why. Inc.com. Consulté à l'adresse https://www.inc.com/bill-murphy-jr/people-are-suing-equifax-in-small-claims-court-its-totally-brilliant-heres-why.html

Nicola Henry, & Anastasia Powell. (2016). Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law. Social & Legal Studies, 25(4), 397-418. https://doi.org/10.1177/0964663915624273

Norton - Symantec. (2013). 2013 Norton Cyber Security Insights Report.

Norton - Symantec. (2016). 2016 Norton Cyber Security Insights Report.

Norton - Symantec. (2017). 2017 Norton Cyber Security Insights Report.

Observatorio de la ciberseguridad en América latina y el Caribe. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Washington, DC: Organisation des États Américains & Banque Interaméricaine de Développement.

OCDE. (2017). Perspectives de l'économie numérique de l'OCDE 2017. Paris, France.

Oliver Wyman. (2017). Cyber Risk in Asia-Pacific. The Case for Greater Transparency. Asia Pacific Risk Center.

Pasricha, J. (2016). Violence Online In India: Cybercrimes Against Women & Minorities on Social Media. Fredom House.

Patton, D. U., Hong, J. S., Ranney, M., Patel, S., Kelley, C., Eschmann, R., & Washington, T. (2014). Social media as a vector for youth violence: A review of the literature. Computers in Human Behavior, 35, 548-553. https://doi.org/10.1016/j.chb.2014.02.043

Pereira, B. (2016). La lutte contre la cybercriminalité: De l'abondance de la norme à sa perfectibilité. The fight against cybercrime: From the abundance of the standard has its perfectibility, 30(3), 387-409. https://doi.org/10.3917/ride.303.0387

Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? Aggression and Violent Behavior, 34, 193-200. https://doi.org/10.1016/j.avb.2017.01.012

Pew Research Centre. (2014). Online Harassment.

Pierson, D. (2017, septembre 8). Caught up in the Equifax hack? Here's one thing you can do to protect yourself. LA Times. Consulté à l'adresse http://www.latimes.com/business/la-fi-equifax-freeze-20170908-story.html

Ponemon Institute LLC. (2016). 2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB).

PwC. (2016). Global Economic Crime Survey 2016.

PwC. (2018). Pulling fraud out of the shadows: Global Economic Crime and Fraud Survey 2018.

Red24. (2015). 2015 Threat Forecast.

RSA. (2016). 2016: Current State of Cybercrime.

Scalar. (2018). Results of the 2018 Scalar Security Study.

Shaw, Margaret. (2001). Investing in Youth : International Approaches to Preventing Crime and Victimization. Montreal, Canada: International Center for the Prevention of Crime.

Shaw, Mark. (2018, janvier 9). Known unknowns: the threat of cybercrime in Africa.

Shiloh, J., & Fassassi, A. (2017, juillet 7). Cybercrime in Africa:

Facts and figures. Consulté 15 février 2018, à l'adresse http://www.scidev.net/index.cfm?originalUrl=/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html&

Singer, P., & Friedman, A. (2014). Cybersecurity and Cyberwar. Oxford: Oxford University Press.

Speer, D. (2000). Redefining borders: The challenges of cybercrime. Crime, Law and Social Change, 34, 259-273.

Stansbury, M. (2003). Access, Skills, Economic Opportunities, and Democratic Participation: Connecting Four Facets of the Digital Divide Through Research. In Proceedings of the Annual Conference of CAIS / Actes du congrès annuel de l'ACSI.

Stewart, E. (2018, février 7). Elizabeth Warren warns Equifax could « wiggle off the hook » for users' credit data getting hacked. Vox. Consulté à l'adresse https://www.vox.com/policy-and-politics/2018/2/7/16984522/elizabeth-warren-equifax-data-breach-cfpb

Stoyanov, R. (2015). Russian Financial Cybercrime: How it Works. Kaspersky.

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? International Journal for Crime, Justice and Social Democracy, 6(2), 17-33.

Sweet, K. (2018, mars 1). Equifax finds additional 2.4 million in U.S. impacted by 2017 data breach. The Star. Consulté à l'adresse https://www.thestar.com/business/economy/2018/03/01/equifax-finds-additional-24-million-in-us-impacted-by-2017-data-breach.html

Symantec. (2016). Cyber Crime & Cyber Security Trends in Africa.

Symantec. (2018). 2018 Internet Security Threat Report.

TNS opinion & political. (2017). Special Eurobaromter 464a. European's attitudes towards cyber security. Commission Européenne.

Trend Micro. (2015). Ascending the Ranks The Brazilian Cybercriminal Underground in 2015.

Trend Micro - Organisation des États Américains. (2013). Latin American and Caribbean Cybersecurity Trends and Government Responses.

Trend Micro, & Interpol. (2017). Cybercrime in West Africa. Poised for an Underground Market.

Turner, K. (2017, septembre 13). The Equifax hacks are a case study in why we need better data breach laws. Consulté 23 avril 2018, à l'adresse https://www.vox.com/policy-and-politics/2017/9/13/16292014/equifax-credit-breach-hack-report-security

United Nations Economic Commission for Africa. (2014). Tackling the challenges of cybersecurity in Africa.

UNODC. (2013). Comprehensive Study on Cybercrime.

van Deursen, A. J., & van Dijk, J. A. (2013). The digital divide shifts to differences in usage. New Media & Society, 16(3), 507-526. https://doi.org/10.1177/1461444813487959

van Dijk, J., & Hacker, K. (2003). The Digital Divide as a Complex and Dynamic Phenomenon. The Information Society, 19(4), 315-326. https://doi.org/10.1080/01972240309487

Wanda Capeller. (2001). Not Such a Neat Net: Some Comments on Virtual Criminality. Social & Legal Studies, 10(2), 229-242. https://doi.org/10.1177/a017404

Warschauer, M. (2004). Technology and social inclusion: Rethinking the digital divide. MIT press.

Wattles, J., & Larson, S. (2017, septembre 16). How the Equifax data breach happened: What we know now. CNN.

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J.-L. (2017). Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap. Deviant Behavior, 1-16. https://doi.org/10.1080/01639625.2017.1411030

WHO. (2015). Preventing youth violence: an overview of the evidence. Geneva.

Yar, M. (2006). Cybercrime and society. https://doi.org/10.4135/9781446212196

Zweig, J., Dank, M., Lachman, P., & Yahner, J. (2013). Technology, Teen Dating Violence and Abuse, and Bullying. Washington, DC, USA: Urban Institute - Justice Policy Center.

Contributions

Mettre fin au processus de l'émergence de la cybercriminalité

Holt, T. J., Burruss, G. W., and Bossler, A. M. (2016) Assessing the macro-level correlates of malware infections using a routine activities framework. International journal of offender therapy and comparative criminology: 0306624X16679162.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. Social Science Computer Review, 30(4), 470-486.

Kigerl, A. (2013). Infringing Nations: Predicting Software Piracy Rates, BitTorrent Tracker Hosting, and P2P File Sharing Client Downloads Between Countries. International Journal of Cyber Criminology, 7(1), 62-80.

Kigerl, A. (2016). Cybercrime Nation Typologies: K-Means Clustering of Countries Based on Cybercrime Rates. International Journal of Cyber Criminology, 10(2), 147-169.

Kigerl, A. (2018). Routine Activity Theory and Malware, Fraud, and Spam at the National Level. Unpublished manuscript.

Song, H., Lynch, M. J., & Cochran, J. K. (2016). A macro-social exploratory analysis of the rate of interstate cyber-victimization. American Journal of Criminal Justice, 41(3), 583-601.

Les statistiques tronquées de la cybercriminalité

Anderson R., Barton C., Böhme R., Clayton R., Van Eeten M., Levi M., Moore T., & Savage S. (2013), « Measuring the Cost of Cybercrime », The economics of information security and privacy, Berlin, Springer: 265-300.

Caneppele, S., & Aebi, M. F. (2017). Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. Policing: A Journal of Policy and Practice.

Côté, A.M., Bérubé, M. Et Dupont, B. (2016). Statistiques et menaces numériques : comment les organisations quantifient la cybercriminalité. Réseaux.

Dupont, B. (2016). Des effets perturbateurs de la technologie sur la criminologie. Revue Internationale de Criminologie et de Police Technique et Scientifique, 69(3): 305-322.

Florêncio D., & Herley C. (2013), « Sex, lies and cyber-crime surveys », Economics of Information Security and Privacy III, New York, Springer, p. 35-53.

Furnell S., Emm D., & Papadaki M. (2015), "The challenge of measuring cyber-dependent crimes", Computer Fraud & Security, 2015(10), p. 5-12.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and Issues. Crime, Law and Social Change, 67(1), 3-20.

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2018). Ransomware payments in the Bitcoin ecosystem. arXiv, https://arxiv.org/abs/1804.04080.

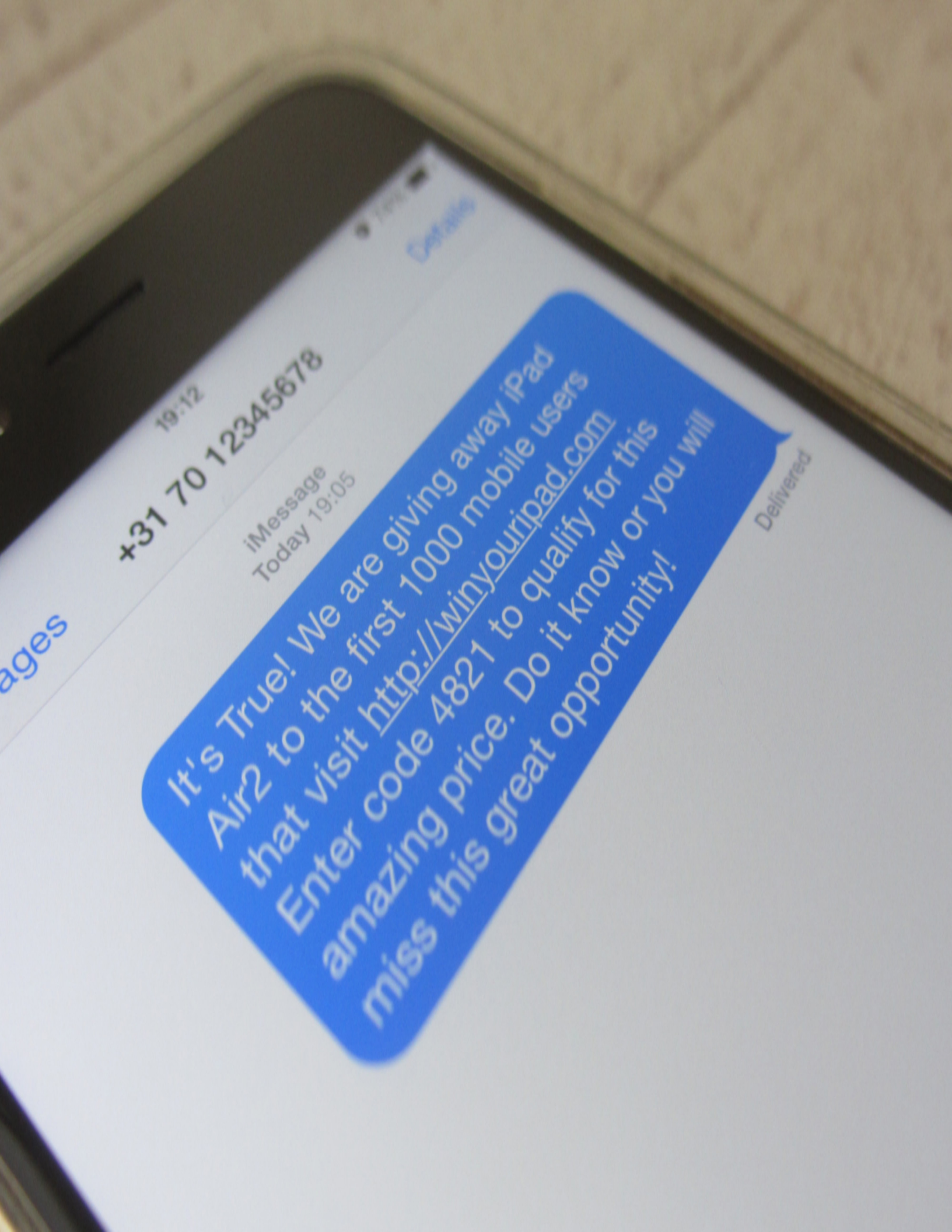
Reep-Van Den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime Science, 7(1), 5.

Sorokin P. (1959), Tendances et déboires de la sociologie américaine, Paris, Éditions Montaigne.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: is cyberspace hiding a crime wave?. Justice Quarterly, 33(5), 890-911.

TNS (2015). CSEW fraud and cyber-crime development: field trial, Newport, Crime Survey for England & Wales.

UNODC (2013). Comprehensive study on cybercrime, New York, Organisation des Nations Unies.


19:12
+31 70 12345678
Details
iMessage
Today 19:05
It's True! We are giving away iPad Air2 to the first 1000 mobile users that visit http://winyouripad.com Enter code 4821 to qualify for this amazing price. Do it know or you will miss this great opportunity!
Delivered

CHAPITRE 3

CYBERCRIMES, CYBERDÉLIQUANTS ET CYBERVICTIMES

Ce troisième chapitre fait l'état des lieux de ce qui se fait aujourd'hui dans la recherche en criminologie sur la cybercriminalité. Qu'entend-on par cybercriminalité? Que sait-on sur les différents cybercrimes? Qui en sont les auteurs et qui en sont les victimes? Autant de questions que les criminologues se posent et pour lesquelles ils cherchent à voir si les théories criminologiques traditionnellement utilisées pour comprendre la délinquance et la victimisation nous sont utiles dans ce nouvel environnement qu'est le cyberespace ou bien s'il est aujourd'hui nécessaire de concevoir une nouvelle approche afin de mieux appréhender ce sujet. Après avoir regardé les différentes perspectives définitionnelles que nous livre la science ainsi que les principales théories appliquées pour comprendre les divers cybercrimes, nous allons par la suite chercher à mieux connaître les avancées de la criminologie sur trois phénomènes en particulier : le piratage informatique, la cyberfraude et les cyberviolences.

Introduction

Le développement massif de ces technologies ainsi que les caractéristiques spécifiques à Internet ont une grande influence sur l'expression de nos interactions sociales (Holt & Bossler, 2014) en même temps qu'il crée de nouvelles opportunités, tant pour des activités légales que pour des activités criminelles et déviantes (Yar, 2006). Grabosky et al. (2001), en rappelant d'ailleurs le principe fondamental de la criminologie qui veut que le crime et les criminels suivent les opportunités, rapportent que la croissance fulgurante des technologies informatiques et d'Internet, a permis une augmentation des opportunités criminelles.

En effet, le relatif anonymat d'Internet, sa facilité d'utilisation ainsi que son caractère transnational et transfrontalier sont autant de spécificités qui permettent à nombre de délinquants d'y voir l'occasion pour accomplir des méfaits (Quéméner et Ferry, 2009; Prates et al., 2013). Ceux-ci exploitent alors le fait que le cyberespace fournit la possibilité de disséminer l'information largement, rapidement et à bon marché (Bryant et Bryant, 2014). Wall (2005) a d'ailleurs fait une liste de six facteurs reliés à Internet et qui ont un impact sur les comportements délinquant et déviant. Le premier facteur soulevé par Wall (2005) est la globalisation qui permet aux criminels de commettre des actes au-delà des frontières traditionnelles. Cette globalisation aura alors une incidence sur l'application de la loi et la culture policière au niveau local, nous parlerons alors de glocalisation. Ensuite, il y a le facteur des réseaux distribués, qui va permettre la création de nouvelles opportunités de relations commerciales et de rencontres mais qui va également engendrer de nouvelles opportunités de victimisation. En même temps, ce flux important d'informations en continu va rendre difficile l'identification et la compréhension de nouvelles formes de risque. Le caractère à la fois synoptique et panoptique[16] d'Internet a également un impact sur le comportement criminel en créant de nouvelles occasions de victimisation. En effet, le délinquant va pouvoir surveiller sa victime et commettre un crime sans être au contact physique de cette dernière. Internet crée ainsi des relations asymétriques, en ce sens que le lien délinquant/victime se trouve déséquilibré. En même temps, la relation asymétrique résidera dans l'opportunité accrue de multiplier les incidents criminels de faible envergure qui ne seront pourtant pas considérés par le système judiciaire et qui ne susciteront aucune mobilisation du système justice/police alors même que, regroupés, ces incidents représenteront une activité criminelle significative. Aussi, chaque transaction effectuée sur Internet va laisser une trace. Ceci combiné à un accès privilégié à la technologie pour certains va faire en sorte que quelques « data double » vont être particulièrement enviables. Si cette caractéristique d'identité virtuelle s'avère très utile pour les forces de l'ordre, elle génère en revanche de nouvelles opportunités pour les vols d'identité. Finalement, à côté des changements dans la nature des opportunités criminelles, Internet va également induire des transformations dans l'organisation des comportements criminels dans le cyberespace. Ainsi, des individus isolés sont capables de commettre des crimes importants dans le cyberespace alors même qu'ils n'en auraient pas eu les moyens (financier et organisationnel) dans le monde réel. En effet, la technologie et Internet mettent en réseau des délinquants solitaires, leur permettant alors de commettre des activités criminelles d'une envergure mondiale.

Cependant, aujourd'hui, notre compréhension des dimensions criminelles d'Internet et de la cybercriminalité en général est largement répandue et entretenue par les médias de masse (Wall, 2001; Yar, 2006; Leman-Langlois, 2006). Une telle représentation produit non seulement une image erronée de la situation mais conduit également à une réaction publique et politique excessive (Yar, 2006). En prenant l'exemple de la pédopornographie, Pansier et Jez (2001, p.88) nous rappellent qu'Internet n'a pas fait augmenter le nombre de pédophiles, il a « seulement facilité la mise en place de nouvelles ramifications de réseaux déjà établis ainsi que l'échange de documents entre leurs membres ». Pour sa part, Leman-Langlois (2006) observe que le phénomène du cyberterrorisme présente tous les éléments de la panique morale développée par Cohen (voir encadré). Ainsi, il met en exergue le traitement médiatique et politique disproportionné au regard du « nombre infinitésimal d'actes empiriquement observables » (p.64).

Encadré 3.1. **La panique morale de Cohen (2002, p.1)**

« De temps en temps, il arrive que les sociétés soient en proie à des épisodes de panique morale. Une condition, un incident, une personne ou un groupe de personnes sont brusquement définis comme une menace pour la société, ses valeurs et ses intérêts ; ils sont décrits de façon stylisée et stéréotypée par les médias ; des rédacteurs en chef, des évêques, des politiciens et d'autres personnes bien pensantes montent au créneau pour défendre les valeurs morales ; des experts reconnus émettent un diagnostic et proposent des solutions ; les

autorités développent de nouvelles mesures ou - plus fréquemment - se rabattent sur des mesures existantes ; ensuite la vague se résorbe et disparaît, ou au contraire prend de l'ampleur. Parfois l'objet de la panique est plutôt inédit et parfois, il existe depuis longtemps mais surgit soudain en pleine lumière. Parfois la panique passe et n'existe plus que dans le folklore et la mémoire collective ; d'autres fois elle a des conséquences plus durables et peut produire des changements dans les lois, les politiques publiques ou même dans la manière dont la société se conçoit. » (traduction Peretti-Watel, 2010, p.1)

La panique morale, selon Stanley Cohen, est donc un problème construit socialement dans lequel les faits réels seront exagérés, notamment par les médias qui seront connus comme des « agents d'indignation morale » (Frau-Meigs, 2010).

Cette panique se présente sous la forme d'un modèle linéaire et séquentiel dans lequel trois phases vont se succéder :

La première phase est la phase d'alerte. La panique ne se manifeste pas encore, mais les médias, des experts, des politiciens… vont commencer à tisser un lien entre plusieurs événements faisant ainsi planer une menace prête à s'abattre sur la société jusque-là « paisible et ordonnée » (Leman-Langlois, 2007).

La deuxième phase correspond à la phase d'impact. Tous les événements sont alors interprétés dans un seul et même sens. Les autorités commencent à mettre en place des mesures de surveillance et de sanction qui amènent à augmenter le sentiment d'insécurité et de menace face à un phénomène perçu comme particulièrement dangereux.

La troisième et dernière phase correspond à une phase de réaction. Le débat est lancé et les « entrepreneurs moraux » renforcent leur position en définissant ce qui est « bien » de ce qui est « mal ».

Dès lors, face à la difficulté de mesurer les activités criminelles dans le cyberespace telle qu'observée dans le chapitre précédent et face à cette panique morale alimentée par les médias (Yar, 2006; Leman-Langlois, 2006), la science criminologique s'est penchée sur le sujet afin de nous aider à mieux appréhender la cybercriminalité. En effet, la criminologie a pour objectif de décrire, comprendre et expliquer de quoi le phénomène criminel est fait. Ainsi, depuis les deux dernières décennies, les chercheurs en criminologie étudient « l'impact des nouvelles technologies sur les pratiques des délinquants, les facteurs affectant le risque de victimisation, et l'applicabilité des théories traditionnelles du crime aux infractions virtuelles » (Holt et Bossler, 2014, p.21).

Dans ce chapitre, nous allons nous intéresser à ces études en criminologie et à leur apport quant à la connaissance sur ce phénomène. Dans un premier temps, nous verrons que la notion de cybercriminalité est loin de faire consensus au sein de la recherche scientifique, amenant alors une difficulté à bien saisir cette dernière, ce qui se répercute sur les données par la suite obtenues. Ensuite, nous nous pencherons sur les principales théories criminologiques aujourd'hui utilisées afin de mieux comprendre certains cybercrimes. Finalement, un examen exhaustif de chacun des crimes envisagés dans le cyberespace n'est pas réaliste au vu de l'étendue de leurs formes et de leurs expressions. Nous avons alors fait le choix de nous pencher sur trois d'entre eux : le piratage informatique, la fraude dans le cyberespace et les cyberviolences. Le piratage informatique caractérise la nouveauté par excellence puisque sans l'ordinateur et sans Internet il n'existerait pas. Aussi, tout est à faire pour comprendre ce crime émergent. La fraude dans le cyberespace est le cybercrime qui aujourd'hui touche le plus grand nombre de victimes et qui se classe au troisième rang des cybercrimes dans le monde (Carignan, 2015). Enfin, nous avons choisi de regarder les violences commises dans le milieu virtuel, car c'est actuellement une catégorie de cybercrimes qui se développe grandement et rapidement, il est donc important de connaître les résultats trouvés par la recherche afin de mettre en place des politiques publiques de prévention efficaces.

La cybercriminalité : définition et typologies

Débat entourant la définition de la cybercriminalité

Au-delà des multiples problèmes méthodologiques rencontrés pour conduire des études empiriques sur la cybercriminalité, la toute première difficulté commence au niveau définitionnel (Diamond et Bachmann, 2015). En effet, malgré le nombre croissant de recherches sur le sujet, la notion de cybercriminalité reste toujours « lacunaire et hétérogène » (Prates et al., 2013, p.5). Ainsi, que l'on vienne des sciences politiques, du droit, de la sociologie, ou de la criminologie, la définition employée pour décrire le concept de cybercriminalité ne sera pas la même (Brown, 2015). Il y aura presque autant de définitions que de personnes qui étudient ce phénomène. La cybercriminalité étant à la fois « un phénomène complexe et quelques fois insaisissable » (Goodman et Brenner, s.d., p.12), cette diversité d'approches n'en simplifie pas sa compréhension. Une définition universellement acceptée de la cybercriminalité n'existe donc pas aujourd'hui (Ngo & Jaishankar, 2017).

Toutefois, cette difficulté à développer une définition consensuelle se rencontre régulièrement dans la recherche en criminologie et sur des sujets variés. Le débat porte souvent en premier lieu sur l'utilisation ou non des définitions légales pour étudier

un fait criminel. En effet, ce qui est déviant ou criminel pour un pays ne le sera pas forcément pour un autre et inversement. De ce fait, certains criminologues choisiront de ne pas utiliser les définitions juridiques, considérées quelque peu « artificielles », quand d'autres fonderont sans problème leur analyse sur la définition légale d'un acte criminel.

Comme Wall (2001) le soulève, la notion de cybercriminalité ne se rapporte pas spécifiquement à un terme juridique. Non seulement les criminologues ne pourront pas s'appuyer sur une définition légale pour étudier la cybercriminalité, mais ils vont être en outre confrontés à un défi supplémentaire : celui d'examiner un phénomène qui prend place dans un environnement tout à fait nouveau et qui leur est jusque-là inconnu.

Le débat conceptuel important dans la recherche en criminologie est donc de savoir si le concept de cybercriminalité constitue une nouvelle forme de crime ou bien s'il se réfère à un type de criminalité déjà existante prenant une nouvelle forme quand exercée dans un nouvel environnement. Plusieurs approches vont alors se dégager de la littérature.

Pour David Wall (1998), certaines formes de crimes dans le monde virtuel trouvent leur pendant dans le monde réel. Il donne l'exemple de la fraude en disant que cette infraction, qu'elle s'exerce dans le milieu virtuel ou bien dans le milieu réel, reste pour autant la même; ce n'est donc pas l'infraction qui change mais le milieu dans lequel elle s'opère qui est nouveau. Ainsi, pour lui, les cybercrimes pourraient être considérés comme du « vieux vin dans de nouvelles bouteilles ». À côté de cela, il existe effectivement des crimes, tels que le piratage ou l'intrusion informatique, qui sont entièrement dépendants des nouvelles technologies et de l'Internet. Ces infractions peuvent alors être vues comme étant du « nouveau vin dans de nouvelles bouteilles ». Ce sont des infractions qui ne pourraient pas être commises si Internet ou l'ordinateur n'existaient pas.

Peter Grabosky (2001) considère également que la criminalité virtuelle constitue du « vieux vin dans de nouvelles bouteilles ». Cet auteur étudie la question sous l'angle des motivations et pour lui, les motivations des délinquants, que ce soit dans un contexte réel ou bien dans un contexte virtuel, restent toujours les mêmes : « la cupidité, la luxure, la vengeance, l'aventure et l'envie de goûter au « fruit défendu » (p.244), à quoi s'ajoute le défi intellectuel de maitriser ce système complexe. Ces motivations, pour Grabosky, ne nous sont donc pas étrangères, cependant, la nouveauté se situe dans la capacité de ces nouvelles technologies à faciliter la mise en œuvre de celles-ci.

En parallèle de cette vision sur le concept de cybercriminalité, il a été observé que l'accès à un bassin potentiel de victimes dans le monde fourni par les objets connectés et le nombre d'usagers d'Internet, conjugué à l'anonymat prodigué par les mondes virtuels, avaient foncièrement changé le processus de délinquance faisant dire à certains que la cybercriminalité était du « nouveau vin sans bouteilles » (Holt et Bossler, 2014).

Bryant et Bryant (2014) apportent un autre point de vue sur cette discussion. Pour eux, les crimes sont situés sur un continuum, qui comprend d'un côté les crimes traditionnels et de l'autre les crimes numériques. Ainsi, selon leurs observations, une grande partie des crimes manifestent des propriétés à la fois traditionnelles et numériques faisant en sorte qu'il soit très rare qu'existe une dichotomie apparente entre traditionnel et numérique. Finalement, Yar (2006) considère que les cybercrimes représentent un nouveau genre de criminalité qui diffère complètement des crimes commis dans le monde réel (Simion, 2009).

En fin de compte, comme le soulève Lusthaus (2013), il n'est pas clair que ce débat conceptuel soit particulièrement utile pour nous aider à mieux saisir le fonctionnement de la cybercriminalité, pas plus que pour mieux comprendre le comportement des cybercriminels. Pour lui, il n'est pas forcément nécessaire de s'embourber dans la catégorisation de nouveaux ou d'anciens crimes si notre intérêt principal est de connaître la structure, l'organisation et les caractéristiques des cybercriminels. La principale question à se poser, selon cet auteur, sera de connaître la manière dont les nouvelles technologies sont venues -ou pas- changer la nature de la criminalité. Cependant, il reconnait qu'une telle approche peut entrainer encore plus de confusion. En effet, dans une telle optique, la cybercriminalité correspondrait alors à n'importe quel crime, du fait de l'imprégnation de la technologie sur toutes nos activités quotidiennes.

Nous le voyons, définir la cybercriminalité est particulièrement difficile et le débat reste encore ouvert. Les chercheurs s'entendent sur le fait qu'il y a utilisation du cyberespace et des technologies informatiques pour faciliter les actes criminels et la déviance (Holt et Bossler, 2013); en revanche, ils ne s'entendent pas forcément sur les types des crimes que la définition devrait englober. La difficulté à saisir la notion de cybercriminalité est en effet amplifiée par le fait qu'elle se rapporte à toute une gamme d'activités illicites et illégales et non pas seulement à un fait pur et simple. Comme nous allons le voir, plusieurs typologies ont alors été développées par le milieu de la recherche afin de nous aider à avoir un portrait plus global de ce qui est contenu dans la notion de cybercriminalité.

Typologies de la cybercriminalité

Wall (2007) explique que le développement des cybercrimes s'est fait en trois étapes. La première génération que nous pouvons situer avant les années 70, est largement constituée de crimes traditionnels dans lesquels les ordinateurs étaient simplement un outil pour la commission des faits.

Pour la deuxième génération de cybercrimes (après les années 70), la nouvelle technologie et les réseaux mis en place ont fait en sorte que les crimes traditionnels sont devenus petit à petit plus distribués et plus globalisés. Enfin, la troisième génération est constituée de crimes qui n'auraient jamais pu exister sans Internet. Ce sont des cybercrimes sui generis, c'est-à-dire des crimes uniques qui existent indépendamment des autres types de crimes.

Ainsi, l'approche commune envisagée pour définir les divers types de cybercrimes se trouve être la distinction entre les crimes assistés par ordinateur et les crimes axés sur l'ordinateur (Furnell, 2004; Yar, 2006). Les premiers font référence à des crimes dits « traditionnels » qui vont avoir une deuxième vie dans le cyberespace. Nous pensons à des crimes tels que la fraude, la pornographie ou le blanchiment d'argent par exemple. La deuxième catégorie concerne des crimes qui se sont développés avec la naissance et l'évolution d'Internet et qui n'existeraient pas sans ce dernier. Nous pensons ici à des crimes comme le piratage ou des attaques virales. Ce genre de classification se contente alors de s'appuyer sur le rôle joué par la technologie et suit une perspective utilitariste; perspective qui va généralement être adoptée par les corps de police. En revanche, elle est quelque peu limitative lorsqu'il s'agit de faire des recherches en criminologie car la relation délinquant/victime est occultée, alors même que c'est une caractéristique fondamentale à prendre en considération dans l'étude d'un acte criminalisé. Ainsi, plusieurs auteurs ont travaillé à développer des typologies qui soient plus opérantes pour la recherche.

Wall (2001) a été l'un de ces premiers auteurs à penser et à développer une typologie des cybercrimes, qui reste aujourd'hui la plus complète et la plus reconnue dans le milieu de la recherche (Holt, 2009; Holt & Bossler, 2014). Il va catégoriser les différents cybercrimes en 4 groupes d'infractions :

i. **Cyber-intrusion :** franchir les limites des biens d'autrui et / ou causer des dommages, par ex. piratage, défacement, virus.

ii. **Cyber-tromperies et vols :** vol (argent, biens), par ex. fraude par carte de crédit, violation de la propriété intellectuelle (par exemple «piratage»).

iii. **Cyber-pornographie :** enfreindre les lois sur l'obscénité et la décence.

iv. **Cyber-violence :** faire du tort psychologique ou inciter à des dommages physiques contre autrui, violant ainsi les lois relatives à la protection de la personne, par ex. discours de haine, harcèlement criminel.

De son côté, Leman-Langlois (2006), modélise une typologie « objective » fondée sur deux caractéristiques : le rôle des réseaux informatiques dans la commission de l'acte criminalisé et l'époque d'incrimination de ce dernier (voir tableau 3.1).

Alkaabi, Mohay, McCullagh, & Chantler (2010) proposent quant à eux une typologie des cybercrimes basée sur trois composantes : le rôle joué par l'ordinateur, la nature du crime et le contexte entourant celui-ci. Elle se présente de cette manière :

i. **Les crimes de type I** comprennent les crimes pour lesquels l'ordinateur, le réseau informatique ou l'appareil électronique est la cible de l'activité criminelle ; quatre sous-groupes :

   a. les infractions d'accès non autorisé telles que le piratage;

   b. les délits de code malveillant tels que la dissémination de virus ou de vers;

   c. les infractions d'interruption de services tels que l'interruption ou le refus de services informatiques et d'applications telles que les attaques par déni de service et les Botnets;

   d. le vol ou la mauvaise utilisation de services tels que le vol ou la mauvaise utilisation du compte Internet ou du nom de domaine d'une personne.

ii. L**es crimes de type II** comprennent les crimes pour lesquels l'ordinateur, le réseau informatique ou l'appareil électronique est l'outil utilisé pour commettre ou faciliter le crime; trois sous-catégories :

Tableau 3.1. **Typologies objective de cybercriminels selon Leman-Langlois (2006)**

Réseaux/cyberespace ont un rôle	Incrimination des actes	-
	traditionnelle (prélnternet)	émergente/imminente (postInternet)
Déclencheur	(non applicable)	attaques distribuées; vandalisme virtuel
Multiplicateur	pornographie juvénile; vol d'identité; fraudes	échange de fichiers; pourriels
Accessoire	Leurre ; terrorisme et sabotage	Terrorisme (support)

a. les infractions de violation de contenu telles que la possession de pornographie juvénile, la possession non autorisée de secrets militaires, les infractions en matière de propriété intellectuelle ;

b. l'altération non autorisée de données ou de logiciels à des fins personnelles ou organisationnelles, comme la fraude en ligne ;

c. l'utilisation incorrecte des télécommunications telles que le cyberharcèlement, le spamming et l'utilisation de services de transport/livraison avec l'intention de commettre des activités nuisibles ou criminelles, notamment dans le cadre d'une conspiration.

Pour ces auteurs, dans le cas de certains crimes, l'ordinateur va jouer des rôles multiples faisant en sorte qu'un même crime pourrait être classé sous plusieurs catégories. Aussi, au-delà d'une telle typologie basée sur le type de ces crimes et sur le rôle joué par l'ordinateur dans la commission du crime, il est primordial, selon eux, qu'elle soit complétée par des informations contextuelles telles que la motivation principale du délinquant (motivation individuelle ou politique par exemple), son lien avec la victime ainsi que le type de victime touchée par ce crime (un individu, une entreprise, un gouvernement ou bien une infrastructure). Finalement, Bryant et Bryant (2014, p.25), classifient les cybercrimes selon leur degré de nouveauté et de complexité numérique (voir Tableau 3.2).

Comme nous venons de le voir, le flou définitionnel entourant le terme de cybercriminalité, ainsi que le manque de consensus sur le sujet, entrainent une difficulté dans l'harmonisation des recherches et conduisent alors à ce que les chercheurs adoptent une définition en fonction de leurs intérêts et de leur axe d'étude.

Pourtant, l'élaboration d'une définition universellement adoptée est au cœur de véritables enjeux.

Enjeux pour l'élaboration d'une définition commune

Le manque de typologie communément acceptée entrave clairement les efforts internationaux pour identifier, rapporter et surveiller les tendances concernant la cybercriminalité (Alkaabi et al., 2010). Ainsi, pour Furnell (2001), il est essentiel et impératif d'avoir une classification harmonieuse des cybercrimes. Cela permettrait, tant pour les individus que pour les organisations concernées, de lutter contre ces problèmes de cybercrimes.

Le bénéfice d'avoir une typologie cohérente et complète des crimes tenant place dans le cyberespace se répercuterait à plusieurs niveaux. D'abord, dans le partage d'information; ensuite pour un rapport précis des cas de cybercrimes; pour la coopération sur les cas actuels; la coopération pour combattre le cybercrime; et enfin pour l'harmonisation des législations et des régulations d'un tel phénomène (Alkaabi et al., 2010).

Ngo et Jaishankar (2017) abondent dans ce sens. En effet, pour eux, il parait essentiel aujourd'hui et pour l'avenir de définir et classifier les différents types de cybercrimes. Tout d'abord, cela permet à l'ensemble des acteurs impliqués sur ce sujet, qu'ils soient chercheurs, experts techniques ou juridiques, d'avoir un langage commun afin de faciliter les discussions et de mettre en place des collaborations efficaces. Ensuite, cela peut aider ces divers acteurs à déterminer l'ampleur du problème. Une définition et une classification admises de tous fait aussi en sorte de soutenir les agences d'application de la loi et les services de justice dans leur ensemble à enquêter, combattre et prévenir ce genre de crimes. Enfin, cela peut rendre possible la compréhension de ce que va devenir la cybercriminalité pour formuler de nouvelles solutions à ce problème.

Tableau 3.2. **Classification de Bryant et Bryant (2014)**

	Augmentation du numérique	
Augmentation de la nouveauté	Crimes traditionnels, peu de caractéristiques de la criminalité numérique, autres que la criminalistique numérique p. cambriolage d'un logement	Crimes traditionnels avec certaines caractéristiques numériques, par ex. fraude de carte de crédit
	Les crimes numériques avec certains traits de crimes traditionnels, par ex. piratage en utilisant l'ingénierie sociale pour obtenir un mot de passe	Crimes numériques, peu de caractéristiques traditionnelles, par ex. Attaques DDos

Comme le rappelle Wall (2017, p.23), plus souvent qu'autrement, le terme cybercrime tend à être utilisé « métaphoriquement et émotionnellement plutôt que scientifiquement et légalement ». Plusieurs termes tels que cybercrime, crime lié à l'informatique, crimes de haute technologie ou bien crimes numériques par exemple sont utilisés de manière interchangeable (Simion, 2009) apportant une grande confusion quand nous cherchons à mieux comprendre ce phénomène. En outre, la recherche sur la cybercriminalité se concentre principalement sur la prévalence des différents types de crimes. Elle manque souvent de bases théoriques. (Kerstens et Veenstra, 2015). Toutefois, certains chercheurs vont essayer de dresser un portrait plus clair de la situation en tentant d'appliquer les théories criminologiques classiques. Les résultats obtenus pourraient alors orienter les politiques publiques dans la prévention.

Encadré 3.2. **Les théories traditionnelles utilisées pour comprendre la cybercriminalité**

Seul un petit nombre d'études sur la cybercriminalité ont cherché à voir si l'utilisation des théories traditionnelles en criminologie pouvait nous aider à comprendre la participation de certains individus à des comportements criminels dans le cyberespace (Kerstens et Veenstra, 2015). Aussi, trois positions sont tenues sur ce sujet, positions qui découlent directement du débat entourant la définition du terme « cybercriminalité », vue précédemment.

Kerstens et Veenstra (2015) rapportent que Grabosky (2001) considère que les comportements en ligne et hors ligne se trouvent être semblables et donc que les théories traditionnelles utilisées en criminologie peuvent tout à fait s'appliquer, notamment la théorie des activités routinières.

Yar (2005) qui part également de la théorie des activités routinières souligne tout de même des différences entre le monde réel et le monde virtuel, plaidant alors pour une innovation technologique. Enfin, Jaishankar (2008) met de l'avant l'interdépendance des deux mondes –virtuel et réel- privilégiant alors, comme nous le verrons dans sa contribution, le développement d'une théorie spécifique à l'explication de la cybercriminalité.

Les théories traditionnelles les plus employées par la recherche actuellement pour comprendre la cyberdélinquance sont la théorie de l'association différentielle de Sutherland (1947), les techniques de neutralisation exposées par Sykes et Matza (1957) et la théorie générale du crime et du faible contrôle de soi mise en oeuvre par Gottfredson et Hirschi (1990). En outre, la théorie des opportunités et des activités routinières de Cohen et Felson (1979) reste aujourd'hui la plus souvent citée pour expliquer la commission d'un acte criminel (Bernier, 2016). Nous allons présenter brièvement ces théories avant de voir comment elles s'appliquent au contexte de la cybercriminalité.

Théories de l'apprentissage

La théorie de l'association différentielle de Sutherland (1947) fait référence aux connaissances et habitudes qu'un individu assimile dans son environnement et dans ses relations avec d'autres personnes. Sutherland (1947) part du principe qu'une personne, au contact de pairs différents va apprendre de nouvelles façons d'envisager le monde mais également de se comporter. Ainsi, la personne ne va pas seulement imiter ce qu'elle voit, elle va également « apprendre à interpréter les actions et le contexte social et matériel qui l'entoure d'une manière favorable à l'accomplissement d'actes criminels » (Leman-Langlois, 2007, p.80). Le comportement criminel est donc acquis et non pas inné. La communication avec d'autres personnes est la source de l'apprentissage, communication qui peut se trouver tant dans le verbal que dans la pratique, l'attitude ou l'aspect physique. Les groupes restreints sont les plus grands contextes d'apprentissage en ce sens que l'individu s'identifie plus facilement aux autres. Cet apprentissage de l'agir criminel se fait au contact de personnes pour qui l'individu manifeste de la confiance, du respect ou de l'amitié. Aussi, il dépasse les simples techniques de l'acte délinquant, il concerne principalement les interprétations (valeurs, motivation, attitudes et rationalisations) favorables pour commettre un acte délinquant. En effet, loin d'être une simple théorie de l'imitation, l'association différentielle concerne surtout l'adoption d'interprétations, de symboles et d'attitudes (Jaquith, 1981).

Sykes et Matza (1957) développent un modèle explicatif de la délinquance, dans la même veine des théories de l'apprentissage, basé sur le fait que pratiquement tout le monde se sent moralement obligé de respecter le loi, incluant les délinquants. Aussi, lorsqu'un individu commet un acte délinquant, il a besoin de justifications pour rationaliser son comportement. Ses justifications sont appelées techniques de neutralisation et sont apprises au contact des pairs. Sykes et Matza ont mis en exergue cinq techniques : le déni de responsabilité, le déni des dommages, le fait de nier l'existence d'une victime, l'accusation des accusateurs (les policiers sont corrompus, le système est hypocrite…) et l'invocation des autorités supérieures (loyauté envers un ami…).

Selon la plupart des criminologues, il est fort probable que la conduite délinquante précède les justifications. Ainsi les techniques de neutralisation ne seraient pas une cause de la délinquance mais un moyen d'échapper à une éventuelle mesure répressive.

Théorie intégrative

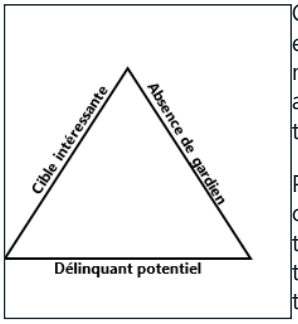
Gottfredson et Hirschi (1990) ont pour idée de faire une synthèse de ce qui était jusqu'alors connu quant à l'étiologie de la délinquance. Comme l'explique Ouimet (2009), ils ont pour ambition d'expliquer tous les comportements criminels, voire même plusieurs formes de déviance en tout temps et en tous lieux. Ils partent de deux postulats : les délinquants sont des êtres rationnels et le crime n'est qu'une manifestation comme une autre d'un même problème. En se basant sur la théorie du choix rationnel et celle du contrôle social, ils vont intégrer à leur modèle une théorie du contrôle personnel. Ainsi, le facteur étiologique[17] de la délinquance le plus important pour ces auteurs va être la faculté pour un individu à contrôler ses pulsions et à retenir ses envies. Le faible contrôle personnel viendrait principalement de l'absence ou de la faiblesse de forces socialisantes et notamment de la négligence de bonnes pratiques parentales. En effet, le fait d'avoir un bon contrôle de soi dépend de trois facteurs selon Gottfredson et Hirschi : la supervision parentale, la reconnaissance des comportements inadéquats et la capacité d'intervenir auprès de l'enfant. Le faible contrôle de soi serait donc entièrement expliqué par l'environnement. Les individus avec un faible contrôle de soi sont généralement caractérisés par une plus grande impulsivité, la recherche de sensations fortes, un goût du risque, une préférence pour les activités physiques par opposition aux activités intellectuelles, une faible tolérance à la frustration et une inclinaison à exprimer physiquement leur frustration.

Une méta analyse conduite par Pratt et Cullen (2000) confirme que la faible maîtrise de soi prédit bien le comportement délinquant, mais qu'en revanche, elle n'expliquerait pas à elle seule l'étiologie délinquante.

Théorie économique de la criminalité

Cohen et Felson (1979) se penchent sur les variations du taux de criminalité en analysant les statistiques criminelles aux États-Unis entre 1960 et 1990. Plutôt que d'examiner les caractéristiques propres au délinquant, ils proposent une approche basée sur les circonstances de l'acte délinquant. Ils envisagent alors la criminalité avec une vision économique. Ils partent du postulat que l'activité criminelle est une activité rationnelle. En effet, selon eux, le délinquant est un être rationnel qui fait un calcul coût/bénéfice avant la commission de son acte. Ainsi, si l'infraction a un coût (risque) inférieur au bénéfice que le délinquant pourrait en tirer alors il passera à l'acte. Aussi, la période étudiée par Cohen et Felson fut caractérisée par une augmentation de la quantité de biens en circulation, faisant en sorte que les opportunités de vols par exemple se multiplient. En outre, cette même période a connu une augmentation significative de la population professionnellement active, notamment avec l'arrivée importante des femmes sur le marché du travail, entrainant alors moins de surveillance dans les maisons au cours de la journée.

Dès lors, selon eux, les variations du taux de criminalité s'expliquent par la présence de trois facteurs : la présence d'une opportunité criminelle, la présence d'une personne prête à saisir l'opportunité et l'absence de gardien.



C'est une théorie qui explique bien la victimisation à répétition ainsi que la concentration de criminalité.

Pour ces auteurs, le crime peut être évité dès lors qu'un des trois éléments constitutifs de la commission de l'acte est désactivé. C'est alors une bonne solution pour prévenir le crime que de jouer sur l'un des trois facteurs. C'est une théorie à la base de la prévention situationnelle, puisqu'en agissant sur l'environnement qui offre aux délinquants des opportunités, ces derniers pourront être dissuadés de passer à l'acte.

D'autres théories sont aujourd'hui examinées dans le cadre de la cybercriminalité, notamment des théories psychologiques. Toutefois, le corpus de recherche reste encore assez réduit mais c'est une approche qui va pouvoir compléter les données actuelles pour une meilleure appréhension des cybercriminels et des cybervictimes.

Nous allons voir, qu'en mettant les théories, précédemment décrites, à l'épreuve de la cybercriminalité, les chercheurs vont apporter quelques éléments de clarification concernant le profil des délinquants et celui des victimes dans la commission de certains cybercrimes en particulier.

Le piratage informatique

Encadré 3.3. **Deux exemples de pirates informatiques**

L'affaire Ryan CLEARY

Ryan Cleary, jeune « hacker » britannique de 19 ans a été condamné en mai 2013 à 32 mois d'emprisonnement pour avoir participé à plusieurs attaques informatiques dirigées contre divers organismes d'application de la loi, notamment le site de la CIA, célèbre agence américaine de renseignements, mais également celui de la SOCA, l'agence britannique de lutte contre la grande criminalité organisée. Si le jeune homme a reconnu faire partie de l'organisation de « hackers » LulzSec, connue notamment pour s'être introduite dans le système informatique de Sony ou du Sénat américain, le groupe a toujours démenti l'implication de Ryan Cleary dans leurs activités.

La méthode utilisée par le jeune pirate est celle d'une attaque par déni de service distribué (DDoS), dont l'objectif est de rendre indisponible un service en ligne en le submergeant de trafic inutile. Elle représente aujourd'hui une réelle menace, dans la mesure où elle est extrêmement difficile à contrer, et de plus en plus facile à mettre en œuvre.

Le syndrome d'Asperger et celui de l'agoraphobie ont été diagnostiqués chez Ryan Cleary, qui affirme avoir agi de façon altruiste, du moins en partie, dans le but de contester des intérêts puissants et démontrer qu'en dépit des idées reçues, les données confidentielles conservées par les grandes entreprises et organisations ne sont pas suffisamment sécurisées.

Suite à son arrestation, le pirate informatique a été exposé par Anonymous qui a publié son nom, son adresse et son numéro de téléphone en guise de représailles pour avoir piraté le site web du groupe AnonOps et exposé plus de 600 surnoms et adresse IP.

L'affaire Kane Gamble

Le 20 avril 2018, Kane Gamble, jeune adolescent britannique de 18 ans, était condamné à deux années de détention et à la saisie de l'intégralité de son matériel informatique pour avoir piraté les comptes de plusieurs hauts responsables américains. Le jeune pirate avait reconnu être l'auteur de dix infractions à la législation sur la sécurité informatique commises entre juin 2015 et février 2016.

Il avait notamment réussi à obtenir de nombreux documents confidentiels du compte de messagerie électronique de l'ancien directeur de la CIA, John Brennan, portant sur des opérations militaires et de renseignement menées en Afghanistan et en Iran, ainsi qu'à prendre le contrôle de l'iPad de son épouse. L'ancien responsable de la sécurité intérieure, Jeh Johnson avait également été pris pour cible, de même que certains conseillers de l'ancien président des États-Unis Barack Obama, l'ancien directeur adjoint du FBI, Mark Giuliano, ou le réseau du ministère de la justice.

Il s'est ainsi vanté notamment d'avoir mis en place un renvoi des appels de James Clapper, ancien directeur du renseignement national, vers le mouvement palestinien libre, ou d'avoir effectué « la meilleure brèche de tous les temps » en parvenant à obtenir les noms de 1000 employés du FBI, y compris l'officier responsable de la fusillade de Michael Brown à Ferguson dans le Missouri.

Tandis que l'accusation considérait l'ensemble de ces actes comme un soutien politique aux Palestiniens, motivé par la mort de civils innocents, ainsi qu'un moyen de protester contre les violences policières et les actes racistes, pour la défense, il ne s'agissait que d'un ensemble de canulars, menés par un adolescent naïf souffrant d'autisme.

Si la notion de cybercriminalité est assez floue et correspond à une vaste gamme d'actes, le terme piratage informatique est également un terme générique pour lequel une variété d'activités distinctes sont associées (Yar, 2006). Décary-Hétu (2013) se pose d'ailleurs la question de savoir si par les abus de langage entourant cette notion, cette dernière n'a finalement pas été dénaturée et vidée de son sens.

Définition du piratage informatique

Leeson et Coyne donnent comme définition :

> « Le piratage correspond à de multiples activités : le décodage de mots de passe, la création de « bombe logique », les attaques par courrier électronique, les attaques par déni de service, l'élaboration et la diffusion de virus, l'accès interdit à des informations conservées électroniquement, la redirection automatique à partir des pages web, le détournement de sites électroniques, ou tout autre activité impliquant l'accès à des systèmes informatiques sans les autorisations nécessaires. » (2014, p.207)

Leur définition est très détaillée, quand la grande majorité des chercheurs dans le domaine se contentent d'une définition plus restrictive. Le piratage informatique est alors conçu comme étant « le geste d'accéder à un système informatique sans autorisation » (Brenner, 2001, p.2 ; Taylor 1999).

De cette définition, Décary-Hétu (2013) fait ressortir trois techniques utilisées par les pirates informatiques : le décryptage, le piratage et l'ingénierie sociale.

Le décryptage correspond au fait de décrypter ou de tenter de décrypter les mots de passe pour accéder à un système informatique (Rowan, 2009). Le piratage, de son côté, est compris comme l'acte cherchant à abuser des mauvaises configurations ou des erreurs commises par les programmeurs. Ces deux techniques, le piratage et le décryptage, utilisent des moyens technologiques alors que la dernière technique, l'ingénierie sociale va utiliser le facteur humain. En effet, cette technique est définie comme étant « l'utilisation d'une interaction sociale dans le but d'obtenir une information sur le système informatique de la victime » (Winkler et Dealy, 1995 tel que cité par Décary-Hétu, 2013, p.4).

Partant de cette définition, les chercheurs s'attachent à approfondir la connaissance des profils, aussi bien ceux des pirates que de leurs victimes.

Typologie et profils des pirates

1) Typologie

Les études sur le piratage informatique se sont intéressées à catégoriser les pirates en fonction de leur profil. Pour ce faire, deux axes ont été privilégiés pour différencier ces derniers : leurs motivations à commettre des actes criminels et leurs connaissances techniques en matière informatique.

L'une des premières typologies développées a été celle de Rogers (1999) qui catégorise les pirates en fonction de leurs capacités techniques, à peine à huit ans après la naissance de la WWW. Il fait alors ressortir quatre groupes :

i. les pirates aînés, non criminalisés, qui s'intéressent à la technologie avant tout et qui estiment que toute information devrait être gratuite ;
ii. le « script kiddies » qui utilisent des logiciels automatisés pour mener à terme des attaques sans avoir les connaissances nécessaires pour comprendre ce qu'ils font ni créer d'autres outils ;
iii. les criminels professionnels qui se dédient à temps complet au piratage, en font un moyen de subsistance et sont embauchés par les gouvernements, les compagnies et le crime organisé ;
iv. les programmeurs qui produisent le code malicieux utilisé par les autres groupes pour pirater.

Les typologies basées sur les motivations des pirates tentent de les classifier selon le but qui les pousse à agir. Les chercheurs mettent l'emphase sur les motivations des pirates car ils voient ces derniers comme des acteurs rationnels[18] qui choisissent consciemment de s'engager dans des activités illicites dans l'espoir d'une récompense ou satisfaction (Yar, 2006). Dès lors, six motivations ressortent de la littérature : la reconnaissance, l'argent, l'idéologie, la curiosité, les défis techniques. À ces cinq motivations, s'ajoute l'altruisme, selon les données collectées durant les recherches de Décary-Hétu (2013). Le pirate altruiste serait l'individu qui cherche à aider les autres en repérant les failles dans leurs systèmes et en les avertissant de ce problème. Malgré le fait que ce genre d'individus apportent leur soutien pour sécuriser des systèmes, il n'en reste pas moins qu'ils ne sont pas autorisés à commettre ces actes et peuvent alors être poursuivis par la justice.

Finalement, en 2006, Rogers a tenté de mettre en place une typologie hybride, construite à la fois sur les motivations des pirates et sur leurs capacités techniques. Il en ressort neuf groupe :

i. le novice qui est le néophyte utilisant des outils automatiques et qui cherche à se faire un nom;
ii. le cyber-punk, légèrement supérieur au novice, qui a quelques connaissance en programmation et qui cherche la gloire et l'argent ;
iii. l'initié qui attaque son employeur de l'intérieur pour se venger ;
iv. le simple voleur qui passe du monde réel au virtuel afin de suivre ses cibles comme les banques et les compagnies de carte de crédit en ayant pour principale motivation l'argent ;
v. le programmeur de virus ;
vi. le pirate de vieille garde qui a hérité de la mentalité des pirates aînés et qui recherche la stimulation intellectuelle ;
vii. le criminel professionnel spécialisé dans la criminalité informatique qui cherche des gains financiers ;
viii. le guerrier de l'information ayant pour objectif de déstabiliser les centres de décisions et qui est motivé par le patriotisme ;
ix. l'activiste politique.

Comme le font remarquer plusieurs auteurs (Yar, 2006, Leeson et Coyne, 2014), il existe une grande variété de pirates, caractérisés par des motivations diverses. Décary-Hétu (2013) insiste alors sur le fait qu'il est difficile de dresser un portrait type du pirate informatique et qu'il semble plus réaliste d'envisager des profils aussi diversifiés que ceux des délinquants plus traditionnels.

Pourtant, certaines recherches se sont penchées plus spécifiquement sur le profil de ces pirates afin de mieux comprendre la prévalence et les causes du comportement de ces derniers.

2) Profils des pirates informatiques

La recherche a essayé de comprendre les causes du comportement des pirates informatiques en l'étudiant au travers des facteurs contextuels et personnels.

En ce qui a trait aux facteurs contextuels, les chercheurs ont abordé le sujet sous deux angles : l'influence des pairs et l'influence de la famille.

Comme le rapportent Holt et Bossler (2014), concernant l'influence des pairs, la première avenue des études qualitatives a été de regarder le comportement des pirates au travers des théories de l'apprentissage avec notamment la théorie de l'association différentielle de Sutherland (1947). Ainsi, une corrélation entre les relations avec les pairs et le fait de participer à du piratage a été démontrée. Au contact de pairs pratiquant le piratage, les individus apprennent que c'est un acte acceptable faisant en sorte qu'ils passent à l'acte plus facilement.

En outre, au contact des pairs, les pirates mobilisent ce que Sykes et Matza (1957) ont appelé des techniques de neutralisation leur permettant d'excuser ou de justifier leurs comportements. Les pirates vont alors prétendre que leurs actions ne causent pas de dommages, ou bien reportent la faute sur les victimes en blâmant leur faible compétences en informatique et sécurité. Toutefois, il est bien difficile de séparer clairement les motivations ex ante des pirates de leurs justifications post ante (Taylor, 1999).

Concernant l'influence de la famille, les études se sont tournées vers la théorie du faible contrôle de soi de Gottfredson et Hirschi (1990). Les études sont encore récentes et le lien entre faible contrôle de soi et piratage n'est pas clair (Holt et Bossler, 2014). Il reste donc beaucoup de recherche à faire sur le sujet au vu de la diversité des actes que sous-tend le piratage. Toutefois, Holt et al. (2012) ont commencé à entrapercevoir un lien entre faible maitrise de soi, relation avec les pairs et piratage. Higgins (2005) montre que le faible contrôle de soi a un lien avec le piratage de logiciels, mais que l'apprentissage social reste un meilleur facteur de compréhension pour ce type d'actes. Pour avoir une meilleure idée du problème, il incite à combiner la théorie du faible contrôle de soi avec celle de l'apprentissage social.

Au regard des facteurs personnels amenant des individus à commettre des actes de piratage, le seul consensus que nous retrouvons dans la recherche est que la grande majorité d'entre eux sont de sexe masculin (Décary-Hétu, 2013; Taylor, 1999), certains auteurs estimant à 99 :1 le ratio homme : femme (Taylor, 1999). Ce sont également plutôt des jeunes, âgés de moins de 30 ans (Leeson et Coyne, 2014; Décary-Hétu, 2013). Sterling (1994) indique d'ailleurs que la plupart des pirates commencent jeunes et abandonnent le piratage au début de leur vingtaine. Ainsi, la masculinité et la jeunesse seraient deux facteurs explicatifs du piratage (Taylor, 1999). À ces caractéristiques s'ajoute le fait que la plupart des pirates sont de type caucasien.

D'autres facteurs amenant un individu à participer à des activités de piratage ont été identifiés. Le premier est une exposition très jeune à la technologie, par le biais des jeux vidéo par exemple. Ensuite, il a été démontré que les pirates avaient une grande curiosité face à la technologie et avaient, en outre, une aptitude d'autogestion plus développée que la moyenne avec pour certains, des traits antisociaux. Enfin, ce seraient des personnes plus créatives avec une meilleure capacité à analyser et à prendre des décisions (Holt, 2007; Taylor, 1999).

Les autres spécificités sociodémographiques, comme le profil scolaire ou le profil professionnel, varient grandement selon l'échantillonnage des études (Décary-Hétu, 2013). Pontell et Rosoff (2009) ont trouvé que les crimes informatiques tels le piratage se produisent le plus souvent dans les classes sociales supérieures.

Une grande partie des études qui se sont intéressées aux causes du piratage informatique s'en sont principalement tenues à examiner des formes de piratage assez simples. Si ces dernières comportent encore beaucoup de zones d'ombre, leur étendue est encore plus importante pour des formes de piratage plus complexes (Holt et Bossler, 2014).

Profil des victimes du piratage informatique

Le piratage informatique touche autant les individus que les entreprises et les gouvernements. Toutefois, il est assez difficile de connaitre les caractéristiques des internautes potentiellement victimes alors que les attaques dirigées contre les entreprises ou les gouvernements sont souvent de plus grande ampleur et donc médiatisées. Nous savons en revanche qu'il existe un chiffre noir important en ce qui concerne le piratage des entreprises ou même des gouvernements car leur réputation est en jeu dans ce genre d'affaire.

Le manque considérable de données sur les victimes individuelles est dû au fait que les personnes ne rapportent pas les faits aux instances compétentes, soit par manque de connaissance sur le sujet, soit par crainte que rien ne soit fait du côté de la justice. Pour pallier à ce problème, les recherches en criminologie se tournent vers les enquêtes de victimisation. Concernant le piratage informatique, les études sont la plupart du temps faites sur un échantillon de collégiens, les résultats s'avérant alors quelque peu limités. (Holt et Bossler, 2013).

La principale manière d'en connaître un peu plus sur les victimes de piratage a été de se tourner vers la théorie des activités routinières développées par Cohen et Felson. Les résultats qui sont ressortis de ces études sont qu'il n'y a pas de corrélation établie entre l'âge et le risque d'être victime d'un acte de piratage. Ceci va alors à l'encontre de ce que les criminologues considèrent comme étant un facteur de risque de victimisation dans le cadre des crimes traditionnels. Également, il semblerait que les femmes soient plus touchées par le piratage informatique et les infections par logiciels malveillants. Toutefois, les données ne sont pas suffisamment probantes en ce sens que les pirates ciblent généralement un bassin très large de victimes et non pas des cibles précises. Aussi, les personnes qui commettent des cybercrimes seraient plus à risque d'être à leur tour victimes. Il en serait ainsi notamment pour les personnes qui commettent des téléchargements illégaux ou celles qui regardent de la pornographie en ligne (Weulen Kranenbarg, Holt et van Gelder, 2017).

Finalement, il y a encore aujourd'hui peu de preuves solides quant à la protection que jouent les logiciels anti-virus par exemple ou bien les firewalls contre le piratage informatique.

Également, des compétences élevées en informatique ne protègent pas non plus du risque d'être victime de piratage. Au contraire, elles peuvent devenir un facteur de risque en ce sens que les individus qui possèdent des compétences techniques élevées vont être plus susceptibles d'avoir des comportements à risque lors de la navigation sur Internet (Van Wilsem, 2013).

La fraude informatique

Encadré 3.4. **La « fraude nigériane »**

Mike, escroc nigérian

L'hameçonnage [phishing] est aujourd'hui l'une des plus illustres techniques de fraude informatique. Le principe est simple : une victime reçoit un courriel ou un appel téléphonique destiné à la tromper, prend les mesures suggérées en fournissant au fraudeur diverses informations personnelles, que ce dernier utilise ensuite pour obtenir des fonds. La « fraude nigériane », ou « fraude 419 » en est une variante extrêmement répandue, particulièrement chez les délinquants basés en Afrique. Une somme d'argent très élevée est promise à la victime, une fois qu'elle se sera acquittée du paiement de divers frais « nécessaires » (Cukier, Nesselroth et Cody, 2007). Au fil des échanges entre le fraudeur et sa victime, celle-ci est constamment invitée à payer des frais supplémentaires avant de pouvoir percevoir les fonds promis. Ce processus se poursuit ainsi jusqu'à ce que la victime cesse de procéder aux paiements (Dyrud, 2005). Il s'agit d'une technique extrêmement efficace qui demeure étonnamment fructueuse, malgré des efforts de sensibilisation du public sans cesse accrus. En effet, selon le FBI, 1200 compagnies ont été escroquées en 2014 pour un montant de 180 millions de dollars, contre 5800 en 2015, et un bénéfice montant à 570 millions de dollars.

C'est grâce à ce procédé que « Mike », escroc nigérian de 40 ans est parvenu à piéger sur internet des centaines de victimes et de détourner ainsi plus de 60 millions de dollars, dont 15,4 millions d'une seule d'entre elles. À la tête d'un réseau transnational constitué d'une quarantaine de membres au Nigéria mais également en Malaisie et en Afrique du Sud, il a été arrêté par Interpol avec l'aide des autorités nigérianes en août 2016. Mike et ses complices se faisaient ainsi passer pour prince, riche héritier ou encore militaire haut gradé qui souhaite transférer de toute urgence des fonds hors de son pays et qui sollicite l'aide de ses victimes, accompagnée de la promesse de toucher des intérêts. La demande peut prendre la forme d'une avance de frais (sous le prétexte du paiement d'honoraires d'avocats, de frais de douane, de taxe fiscale, etc.) mais également des coordonnées bancaires et papiers d'identité afin de procéder au transfert de la somme, informations qui seront ensuite utilisées par les fraudeurs pour usurper l'identité de leurs victimes et s'emparer du contenu de leur compte en banque.

La célèbre « arnaque au PDG » était également utilisée par le réseau, consistant à pirater le compte d'un haut responsable d'entreprise avant d'envoyer en son nom un message à un employé afin qu'il procède au transfert rapide d'une somme d'argent sur un compte bancaire spécifique. C'est ainsi que le réseau a compromis les comptes de courrier électronique de petites et moyennes entreprises du monde entier, notamment basées en Inde, en Australie, au Canada, en Malaisie, en Thaïlande, en Roumanie, en Afrique du Sud, etc. L'argent était ensuite blanchi par le biais de contacts en Chine, en Europe et aux États-Unis qui produisaient des relevés de comptes bancaires pour le flux de fonds illicites.

La fraude est un acte criminel qui a toujours existé mais pour lequel l'essor d'Internet décuple les possibilités et fait en sorte que les délinquants vont se retrouver face à un bassin de victimes beaucoup plus large. En même temps qu'Internet devient de plus en plus un lieu de commerce, il va devenir un lieu de fraude (Grabosky, 2001). Le cyberespace peut en effet être vu comme un « terreau » pour ce genre de crimes (Fried, 2001).

Comme pour beaucoup d'autres cybercrimes, l'analyse de la fraude est entravée par le manque de données fiables (Yar, 2006, Holt et Bossler, 2014). La variété et l'ampleur de la fraude en ligne sont difficiles à déterminer : manque de report, manque de consensus international sur les catégories de fraudes, mélange de méthodes pour beaucoup de fraudes (en ligne et hors ligne) et manque de publication des données et informations relatives à la cyberfraude de la part des organismes nationaux sont autant d'entraves pour une meilleure compréhension du phénomène (Button, McNaughton Nicholls, Kerr et Owen, 2014).

En outre, la fraude en ligne est intimement liée au piratage informatique (Holt et Bossler, 2014), faisant en sorte que plusieurs acteurs et plusieurs actes sont à considérer. Cela rend très difficile l'appréhension de ces auteurs.

Définition et typologie de la fraude sur Internet

La fraude peut être envisagée comme étant une « une fausse représentation au moyen d'une déclaration ou d'une conduite faite sciemment ou imprudemment pour obtenir un avantage matériel » (Martin, 2003, p.1). Les victimes de fraude se voient alors dépossédées d'un bien ou d'argent par désinformation ou

tromperie. La fraude par internet (ou cyberfraude) est ainsi un terme général qui ne fait pas référence à un seul type d'actes mais qui englobe plutôt une variété de types d'actes.

Ainsi, Wall (2007) a développé une typologie très détaillée des fraudes sur internet. Elle se présente comme suit :

i. Les fraudes d'arbitrage des marchés
   a. contre l'État et les monopoles
      - médicaments
      - parfums
      - cigarettes
      - paris et casinos en ligne
   b. contre les annonceurs publicitaires (clics)
   c. contre les usagers (lignes surtaxées)

ii. Les fraudes associées au développement d'une économie en ligne
   a. contre les consommateurs
      - fraude aux enchères
      - fraude à l'abonnement
      - fraude aux locations de vacances
      - fraude au crédit facile
      - fraude aux investissements exotiques
   b. contre les aspirants à un rôle d'acteur

iii. Les fraudes par avance de fonds
   a. la fraude nigériane
   b. la fraude à la loterie
   c. la fraude au site de rencontre

Ryan, Lavoie, Dupont et Fortin (2011), pour leur part, se sont intéressés spécifiquement à la fraude via les médias sociaux. Ils classent ainsi ces fraudes en deux grands groupes : la fraude élaborée et le vol d'identité. La fraude élaborée se divise ensuite en quatre catégories : la fraude par abus de confiance, la fraude de location immobilière, la fraude par usage de faux et l'offre de service sans permis.

La fraude élaborée est définie par Ryan et al. (2011, p.7) comme étant « un acte de tromperie commis dans le but de réaliser un gain, et ce, sans vol d'identité ».

Koops et Leenes (2006, p.556) définissent le vol d'identité comme : « une fraude ou tout autre activité illégale dans laquelle l'identité d'une personne existante est utilisée comme cible ou outil principal sans le consentement de cette dernière ».

Il existe de multiples méthodes pour commettre une fraude, dont le hameçonnage ou le piratage. Le hameçonnage est un acte de tromperie par lequel l'usurpation d'identité est utilisée pour obtenir des informations d'une cible (Lastdrager 2014, 8). Il s'agit d'une technique par laquelle des fraudeurs tentent d'obtenir des renseignements personnels, souvent en envoyant un courriel falsifié. À cela s'ajoute l'ingénierie sociale, une méthode de piratage, précédemment définie.

Profil des fraudeurs

Avec Internet, les fraudeurs vont avoir une plus grande flexibilité pour mettre en place leur plan et réussiront à convaincre plus facilement leurs victimes. En effet, sans présence physique, nous nous laissons plus facilement influencer. La technologie va non seulement permettre une certaine perte de qualité dans les interactions mais elle va également permettre une désindividuation[19] des acteurs (Warschauer, 2003). L'anonymat d'Internet va faire en sorte que l'individu perd de son contrôle personnel et va alors adopter des comportements qu'il n'aurait pas eus hors de ce contexte. Cet anonymat « perçu » d'Internet est lié à la désinhibition en ligne. Les personnes ont beaucoup moins de restrictions dans le monde virtuel (Suler, 2004).

Ryan, Lavoie, Dupont et Fortin (2011) montrent que les fraudeurs sont en moyenne un peu plus jeunes que les victimes. Les personnes impliquées dans la fraude élaborée seraient plus âgées que celles impliquées dans le vol d'identité. Comme pour la majorité des crimes commis dans le cyberespace, les fraudeurs seraient principalement de sexe masculin. Aussi, une plus grande proportion de femmes impliquées dans la fraude se tournerait vers le vol d'identité plutôt que vers la fraude élaborée.

Un haut degré de compétence semble ne pas être nécessaire concernant les délits de fraude. Carignan (2015) a soulevé le fait que la fraude serait commise majoritairement par des cybercriminels venant d'Afrique et de péninsule Arabique, comme nous l'avons souligné dans le chapitre précédent. C'est l'une des rares recherches à s'être intéressée aux profils des cybercriminels en fonction de leur lieu d'origine. Cette auteure s'est inspirée de la théorie des activités routinière de Cohen et Felson et les résultats de son étude amènent à penser que l'accès à l'emploi, les inégalités financières, la vitesse d'Internet et l'accès au matériel informatique, différents à l'échelle mondiale, auront un impact sur les opportunités de commission de fraudes pour le délinquant.

En effet, si nous regardons les « YahooBoys »[20] , ces jeunes fraudeurs nigerians, il est évident que la fraude en ligne a été observée comme un moyen de subsistance et le chômage considéré comme un facteur crucial attirant toujours plus de jeunes vers ce cybercrime (Adeniran, 2008; Tade et Aliyu, 2011).

Profil des victimes de fraude sur Internet

La fraude en ligne est devenue un problème majeur dans plusieurs pays, faisant des millions de victimes. Les victimes de fraude sont souvent négligées par la recherche en comparaison des victimes d'autres genres de crimes (Button, McNaughton Nicholls, Kerr et Owen, 2014).

Cette négligence peut, entre autres, venir du fait qu'il y un

faible taux de report de cet acte. Les raisons de ce faible report sont, selon la littérature, les mêmes que pour la fraude dans le milieu physique : les victimes se blâment d'être tombées dans un piège, elles sont embarrassées et aussi ne savent pas vers qui se tourner pour parler de leurs mésaventures surtout s'il s'agit d'une perte d'argent minime.

La particularité de la cyberfraude, quel qu'elle soit, est que la victime va jouer un rôle actif dans la commission de l'acte. Ainsi, ce rôle actif va être un facteur important de honte chez les victimes, qui se demanderont généralement pourquoi elles ont été aussi naïves. En même temps, elles vont avoir un fort sentiment de culpabilité car pour elles, elles ont contribué à la réussite du fraudeur (Burgard et Schlembach, 2013).

En termes d'importance, les individus sont plus touchés par la fraude, viennent ensuite les entreprises et les gouvernements (Carignan, 2015).

Concernant les victimes individuelles, certaines caractéristiques vont tout de même ressortir des résultats des recherches sur le sujet. Toutefois, au vu de la variété des types de fraudes qui existent, les chercheurs n'ont pas relevé un profil unique de victimes en ligne. En effet, ils vont plutôt se pencher sur un type de fraude en particulier pour analyser les facteurs de risques de victimisation rattachés spécifiquement à chaque fraude.

Concernant les fraudes réalisées au travers des médias sociaux, Ryan, Lavoie, Dupont et Fortin (2011) ont fait ressortir des caractéristiques sociodémographiques et ont trouvé que ces fraudes touchent autant les hommes que les femmes. Aussi, les victimes auraient une moyenne d'âge plus élevée que les délinquants (33,3 ans). En outre, les résultats de l'étude de Reyns (2013) sur le vol d'identité montrent que les hommes et les personnes âgées sont plus susceptibles d'être victimes que les femmes et les jeunes. Les individus qui ont des revenus plus élevés sont également plus susceptibles d'être victime de de vol d'identité que les individus qui ont un revenu de moins de 90 000 $ CAD par an.

Reyns (2013) a testé la théorie de l'activité routinière de Cohen et Felson. Ses résultats ont montré que les personnes qui utilisent internet pour envoyer des courriels ou des messages instantanés et/ ou pour effectuer des opérations bancaires en ligne ont 50 % plus de risque d'être victimes de vol d'identité que les autres. Celles qui font du magasinage en ligne et qui font du téléchargement ont 30 % plus de risque d'être victimes. Ses résultats corroborent les résultats trouvés par Koops et Leenes (2006) pour qui tous ces comportements routiniers sont autant d'activités risquées qui exposent les utilisateurs à une menace de vol d'identité.

Van Wilsen (2013) a pour sa part étudié la fraude à la consommation en appliquant la théorie du faible contrôle de soi de Gottfredson et Hirschi. Il a trouvé que les personnes avec un faible contrôle de soi avaient un plus haut risque d'être victime.

Il est toutefois à noter que pour de nombreux auteurs, l'approche des activités routinières n'est pas le meilleur cadre pour étudier la fraude en ligne de manière générale et qu'il est donc conseillé de continuer à chercher les meilleurs facteurs de risque pour ce genre de crime (Ngo et Paternoster, 2011).

Par ailleurs, il est intéressant de noter que, concernant la fraude bancaire en ligne, il ne semble pas exister de cible appropriée et spécifique. Devenir victime est une coïncidence, un phénomène contextuel. La victimisation semble se produire parce que les fraudeurs ajustent continuellement leur modus operandi en fonction des évènements, parce qu'ils parviennent à gagner la confiance des clients ou parce que les clients ne prêtent pas assez d'attention (Jansen et Leukfeldt, 2016).

L'ingénierie sociale étant la technique privilégiée des fraudeurs, devant les compétences techniques, les solutions technologiques concernant la prévention de ce genre de cybercrime est alors limitée. La meilleure option à envisager selon Ryan et al. (2011) est alors l'éducation et la sensibilisation des usagers avec des alertes publiques fréquentes sur le risque de fraude en ligne.

Également, une collecte de données standardisée pourrait permettre d'aider le travail de prévention des organismes anti-fraude.

La cyberviolence

Encadré 3.5. **Piratage de photos intimes**

Christopher CHANEY

Entre novembre 2010 et octobre 2011, Christopher Chaney, citoyen américain âgé de 35 ans, s'est servi des informations disponibles sur différents blogs de célébrités pour deviner les mots de passes de leurs comptes de messagerie Google ou Yahoo. Il a réussi à pirater les comptes d'une cinquantaine d'entre elles, telles que Scarlett Johansson, Mila Kunis, Christina Aguilera, et Renee Olstead, et d'accéder ainsi à d'innombrables courriels, photos et documents confidentiels.

Deux femmes de son entourage ont également été victimes de ces cyberattaques, Christopher Chaney ayant notamment transféré à son père des photos à caractère sexuel d'une ancienne collègue de travail. Ce type de cyber-violences est généralement très lourd de conséquences chez les victimes : tandis que l'une d'entre elles connaît depuis de graves crises d'anxiété et de panique, l'autre a développé une forte tendance à la dépression et la paranoïa. Selon elles, Christopher Chaney est un homme cruel, effrayant, dont les actes

ont affecté leur vie de façon irrémédiable.

De la même manière, Christina Aguilera, Mila Kunis et Scarlett Johansson ont toutes les trois accepté de témoigner publiquement contre l'auteur des faits, dans l'espoir de sensibiliser la population à de telles cyberviolences. Christina Aguilera a avoué qu'aucune indemnisation ne pourra atténuer le sentiment d'insécurité né d'une telle atteinte à la vie privée. Scarlett Johansson a fait part de l'humiliation et de la honte ressentie lorsque Christopher Chaney a divulgué des photos d'elle nue, tandis que l'actrice et chanteuse Renee Olstead a déclaré au tribunal avoir tenté de se suicider.

Si Christopher Chaney s'est excusé pour l'ensemble de ses actions et reconnu un sentiment de compassion à l'égard de ses victimes, les faits révèlent une tendance certaine au voyeurisme, renforcée par un comportement obsessionnel et compulsif. Il a été condamné en décembre 2012 à 10 ans de réclusion criminelle. Selon le juge de district américain S. James Otero, « ces types de crimes sont aussi graves et pernicieux que le harcèlement physique ».

Les recherches commencent à s'intéresser aux cyberviolences et notamment à l'utilisation d'Internet pour faciliter ce type d'actes (Holt et Bossler, 2014). La fréquence d'utilisation des médias électroniques associée à l'augmentation vertigineuse de l'utilisation des téléphones mobiles accroît les opportunités d'être impliqué dans des cas de cyberviolence, à la fois comme victime ou comme délinquant (Smith, Mahdavi, Carvalho, Fisher, Russell, et Tippett, 2008; Holt et Bossler, 2014).

Wall (2001) définit les cyberviolences comme étant une distribution de matériel injurieux, blessant et dangereux en ligne. Comme pour les précédents cybercrimes, la cyberviolence est une catégorie générique qui englobe une variété d'actes. Parmi ceux-ci, nous retrouvons notamment l'intimidation [bullying] et le harcèlement [stalking, harassment]. Ce sont les catégories qui sont aujourd'hui le plus référencées et sur lesquelles nous avons el plus de données (Holt et Bossler, 2014).

Dubé et Drouin (2015, tel que cité par Bernier, 2016) parlent de cyberharcèlement pour définir l'utilisation des technologies de l'information et de la communication (TIC) afin établir une communication virtuelle itérative avec une autre personne dans le but de commettre des actes répétés de violence psychologique. Le harcèlement électronique consiste à menacer, à insulter, à harceler ou à blesser des individus par le biais de communications électroniques telles que le courrier électronique et les téléphones cellulaires (Beran et Li, 2005).

Le cyberharcèlement peut prendre la forme de sollicitation sexuelle indésirable, de harcèlement sexuel, de comportement voyeuriste, de commentaires obscènes et de spam (Behm-Morawitz et Schipper, 2015). Une des formes qui commence à être très répandue est « la vengeance pornographique ». Ceci consiste en la diffusion ou le partage en ligne (parfois hors ligne) et non consenti, d'images explicites de quelqu'un, par un partenaire ou ex-partenaire, ou par des pirates (Hall, 2017).

La cyberintimidation est définie comme une conduite hostile et répétitive, médiatisée par un support électronique, qu'un individu ou groupe de personnes utilise dans le but de causer du tort ou de l'inconfort aux autres (Tokunaga, 2010). Nous pouvons retrouver plusieurs formes de cyberintimidation : des agressions à caractère direct, qui impliquent la participation de la victime, et des agressions à caractère indirect, qui affectent la victime de façon détournée (Willard, 2005).

Willard (2005) identifie sept formes d'agression pouvant être associées à la cyberintimidation :

i. Le harcèlement en ligne [online harrassment] qui implique l'envoi direct à la personne ciblée de multiples messages blessants via courriel ou messagerie instantanée;

ii. Les propos inflammatoires [flaming] sont des attaques personnelles, à l'endroit d'un membre ou groupe de membres d'un réseau social, qui sont publiées avec pour but de châtier les tenants d'une opinion plutôt que de faire avancer une discussion;

iii. La médisance [putdowns] implique la publication ou le partage avec d'autres personnes d'un même réseau social de matériel intentionnellement nocif ou sans fondement (fausses rumeurs, images trafiquées, compilation vidéo d'incidents embarrassants, etc.) concernant la personne ciblée;

iv. La sortie [outing] consiste à rendre publiques, de façon parfois faussement accidentelle, des informations à caractère privé ou embarrassant (publication de coordonnées personnelles, photos compromettantes, mention d'une relation gardée secrète, etc.) concernant la personne ciblée;

v. Les tentatives de rapprochement indésirables [cyberstalking] se produisent lorsqu'un individu cause de la détresse à la personne ciblée en sollicitant à répétition son attention de façon inappropriée ou non désirée ou en supervisant ses activités en ligne dans le but de faciliter de futurs rapprochements;

vi. La mascarade [impersonation] se produit lorsque l'agresseur prétend être quelqu'un d'autre afin de diffuser du matériel nocif ou utilise l'identité de la personne ciblée afin de manipuler ses relations sociales;

vii. Le rejet [exclusion] est le renvoi d'un membre d'un groupe en ligne d'une façon injuste ou qui s'avère inutilement cruelle.

Welsh et Lavoie (2012) soutiennent que la cyberintimidation et le cyberharcèlement sont des formes différentes de cyber-harcèlement. Le paramètre pour différencier ces deux types de cy-

berharcèlement serait l'âge. Ainsi, la cyberintimidation décrirait une catégorie de cyberharcèlement impliquant plutôt des enfants et des jeunes alors que le cyberharcèlement ferait plutôt référence à des adultes (Miller, 2006, Welsh et Lavoie, 2012).

Profil des délinquants

Comme vu dans le cas de la fraude, le fait de ne pas être face à la victime provoque souvent sa déshumanisation, faisant en sorte que l'agresseur se permet d'être beaucoup plus extrême et offensant dans ses propos (Bernier, 2016). L'intimidation va impliquer un rapport de force et de pouvoir de l'intimidateur sur la victime, grandement favorisé par l'anonymat offert par Internet (Bourque, 2012). Ce rapport de force va devenir plus accessible pour de nouvelles personnes de par la configuration d'Internet. Aussi, il a été démontré que ce rapport de force était la plupart du temps imposé par un « ami » (au sens des réseaux sociaux) plutôt que par un étranger (Mishna, Wiener & Pepler, 2008).

La cyberintimidation concernerait plutôt des jeunes adolescents. En outre, alors que la majorité des intimidateurs traditionnels sont des garçons, la cyberintimidation serait commise autant par des filles que des garçons (Cappadocia, Craig et Pepler, 2013).

La vengeance et le défoulement vont être deux motivations principales concernant les diverses manifestations de cyberintimidation (Shariff, 2009, p. 35).

Les chercheurs ont trouvé que le comportement d'intimidation serait lié à un faible contrôle de soi. Toutefois, la relation ne serait pas aussi forte pour la cyberintimidation que pour le harcèlement traditionnel (Kerstens et Veenstra, 2015). Les personnes qui participent à un acte de cyberintimidation éprouvent un sentiment d'impunité. Il est toutefois établi que ces jeunes manifestent de l'empathie.

De bonnes compétences en informatiques ainsi qu'une connaissance des milieux virtuels sont généralement liées à un risque d'être intimidateur ou harceleur (Chehab, 2016).

Aussi, les jeunes auteurs d'intimidation et de harcèlement seraient également eux-mêmes victimes d'intimidation et de harcèlement, à la fois en ligne et hors ligne (Kerstens et Veenstra, 2015). Il est intéressant de rajouter que la qualité de la supervision parentale joue un rôle sur les comportements des jeunes en ligne. En discutant régulièrement de leurs habitudes de navigation avec leurs parents, ces jeunes auraient deux fois moins de chance de victimiser leurs pairs (Ybarra et Mitchell, 2004).

Outre ces profils d'intimidateur, la vengeance pornographique est aussi le fait d'individus qui veulent exercer du pouvoir et du contrôle sur leurs victimes. Nous verrons, dans la contribution de Hall et Hearn, que le profil de ces auteurs commence à être analysé aujourd'hui et qu'au-delà de la simple vengeance justifiant l'acte commis, il s'agit plutôt d'une réaction de l'émasculation ressentie par les hommes lorsqu'ils perdent le pouvoir dans leur relation (Hall, 2017).

Profil victimes

Davantage de filles que de garçons seraient victimes de formes quelconque de harcèlement lorsqu'elles interagissent en ligne (Cappadocia, Craig et Pepler, 2013 ; Wade et Beran, 2011). En effet, selon Holt et Bossler (2008), le simple fait d'être une femme augmente de 2,75 les risques d'être harcelé en ligne et triple le risque d'être l'objet d'avances sexuelles.

Holt et Bossler (2008) tout comme Reyns, Henson et Fisher (2011) visent à montrer que plusieurs liens peuvent être faits entre la théorie des activités routinières et la victimisation associée au cyberharcèlement. La cible adéquate, l'un des trois facteurs à réunir pour la commission d'un acte délictuel, serait une personne qui passe beaucoup de temps sur les sites de conversation en ligne, qui utilise beaucoup les réseaux sociaux et qui se sert souvent de sa boite de messagerie. Les compétences informatiques seraient un facteur de protection uniquement chez les hommes. Les anti-virus et autres logiciels de protection ne seraient pas utiles pour empêcher les risques de victimisation dans le cadre du cyberharcèlement en ce sens qu'ils ne protègent que les attaques commises contre l'ordinateur. Le fait pour des femmes de s'adonner à des comportements déviants en ligne, tel que le piratage, ou bien le fait d'avoir des amis qui se livrent à ce genre de comportement, augmente considérablement les risques de victimisation de harcèlement et d'intimidation. En outre, le fait de mettre des photos en ligne, le fait d'ajouter des personnes inconnues sur ces profils de réseaux sociaux a un impact sur le risque de victimisation.

Les cyberviolences, harcèlement ou intimidation, ont des impacts dévastateurs sur la vie des victimes. Blaya (2011) rapporte, en effet, que l'impact de la cyberviolence pourrait être plus grave que celui de la violence traditionnelle. Le harcèlement ou l'intimidation peut avoir lieu partout et à n'importe quel moment, la maison n'étant plus un refuge. Aussi, l'identité de l'intimidateur ou du harceleur n'est pas forcément connue de la victime, faisant en sorte qu'elle vit dans une angoisse perpétuelle de peut-être croiser son agresseur. Les victimes de ces cyberviolences vivent de sérieuses conséquences psychologiques. Elles sont notamment plus à risque de dépression ou de suicide (Holt et Bossler, 2014).

Il est donc nécessaire aujourd'hui de mieux prévenir ce genre de crime et la recherche doit commencer à évaluer les impacts des plans de prévention déjà mis en place, comme nous le verrons dans le prochain chapitre.

Conclusion

Ce chapitre avait pour objectif d'examiner l'avancée de la recherche criminologique en ce qui concerne la cybercriminalité. En effet, une meilleure compréhension des facteurs de risque personnels et contextuels est essentielle pour la mise en place d'une prévention plus efficace et mieux dirigée. Ainsi, nous avons d'abord vu que, malgré le fait que la cybercriminalité ne soit pas une réalité nouvelle, la recherche a encore beaucoup de travail à accomplir afin de mieux comprendre ce phénomène, dont l'ampleur et la vitesse à laquelle il a émergé constituent des défis importants pour le secteur académique comme pour les décideurs.

Le premier problème que nous avons soulevé concerne le manque de consensus sur la définition même de la cybercriminalité. Ce manque de consensus à un effet domino sur tout le processus de la recherche. En ne considérant pas la même définition de la cybercriminalité en général, et des cybercrimes en particulier, les résultats obtenus sont quelque peu sporadiques et sont très difficilement comparables à un niveau international. Ce manque de résultats probants ne va pas aider à élaborer des politiques publiques efficientes ni même à mettre en œuvre des collaborations effectives.

Aussi, les recherches sont assez limitées et pour la plupart conduites dans des pays développés alors même qu'Internet est maintenant largement répandu dans le monde (Carignan, 2015). Nous avons ensuite vu que les théories criminologiques aujourd'hui utilisées sont principalement d'orientation sociologique même s'il existe un corpus de recherche avec une approche psychologique qui commence à émerger mais qui reste encore à approfondir.

Finalement, les trois cybercrimes étudiés ici reflètent bien la complexité de la cybercriminalité. Il est très difficile voire quasiment impossible de faire ressortir un profil spécifique de délinquants et de victimes. Les facteurs de risques d'Internet (voir encadré) viennent s'ajouter et rendent plus difficile l'étude de ce problème.

La cybercriminologie, qui est définie comme « l'étude des causes des crimes se produisant dans le cyberespace et qui ont un impact dans l'espace physique » (Jaishankar, 2007, p.1), pourrait permettre de pallier à tous les problèmes que rencontre aujourd'hui la recherche sur la cybercriminalité.

ENCADRÉ 3.6. **Facteurs de risque d'Internet (Koops, 2011, p.740)**

1. Une portée globale, qui permet aux auteurs de rechercher les ordinateurs et les victimes les plus vulnérables, où qu'ils se trouvent dans le monde, sans avoir à quitter leur foyer ou le cyber café le plus proche (Yar, 2005: 421).
2. De ce fait, la déterritorialisation implique que la cybercriminalité est, par définition, essentiellement internationale, avec des défis conséquents en termes de juridiction et de collaboration internationale.
3. L'organisation du cyberespace permet des réseaux flexibles et décentralisés au sein desquels les auteurs criminels peuvent s'organiser de manière souple afin de diviser le travail ou partager des compétences, des connaissances ou des outils (cf. infra, section 3.3).
4. Le cyberespace facilite en outre l'anonymat pour les criminels possédant les connaissances nécessaires et faisant l'effort d'utiliser les outils d'anonymisation (…). En revanche, des criminels moins technologiquement compétents sont (ou se sentent) relativement anonymes lorsqu'ils développent leurs activités à grande distance, abrités derrière une adresse IP, un courriel ou un compte Facebook frauduleux, souvent difficile à connecter à un individu spécifique (Sandywell, 2010, p. 44).
5. La possibilité d'interactions à distance entre les auteurs et les victimes effacent de potentielles barrières sociales rencontrées par les auteurs dans les relations en personne; ainsi, le cybercrime implique des relations anonymes, rhyzomatiques et en réseau entre les victimes et les auteurs de crimes (Sandywell, 2010: 44).
6. L'environnement virtuel facilite la manipulabilité des données et des programmes à un coût minimal (Sandywell, 2010: 44) car il est fondé sur une représentation digitale (permettant de copier sans perdre de qualité, et de modifier sans laisser de traces), mais aussi car Internet fut construit comme une infrastructure ouverte, afin d'encourager l'innovation apportée par ses propres usagers.
7. En outre, cet environnement permet l'automatisation des processus criminels, où un programme diffuse par Internet peut lancer et répliquer une attaque à des millions de reprises simultanément et pour de longues périodes, et où des programmes très simples peuvent également être facilement adaptés par les fameux « script kiddies », afin de créer de nouveaux virus (Wall, 2007).
8. La question de l'échelle est également importante, car la cybercriminalité peut ainsi faire exploser l'échelle d'un crime, minimal quand il est pris individuellement, mais qui devient un facteur de dommages majeurs en raison de sa portée globale et massive (Franks, 2010).
9. De la même manière, l'explosion des échelles per-

met l'accumulation de gains individuellement non substantiels grâce à des techniques dites « salami»; ceci constitue l'un des principaux défis liés au cybercrime, minimisant le signalement, mais aussi les causes pour enquêter et poursuivre les criminels (Wall, 2007).

10. Ainsi, l'information devient, dans le cyberespace, un bien de grande valeur, dans les marchés légal et illégal (Wall, 2007: 32).

11. Le cyberespace possède des caractéristiques structurales qui limitent la possibilité des contrôles qui servent, dans le monde réel, d'obstacles sociaux et techniques à la commission de crimes (Yar, 2005 : 423).

12. Enfin, le cycle d'innovation est, dans le cyberespace, particulièrement rapide, permettant ainsi le développement de nouvelles techniques et de nouveaux outils au sein de délais très court, ce qui facilite le contournement des mesures de sécurité et la création de nouveaux vecteurs et activités criminels.

Contribution

La cyber-criminologie et la théorie de la transition spatiale : contribution et impact

K. Jaishankar
Professeur
Raksha Shakti University (Police and Internal Security University)
International Journal of Cyber Criminology
International Journal of Criminal Justice Sciences
Inde

Introduction

Le cyberespace a été exploité par de nombreux domaines d'études ; cependant, la criminologie a trop tardivement exploré cet espace et abordé cette nouvelle forme de criminalité que l'on nomme la cybercriminalité. J'ai fondé une nouvelle sous-discipline académique de criminologie, la « cyber-criminologie » en 2007, avec le lancement d'une revue, « the International Journal of Cyber Criminology » (www.cybercrimejournal.com). J'ai inventé le terme « cyber-criminologie » et défini la cybercriminalité comme étant « l'étude de la causalité des crimes qui se produisent dans le cyberespace et son impact dans l'espace physique » (Jaishankar, 2007a, par. 1). En tant que discipline universitaire, la cyber-criminologie englobe un champ de recherche multidisciplinaire – criminologie, sociologie, psychologie, victimologie, technologie de l'information et sciences informatiques / de l'internet. « Au fond, la cyber-criminologie implique l'examen du comportement criminel et de la victimisation dans le cyberespace selon une perspective théorique criminologique ou comportementale » (Jaishankar, 2010, 2011 ; Ngo & Jaishankar, 2017, p. 4 ; Jaishankar, 2017).

Théorie de la transition spatiale de la cybercriminalité : une théorie unique pour faire avancer la discipline de la cyber-criminologie

De nombreux chercheurs ont tenté d'aborder les causes de la cybercriminalité à l'aide de théories traditionnelles telles que la théorie de l'apprentissage social, la théorie des activités routinières et la théorie de la dérive et de la neutralisation. Cependant, ils n'ont pas pleinement réussi à expliquer les cybercrimes, car le cyberespace est un tout nouvel espace, et la cybercriminalité une toute nouvelle forme de criminalité (Yar, 2005 ; Jaishankar, 2007b, 2015). J'ai proposé la théorie de la transition spatiale de la cybercriminalité (2008) car j'ai constaté qu'aucune théorie n'a spécifiquement été créée pour aborder les causes de la cybercriminalité. J'ai premièrement présenté cette théorie au John Jay College of Criminal Justice de l'université de la ville de New York, aux États-Unis, en 2007. Plus tard, j'ai publié cette théorie sous forme d'un chapitre dans un ouvrage intitulé « Crimes of the Internet », édité par Frank Schmalleger et Michael Pittaro (2008), et publié par Prentice Hall, aux États-Unis (Jaishankar & Chandra, 2017).

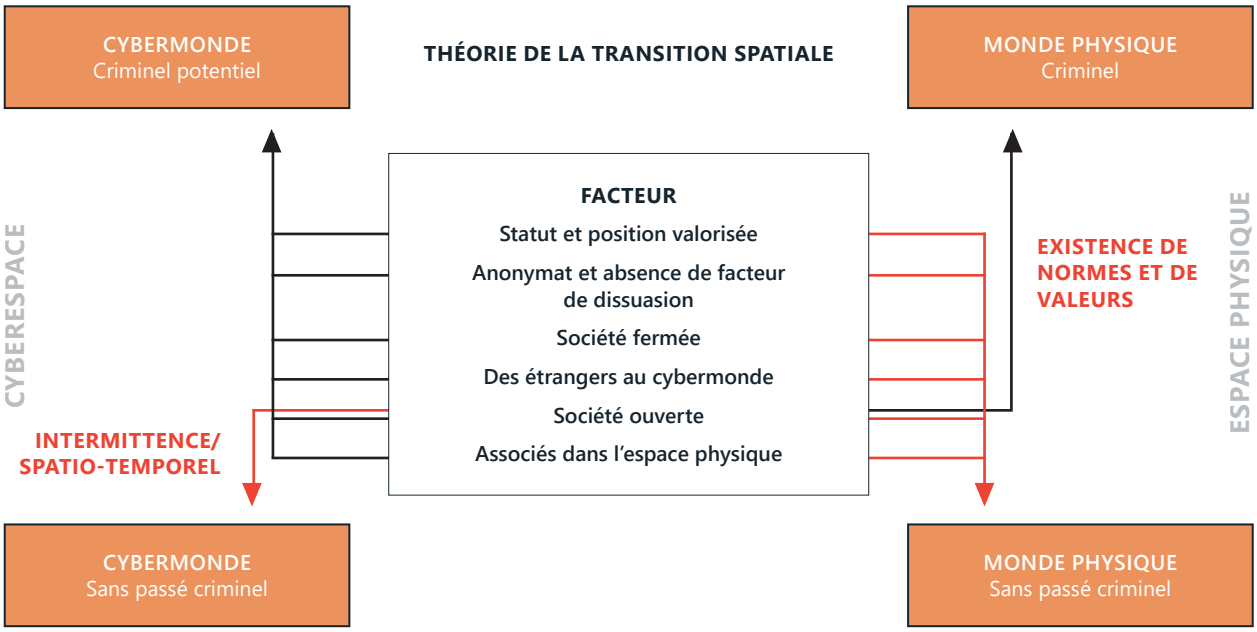
La théorie de la transition spatiale de la cybercriminalité (2008) fait progresser le domaine de la cyber-criminologie. La « théorie de la transition spatiale » est une explication sur la nature du comportement des personnes qui font ressortir leur comportement conforme et non-conforme dans l'espace physique et le cyberespace » (Jaishankar, 2008, pp. 292-296). Selon la théorie de la transition spatiale, les gens se comportent différemment lorsqu'ils se déplacent d'un espace à un autre (Jaishankar, 2008, p. 292-296 ; Jaishankar & Chandra, 2017).

Propositions issues de la théorie de la transition spatiale (Jaishankar, 2008)

1. Les personnes ayant un comportement criminel réprimé (dans l'espace physique) ont une propension à commettre des crimes dans le cyberespace, qu'elles ne commettraient pas dans l'espace physique, en raison de leur statut et de leur position.
2. La souplesse de l'identité, l'anonymat dissociatif et l'absence de facteur de dissuasion dans le cyberespace offrent aux délinquants le choix de commettre un cybercrime.
3. Le comportement criminel des délinquants dans le cyberespace est susceptible d'être importé dans l'espace physique, qui, dans l'espace physique, peut également être exporté dans le cyberespace.
4. Les incursions intermittentes des délinquants dans le cyberespace et la nature spatio-temporelle dynamique de celui-ci offrent la possibilité de s'évader.
5. (a) Des étrangers sont susceptibles de s'unir dans le cyberespace pour commettre des crimes dans l,espace physique. (b) Des associés dans l'espace physique sont susceptibles de s'unir pour commetre des crimes dans le cyberespace.
6. Les personnes issues d'une société fermée sont plus susceptibles de commettre des crimes dans le cyberespace que les personnes issues d'une société ouverte.
7. Le conflit entre les normes et les valeurs de l'espace physique et les normes et les valeurs du cyberespace peut mener à la cybercriminalité. Les enjeux de la mise à l'essai de la théorie de la transition spatiale.

Les enjeux de la mise à l'essai de la théorie de la transition spatiale

Cette théorie est testée empiriquement par peu de chercheur: Zhang (2009), Danqua et Longe (2011) et plus récemment Kethineni, Cao et Dodge (2017). Danqua et Longe (2011) ont testé la théorie de la transition spatiale au Ghana. Ils ont constaté que la théorie de la transition spatiale s'applique davantage à la cyberintrusion, à la cyberdéception et au vol, et à la cyberpornographie qu'à la cyberviolence (Kethineni, Cao et Dodge, 2017, p. 7). Kethineni, Cao et Dodge (2017, pp. 13-14) ont testé



Source: Space Transition Model inspiré de Jaishankar (2008) par Danquah and Longe (2011)

la théorie de la transition spatiale dans leur étude et ont trouvé un certain soutien. Ils mentionnent « l'étude actuelle appuie certaines des explications théoriques proposées par la théorie de la transition spatiale. En particulier, la souplesse de l'identité, l'anonymat dissociatif, l'association facile en ligne et le manque de dissuasion, amènent de plus en plus de criminels traditionnels sur internet. De plus, l'idée que lorsqu'il y a un conflit entre les normes et les valeurs de l'espace physique, et les normes et les valeurs du cyberespace, les délinquants choisissent le cyberespace, a été appuyée dans cette étude (Jaishankar et Chandra, 2017).

De plus, la théorie de la transition spatiale n'explique pas toutes les formes de cybercriminalité (Danqua & Longe, 2011 ; Jaishankar & Chandra, 2017). Si une seule théorie criminologique n'est pas en mesure d'expliquer toutes les formes de criminalité, comment une seule théorie de la cybercriminalité expliquerait-elle toutes les formes de cybercriminalité ? Je crois que la théorie de la transition spatiale n'est qu'un point de départ des théories sur la cybercriminalité et, à l'avenir, je m'attends à ce que d'autres théories sur la cybercriminalité soient créées par des universitaires.

Conclusion

La croissance du champ de la cyber-criminologie est impérative dans la mesure où il y a eu une recrudescence de la cybercriminalité au cours de la dernière décennie. Bachmann (2008) a souligné que le développement du domaine de la cyber-criminologie se traduit par deux indicateurs forts. D'une part, le lancement de la revue exclusive, le International Journal of Cyber Criminology en 2007 et d'autre part, l'augmentation significative des publications scientifiques sous forme de livres, d'articles de revues et de critiques de livres dans le domaine de la cybercriminalité / cybercriminologie au cours des dix dernières années de la création du champ de la cyber-criminologie par K. Jaishankar. De plus, la théorie de la transition spatiale des cybercrimes est « reconnue par de nombreux chercheurs (Diamond & Bachmann, 2015 ; Holt & Bossler, 2014, 2016 ; Holt, Bossler, 2015 ; Holt, Bossler, & Spellar, 2015 ; Moore, 2012, Wada, Longe, & Danquah, 2012) comme une contribution remarquable au domaine de la criminologie en général et de la cybercriminalité en particulier » (Ngo & Jaishankar, 2017, p. 5 ; Jaishankar, 2017).

Moore (2010) a consacré un chapitre sur la « cybercriminalité » dans son livre intitulé « Cybercrime investigating high-technology computer crime ». Stalans et Finn (2016, pp. 502-503) estiment que « le domaine est jeune, mais il a commencé à accumuler des connaissances sur de nombreuses formes de cybercriminalité, y compris des collections de livres présentant des recherches dans le monde entier (p. ex, Jaishankar, 2011 ; Kshetri, 2013 ; Wall, 2007) et neuf (ma propre accentuation) revues sur l'état actuel des connaissances » (Bachmann, 2008 ; Choi, 2015 ; Diamond & Bachmann, 2015 ; França, 2018 ; Holt & Bossler, 2014, 2016 ; Maras, 2016 ; Nhan & Bachmann, 2010 ; Ngo & Jaishankar, 2017 ; Stalans & Finn, 2016).

Ngo et Jaishankar (2017, p. 5) estiment que « l'avancement du domaine de la cyber-criminologie est un domaine d'enquête saillant et pertinent (Jaishankar, 2010) parce que, contrairement au crime traditionnel ou au crime commis dans le monde physique, la cybercriminalité ou le crime commis dans le monde virtuel a le potentiel de causer des dommages énormes, tant tangibles (c.-à-d. pertes économiques) qu'intangibles (p. ex. l'utilisation non autorisée de données personnelles) ». Selon Moore (2012, p. 283), « il est indéniable que ce domaine de la criminologie (la cyber-criminologie) est extrêmement excitant et qu'il est certain qu'il deviendra un domaine bien documenté du comportement criminel ». Il est donc prévu que le champ de la cyber-criminologie prendra de l'ampleur et qu'il n'y aura plus de négligence ou de marginalisation de la criminologie dominante (Jaishankar, 2017).

Contribution

Infraction de distribution d'images intimes, « vengeance pornographique », abus en ligne et prévention

Matthew Hall
Ph. D, Chercheur à l'université d'Ulster, Royaume-Uni

Jeff Hearn
Professeur émérite
Hanken School of Economics, Finlande

Introduction

Les infractions liées à la distribution d'images intimes, d'abus sexuels ou de «pornographie» non consensuelle, connue plus familièrement comme «vengeance pornographique», se caractérisent par la distribution en ligne non consentie, parfois hors ligne, ou le partage d'images explicites d'une autre personne dans le but de se venger, divertir les autres ou pour des raisons politiques. Bien que les ex-conjoints soient souvent désignés comme les principaux auteurs de ce délit, les conjoints actuels, les (ex)amis à la fois des victimes et des auteurs, les personnes connues par la victime, les personnes qui cherchent à venger leurs amis, les pirates en ligne et les trolls, entres autres, peuvent également être impliqués (Tyler, 2016).

L'impact négatif sur les victimes est tout aussi important et profond en termes de santé physique, psychologique et de bien-être comme c'est le cas pour de nombreuses autres formes de violence et d'abus sexuels ou basés sur le genre. Les victimes parlent de toute une série d'effets négatifs: sentiments d'humiliation, honte, embarras et Atteinte à leur réputation que ce soit auprès de partenaires intimes, de la familles, des ami(e)s, des collègues du travail comme auprès du public en général; honte sexuelle, problèmes sexuels et problèmes d'image corporelle avec des partenaires intimes; perturbations au niveau de l'éducation et de l'emploi; développement de caractère paranoïaque ou hyper vigilant, préoccupation quant à la sécurité personnelle. Certaines victimes ont par exemple révélé avoir été suivies, harcelées et menacées de viol collectif en raison de la divulgation de leurs informations personnelles, d'autres victimes se sont même enlevé la vie (Citron et Franks, 2014).

Technologie, distribution d'images et abus en ligne

Le développement des téléphones intelligents a favorisé l'explosion des « sextos » - c'est-à-dire l'envoi d'images sexuellement explicites par message texte (Hasinoff, 2015). Une enquête auprès de 5 000 adultes (Match.com, 2012) a révélé que 57 % des hommes et 45 % des femmes avaient reçu une photo explicite sur leur téléphone, et que 38 % des hommes et 35 % des femmes en avaient envoyé une. Une fois envoyées, ces images supposément « privées » sont potentiellement accessibles à tous si elles sont téléchargées et partagées sur le Web (Penney, 2013).

Le partage d'images explicites d'une personne tierce sur le Web sans son consentement est une des multiples facettes qui résultent des échanges sociaux, de la sexualité ou bien des violences en ligne, et plus particulièrement les cyber abus. On entend par cela, une action intentionnelle, en ligne, dont le but est de nuire à l'autre, de manière répétée, sans que la victime ne soit généralement en mesure de se défendre (Slonje, Smith & Frisén, 2013). Le plus grave dans les cas d'abus en ligne est le déséquilibre entre celui qui détient le pouvoir et le manque de consentement, souvent accentué par la capacité de ce dernier à rester anonyme. L'abus en ligne peut prendre plusieurs formes telles que l'intimidation et le harcèlement en ligne, c'est-à-dire l'intention de menacer ou créer la peur chez la personne ciblée en diffusant ou en envoyant des messages répétés et des photos (généralement via des hyperliens diffusés sur des sites de vengeance pornographique), les agressions en ligne, les propos enflammés (flaming[21]), les vidéolynchages (happy slapping[22]), la surveillance et les menaces en ligne (stalking and trolling) (Hearn & Parkin, 2001). La « vengeance pornographique » englobe et partage des similitudes avec ces formes d'abus en ligne, tel que le fait de diffuser des images explicites ou des vidéos accompagnés de propos offensifs ayant pour but de porter atteinte, faire du mal, agresser ou humilier. Ces images ou ces vidéos peuvent également être accompagnées de courriels abusifs, être relayés en masse sur des forums en ligne ou susciter des attaques personnelles sur les blogs et dans les commentaires d'articles de journaux (Svoboda, 2014, p. 48). La « vengeance pornographique » peut également avoir les mêmes caractéristiques que d'autres formes d'abus en ligne, pour ne citer que le fait de chercher à porter atteinte intentionnellement à la réputation d'une personne en propageant des propos diffamatoires, des rumeurs ou des photos (numériquement retouchées, on peut citer comme exemple les deepfakes[23]), ou avoir recours à la tromperie et la supercherie, qui consiste à amener ou pousser une personne à révéler des détails de sa vie privée, dans le but de l'embarrasser (Lacey, 2007).

La vengeance pornographique exploite les nombreuses caractéristiques des TIC et les développe de multiples façons, avec des possibilités et des effets illimités et indéfinis. Les TIC apportent un certain nombre de particularités à la vie quotidienne : compression temps/espace de la distance et de la séparation physique, instantanéité en temps réel, asynchronisme, reproductibilité des images, création de corps virtuels, brouillage du « réel » et du « figuratif ». Plus précisément, les propriétés des réseaux de communication informatisés comprennent une largeur de bande plus large, la portabilité sans fil, la connectivité mondialisée, la personnalisation (Wellman, 2001) et l'effacement, voire l'abolition, des frontières strictes entre en ligne et hors ligne, codex et net (Gilbert, 2013). Cela soulève des questions complexes, comme celle de savoir comment de telles violations peuvent être simultanément matérialisées et virtuelles. Il n'est pas réductible à une seule forme ou possibilité, peut être multi-médial, et ne peut être compréhensible que dans le contexte d'un éventail de pratiques sociales envisagé au-delà du texte de vengeance pornographique visible et lisible. Par exemple, un

message particulier peut faire référence, implicitement ou explicitement, à un autre sujet ou évènement social antérieur hors ligne et hors écran, positif ou négatif, pour une, les deux ou plusieurs parties, ce qui ne serait pas déchiffrable par une partie ou un téléspectateur non impliqué. Des circonstances spécifiques peuvent faire partie d'une chaine d'évènements, d'occurrences, de moments et de lieux. De plus, la vengeance pornographique et les violations qui y sont associées, par le biais d'images sexuelles, peuvent être envisagées comme étant la nature processuelle du web interactif, dans lequel des « pro-utilisateurs», des « pro-consommateurs » et d'autres personnes avec un statut hybride créent le web de manière interactive, parfois pour des publics présumés mais inconnus (Whisnant, 2010), comme en témoigne la pornographie amateur, les selfies, les selfies de célébrités, les selfies nus, les médias de la réalité, les vies en ligne, les défis neknominate (boire cul-sec), et le reste.

Lutte contre la violation par la distribution d'images, la vengeance pornographique et les cyber-abus

La lutte contre les cyber-abus en général devrait englober des questions de politiques, de stratégies, de droit, d'éducation, d'intervention et de soutien. Par exemple, il n'existe pas de lois universelles pour condamner les auteurs de violations par distribution d'images et de vengeance pornographique. Dans de nombreux pays, les cadres juridiques criminels sont soit inexistants, soit il est très difficile d'obtenir des condamnations (Franks, 2016). En l'absence de lois internationales et transfrontalières, il sera probablement très difficile de poursuivre les auteurs de ces crimes et ceux qui en facilitent la commission (Topping, 2016). Beaucoup doit être fait pour arrêter les organisations qui hébergent de telles images sexuelles, ainsi que les moteurs de recherche qui renvoient vers des sites de vengeance pornographique. Nous pouvons soutenir que des lois civiles plus strictes devraient également être en place afin que les victimes puissent poursuivre les auteurs de ces actes pour obtenir des dommages-intérêts.

Il est également nécessaire de sensibiliser le public et la population aux risques potentiels de la vengeance pornographique, pouvant découler du sexting, par exemple (Hasinoff, 2015). A cet effet, l'une des méthodes consiste à l'inclure dans les programmes d'enseignement sur le sexe et les relations interpersonnelles. Les organismes de bienfaisance et les groupes éducatifs s'inquiètent du fait que de nombreux adolescents ne reçoivent pas d'enseignement sur des enjeux comme le « sexting », la pornographie en ligne, le consentement et les relations saines, y compris l'illégalité du sexting chez les mineurs, et la vengeance pornographique. Les programmes d'études sur le sexe et les relations ont tendance à mettre l'accent sur la sexualité et la santé, et sur ce qui constitue une relation saine ; mais cela devrait comprendre également la façon de communiquer en ligne, ainsi que la manière de faire face à la fin d'une relation, la résolution de problèmes et une formation sur les aptitudes relationnelles et la régulation des émotions (Lundgren et Amin, 2015).

De nombreux programmes d'aide aux victimes de crimes liés au genre et à la sexualité tendent à se concentrer sur les moyens de réduire le risque de revictimisation, tels que le soutien social et l'adoption de comportements sécuritaires. Toutefois, la plupart d'entre eux ont tendance à se concentrer sur le processus juridique de présentation des délinquants devant les tribunaux ou de retrait des images. Pourtant, il faut faire davantage pour aider les victimes à faire face aux retombées. Il serait donc utile que les protocoles de coopération entre les autorités compétentes et les services de soutien existants soient renforcés, afin de fournir une gamme de services de soutien émotionnel et pratique, et qu'une page Web soit créée pour la diffusion de matériel d'apprentissage et de soutien à l'intention des victimes, des éducateurs, des organismes et des médias.

La criminalisation de la distribution non consensuelle d'images sexuelles et plus particulièrement de la vengeance pornographique est susceptible d'avoir un effet dissuasif pour certains, mais pas pour d'autres. Lorsque la loi n'a pas cet effet dissuasif, les enquêteurs peuvent utiliser un logiciel, tel que « EnCase », pour produire une image du disque dur du présumé contrevenant, ce afin de voir les fichiers informatiques supprimés, comme les fichiers de cache, les fichiers d'échange, les fichiers temporaires, l'espace non alloué ou l'espace libre, et laisser des traces de l'historique de leur navigateur, les carnets d'adresses, la date et l'heure, et ainsi de suite, afin de les utiliser comme preuve admissible (Widup, 2014). Une fois condamné et puni, une intervention de rééducation peut être une voie possible offerte aux délinquants, qui sont majoritairement des hommes. Cela dit, il faut faire preuve d'une grande prudence quant au succès éventuel de telles interventions. Cela s'explique en partie par le fait que les méta-analyses des évaluations de ces types d'interventions pour mettre fin à la violence, dans d'autres contextes, notamment la « violence domestique » et la violence conjugale, montrent une efficacité mitigée (Wathen & MacMillan, 2003 ; Smedslund et al. 2007 ; Feder et al. 2008 ; Arias et al. 2013).

Dans la lutte contre ces diverses formes relativement récentes de violences en ligne et celles fondées sur l'image sexuelle, les principales leçons tirées des interventions menées sur des délinquants reconnus devraient être reprises, à l'image du traitement de groupe de rééducation féministe axé sur le pouvoir et le contrôle (en grande partie masculin) (Eckhardt et al., 2013). De telles approches pourraient être appliquées et modifiées dans le cadre de la prévention de la vengeance pornographique. Certaines méthodes assez bien établies ont été développées au sein d'ateliers et et campagnes anti-pornographie, comme les divers groupes «Men against pornography», qui peuvent être adaptées afin de travailler avec les délinquants, au sens le plus large du terme, contre la vengeance pornographique. Au-delà de ces interventions, il existe toute une gamme de méthodes et de techniques spécifiques pour travailler avec ceux qui ont commis des crimes de violence sexuelle.

Remarques conclusives

En résumé, afin de s'attaquer aux atteintes par distribution d'images sexuelles, et plus généralement aux cyber-abus, nous recommandons quatre réponses-clés pour enrayer ce phénomène contemporain. Premièrement, il devrait y avoir des lois civiles plus strictes en place afin que les victimes puissent poursuivre les auteurs de ces actes en dommages-intérêts. Deuxièmement, nous avons besoin d'une plus grande coopération internationale. Cela signifie une coopération entre les États pour faciliter les poursuites transfrontalières et le démantèlement des sites Web où les images sont publiées ; soit ceux qui profitent de ce crime. La troisième réponse est axée sur le soutien. À l'heure actuelle, l'accent est mis sur la comparution des délinquants devant les tribunaux ou le retrait des images, mais il faut faire davantage pour soutenir les victimes et, en particulier, la manière de gérer les retombées de ces crimes. Enfin, les programmes éducatifs dans les écoles et ailleurs doivent être adaptés pour mettre en évidence les risques et les conséquences potentielles de la prise et de l'envoi d'images. Ce problème ne disparaîtra pas. Ce n'est que par des réponses multidisciplinaires davantage orientées vers l'action que nous pouvons contribuer à éliminer la stigmatisation et le traumatisme que ce type de crime cause (Hall & Hearn, 2017).

Notes

16 Synoptique : permet d'avoir une vision complète d'un seul coup d'œil / Panoptique : permet de voir sans être vu.

17 L'étiologie est l'étude des causes de la délinquance. Ces causes peuvent être d'ordre individuel, situationnel ou contextuel.

18 Voir partie précédente concernant la théorie économique.

19 Concept de psychologie sociale inspirée par la psychologie des foules de LeBon (1895) et appliquée par Zimbardo (1973) dans sa célèbre expérience de la prison de Stanford.

20 « Yahoo Boys » : les fraudeurs nigérians sont prénommés ainsi d'après la célèbre société Internet Yahoo! Ces derniers utilisent souvent leurs comptes de messagerie gratuits pour commettre leurs fraudes.

21 Une interaction hostile en ligne entre des personnes impliquant des propos grossiers.

22 Un groupe de personnes qui filme ou prend des photos de leur agression sur une personne et la diffuse en ligne.

23 L'utilisation de la technologie pour combiner ou superposer une image ou une vidéo d'une personne sur l'image ou la vidéo d'une autre personne pour donner l'impression qu'il s'agit de cette personne.

Références

Chapitre 3 : Cybercrimes, cyberdélinquants et cybervictimes

Adeniran, A.I, (2008). The internet and emergence of yahoo-boys sub-Culture in Nigeria. International Journal of Cyber Criminology (IJCC), 2(2): 368-381. ISSN: 0974 – 2891

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, N. (2011). Dealing with the Problem of Cybercrime. Dans I. Baggili (Éd.), Digital Forensics and Cyber Crime (Vol. 53, p. 1-18). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-19513-6_1

Behm-Morawitz, E., et Schipper, S. (2016). Sexing the avatar: gender, sexualization, and cyber-harassment in a virtual world. Journal of Media Psychology, 28(4), 161-174.

Beran, T, et Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. Journal of Educational Computing Research, 32(3), pp. 265 – 277 https://doi.org/10.2190/8YQM-B04H-PG4D-BLLH

Bernier, P. A. (2016). L'utilisation des TIC à des fins de harcèlement criminel en situation de violence conjugale : la théorie des opportunités et des activités routinières de Cohen et Felson (1978) remaniée, 89.

Blaya, C. (2011). Cyberviolence et cyberharcèlement : approches sociologiques. La nouvelle revue de l'adaptation et de la scolarisation, 53(1), 47. https://doi.org/10.3917/nras.053.0047

Bourque, S. (2012). La cyberintimidation: comprendre le phénomène. Les cahiers de PV, 8, 60-63.

Brenner, S. W. (2001). Is there such a thing as 'virtual crime'? California Criminal Law Review, 4(1), 1-72. DOI: 10.15779/Z38MC94

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55-119.

Burgard, A., & Schlembach, C. (2013). Frames of fraud: A qualitative analysis of the structure and process of victimization on the internet, 7(2), 112-124.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408. https://doi.org/10.1177/0004865814521224

Cappadocia, M. C., Craig, W. M., & Pepler, D. (2013). Cyberbullying: prevalence, stability, and risk factors during adolescence. Canadian Journal of School Psychology, 28(2), 171-192. https://doi.org/10.1177/0829573513491212

Carignan, M. (2015). L`origine géographique en tant que facteurs explicatif de la cyberdélinquance (mémoire). Récupéré par https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12549/Carignan_Mira_2015_memoire.pdf.

Cohen, S. (2002). Folk Devils and Moral Panics: Creation of Mods and Rockers. London, UK: Routledge ISBN : 0415267129, 9780415267120

Cohen, L.E. et Felson, M. (1979). Social change and crime rate changes: a routine activity approach. American Sociological Review, 44(4), 588-608.

Cusson, M. (2017). La criminologie (7e éd.). Vanves, FRA : Hachette Éducation.

Décary-Hétu, D. (2013). Piratage informatique. Dans Cybercriminalité: Entre inconduite et crime organisé (183–210). Montréal, QC : Presses internationale Polytrechnique.

Diamond, B., & Bachmann, M. (2015). Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology. International Journal of Cyber Criminology 9(1), 24-34. https://doi.org/10.5281/zenodo.22196

Dupont, Benoit. (2012a). L'environnement de la cybersécurité à l'horizon 2022 : Tendances, moteurs et implications. Ottawa: Sécurité Publique Canada–Direction Nationale de la Cybersécurité.

Dupont, Benoit. (2012b). Nouvelles technologies et crime désorganisé : incursion au cœur d'un réseau de pirates informatiques. Sécurité et stratégie, 11(4), 25. https://doi.org/10.3917/sestr.011.0025

Franks, M.A. (2010). The banality of cyber discrimination or the eternal recurrence of September. Denver Law Review Online, 87, 1-6.

Frau-Meigs, D. (2010). La panique médiatique entre déviance et problème social : vers une modélisation sociocognitive du risque. Questions de communication, (17), 223-252. https://doi.org/10.4000/questionsdecommunication.387

Fried, R. (2001) Cyber scam artists: A new kind of .con. SANS Institute InfoSec Reading Room. Récupéré de https://www.sans.org/reading-room/whitepapers/threats/cyber-scam-artists-kind-con-482

Furnell, S. M. (2001) The Problem of Categorising Cybercrime and Cybercriminals. Proceedings of the 2nd Australian Information Warfare and Security Conference.

Furnell, S. M. (2004). Hacking begins at home: Are company networks at risk from home computers? Computer Fraud and Security, 2004(1), 4-7. DOI: 10.1016/S1361-3723(04)00016-8

Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. International Journal of Law and Information Technology, 10(2), 139-223. https://doi.org/10.1093/ijlit/10.2.139

Gottfredson, M. et Hirschi, T. (1990). A general theory of crime, Stanford, Stanford University Press.

Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? Social & Legal Studies, 10(2), 243-249. https://doi.org/10.1177/a017405

Grabosky, Peter, Russell G. Smith, and Gillian Dempsey (2001). Electronic Theft: Unlawful Acquisition in Cyberspace, Cambridge, Cambridge University Press Cambridge.

Higgins, G. E., & Makin, D. A. (2004). Self-Control, Deviant Peers, and Software Piracy. Psychological Reports, 95, 921-931. https://doi.org/10.2466/pr0.95.3.921-931

Holt, Thomas J. (2007). Subcultural Evolution? Examining the Influence of On-and Off-Line Experiences on Deviant Subcultures. Deviant Behavior, 28, 171–198. DOI: 10.1080/01639620601131065

Holt, Thomas J. (2009). Lone Hacks or Group Cracks: Examining the Social Organization of Computer Hackers. Dans Frank Smalleger and Michael Pittaro (dir), Crimes of the Internet, edited par Upper Saddle River, Pearson Prentice Hall.

Holt, Thomas J. and Adam M. Bossler. (2009). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. Deviant Behavior, 30, 1–25. DOI: 10.1080/01639620701876577

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. Journal of Contemporary Criminal Justice, 29(4), 420–436.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. Deviant Behavior, (35), 20-40. https://doi.org/10.1080/01639625.2013.822209

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. International Journal of Cyber Criminology, 6(1), 13.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. International Journal of Cyber Criminology, 1(2), 3. ISSN: 0974 – 2891

Jaishankar, K. (2008), Space transition theory of cyber crimes. Dans Schmalleger, F., & Pittaro, M. (eds), Crimes of the Internet (pp.283-301). Upper Saddle River, US: Prentice Hall. ISSN: 0974 – 2891

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. International Journal of Cyber Criminology, 10(1), 79-91. https://doi.org/10.5281/zenodo.58523

Jaquith, S.M (1981), Adolescent marijuana and alcohol use: An empirical test of differential association theory. Criminology, 19(2), p.271-280. DOI: 10.1111/j.1745-9125.1981.tb00416.x

Kerstens, J. et Veenstra, S. (2015), Cyber bullying in the Netherlands: A criminological perspective. International Journal of Cyber Criminology, 9(2), 144-161. DOI: 10.5281/zenodo.55055

Kerstens, J., Veenstra, S. (2016). Cyber bullying in the Netherlands: A criminological perspective. International Journal of Cyber Criminology, 9(2), 144-161. https://doi.org/10.5281/zenodo.55055

Koops, B.-J. (2010). The internet and its opportunities for cybercrime. Transnational Criminology Manual, 1, 735-754.

Koops, B.-J., & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime: Definitions matter. Datenschutz Und Datensicherheit - DuD, 30(9), 553-556. https://doi.org/10.1007/s11623-006-0141-2

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Science, 3(1), 1-10, https://doi.org/10.1186/s40163-014-0009-y

Leeson, P. T., & Coyne, C. J. (2014). Une analyse économique du piratage informatique. Tracés. Revue de Sciences humaines, (26), 203-231.

Leman-Langlois, S. (2006). Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial. Criminologie, 39(1), 63. https://doi.org/10.7202/013126ar

Leman-Langlois, S. (2007). La sociocriminologie, Montréal, Les Presses de l'Université de Montréal.

Lusthaus, J. (2013), How organized is organized cybercrime? Global Crime, 14(1): 52–60. DOI : 10.1080/17440572.2012.759508

Miller, C. (2006). Cyber harassment: Its forms and perpetrators. Law Enforcement Technology, 33(4), 26-30.

Mishna, F., Wiener, J., & Pepler, D. (2008). Experiences of bullying in friendship. School Psychology International, 29(5), 549-573. DOI: 10.1177/0143034308099201

Ouimet, M. (2009). Facteurs criminogènes et théories de la délinquance. Les Presses de l'Université Laval, Québec.

Ngo, F., & Jaishankar, K. (2017). Commemorating a decade in existence of the international journal of cyber criminology: A research agenda to advance the scholarship on cyber crime. International Journal of Cyber Criminology, 11(1), 1–9.

Ngo, F.T. & Paternoster, R. (2011), Cybercrime Victimization: An examination of Individual and Situational level factors. International Journal of Cyber Criminology (IJCC), 5(1): 773–793. ISSN: 0974 – 2891

Peretti-Watel, P. (2010). La Société du Risque. Paris, FRA : La Découverte. ISBN : 978-2707164568

Pontell, H. N., & Rosoff, S. M. (2009). White-collar delinquency. Crime, Law and Social Change, 51, 147–162. DOI:10.1007/s10611-008-9146-0

Prates, F., Gaudreau, F., & Dupont, B. (2013). La cybercriminalité: état des lieux et perspectives d'avenir. Dans Institut Canadien d'Études Juridiques Supérieures (415-442). Cowansville, QC: Éditions Yvon Blais

Pratt, T. C. and Cullen, F. T. (2000), The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. Criminology, 38(3), 931–964. DOI : 10.1111/j.1745-9125.2000.tb00911.x

Quémener, M. et Ferry, J. (2009). Cybercriminalité : défi mondial, 2e édition, Paris, Economica, Bryant, R. et Bryant, S. (2014). Policing Digital Crime, Ashgate Publishing.

Reyns, B.W., Henson, B. et Fisher, B.S. (2011). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. Deviant Behavior, 33(1), 1-25. DOI: 10.1080/01639625.2010.538364

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency, 50(2), 216-238. https://doi.org/10.1177/0022427811425539

Rogers, M. K. (1999). Psychology of Hackers: Steps Toward a New Taxonomy. Repéré à http:// homes.cerias.purdue.edu/mkr/hacker.doc.

Rogers, M. K. (2006). A Two-Dimensional Circumplex Approach To The Development of a Hacker Taxonomy. Digital Investigation. 3(2), 97-102. Repéré à https://doi.org/10.1016/j.diin.2006.03.001

Rowan, T. (2009). Password Protection: The Next Generation. Network Security, vol. 2, 4-7. Repéré à https://doi.org/10.1016/S1353-4858(09)70015-7

Ryan, N., Lavoie, P.E., Dupont, B. et Fortin, F., (2011), La fraude via les médias sociaux, Note de recherche n.13, Chaire de recherche du Canada en sécurité, identité et technologie.

Sandywell, B. (2010). On the globalisation of crime: the Internet and new criminality, dans Jewkes, Y. et Yar, M. (2010), Cullompton: William Publishing, pp.38-66

Shariff, S. (2009). Confronting Cyber-Bullying. Cambridge, UK: Cambridge University Press.

Simion, R. (2009). Cybercrime and its challenges between reality and fiction. Where do we actually stand? Rivista di Criminologia, 3(2), 296-312.

Smith, P.K, Mahdavi, J., Carvalho, M., Fisher, S, Russel, S. & Tippet, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. The Journal of child psychology and psychiatry, 49(4), 376-395. DOI: 10.1111/j.1469-7610.2007.01846.x

Sterling, B. (1994). The Hacker Crackdown, London, UK: Penguin Books. ISBN: 0-553-56370-X

Suler, J. (2004), The online disinhibition effect. Cyber psychology & behaviour: The impact of the internet, multimedia and virtual reality on behaviour and society, 7 (3): 321–326 https://doi.org/10.1089/1094931041291295

Sutherland, E.H. (1947), Principles of Criminology, (4ème éd), Philadelphia, US: Lippincott.

Sykes, G. et Matza, D. (1957). Techniques of neutralization: A theory of delinquency. American Sociological Review, 22, 664-670.

Tade, O., & Aliyu, A. (2011). Social Organization of Internet Fraud among University Undergraduates in Nigeria. International Journal of Cyber Criminology, 5(2), 860-875.

Taylor, P. (1999). Hackers: Crime in the Digital Sublime, London, UK: Routledge. ISBN-13: 978-0415180726, ISBN-10: 0415180724

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. Computers in Human Behavior, 26(3), 277-287. https://doi.org/10.1016/j.chb.2009.11.014

van Wilsem, J. (2013). Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. European Sociological Review, 29(2), 168-178. https://doi.org/10.1093/esr/jcr053

Wade, A., & Beran, T. (2011). Cyberbullying: The new era of bullying. Canadian Journal of School Psychology, 26(1), 44-61. https://doi.org/10.1177/0829573510396318

Wall, D. S. (1998). The Chief Constables of England and Wales: The socio-legal history of a criminal justice elite, Aldershot: Dartmouth.

Wall, David S. (2001). Cybercrimes and the Internet. Journal of Research in Crime and Delinquency, 47(3), 267-296. DOI : 10.1177/0022427810365903

Wall, D. S. (2005). The Internet as a conduit for criminals. In Pattavina, A. (éd), Information Technology and the Criminal Justice System (77-98). Thousand Oaks, CA: Sage.

Wall, D. S. (2007). Cybercrime. The transformation of crime in the information age. Cambridge, UK: Polity Books.

Warschauer, M. (2004). Technology and social inclusion: rethinking the digital divide. Cambridge, US: MIT Press.

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J.-L. (2017).

Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. Deviant Behavior, 1-16. https://doi.org/10.1080/01639625.2017.1411030

Welsh, A., & Lavoie, J. (2012). Risky ebusiness: An examination of risk-taking, online disclosiveness, and cyberstalking victimization. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6(1), article 4. http://dx.doi.org/10.5817/CP2012-1-4

Willard, N. E. (2005, August 15). Cyberbullying and cyberthreats. Paper presented at the 2005 OSDFS National Conference, Washington, DC (21-31).

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. European Journal of Criminology, 2(4), 407-427. https://doi.org/10.1177/147737080556056

Yar, M. (2006). Cybercrime and Society (1st ed.). Thousand Oaks, CA: SAGE Publications. http://dx.doi.org/10.4135/9781446212196

Ybarra, M. L., & Mitchell, K. J. (2004). Youth engaging in online harassment: associations with caregiver–child relationships, internet use, and personal characteristics. Journal of Adolescence, 27(3), 319-336. https://doi.org/10.1016/j.adolescence.2004.03.007

Zimbardo, P. G. (1969). The human choice: individuation, reason and order vs. deindividuation, impulse and chaos. Nebraska Symposium on Motivation, 17, 237-307.

Contributions

La cyber-criminologie et la théorie de la transition spatiale

Bachmann, M. (2008). What makes them Click? Applying the rational choice perspective to the hacking underground. Doctoral Dissertation Submitted to the University of Central Florida. Retrieved from http://etd.fcla.edu/CF/CFE0002258/Bachmann_Michael_200807_PhD.pdf.

Choi, K. S. (2015). Cybercriminology and Digital Investigation. El Paso, Texas: LFB Scholarly Publishing LLC.

Danquah, P., & Longe, O. (2011). An empirical test of the space transition theory of cyber criminality: Investigating cyber crime causation factors in Ghana. African Journal of Computing & ICT, 2(1), 37-48.

Diamond, A., & Bachmann, M. (2015). Out of the beta phase: Obstacles, challenges, and promising paths in the study of cyber criminology. International Journal of Cyber Criminology, 9, 24-34.

França, L. A. (2018). Cyber-Criminologies. In P. Carlen and L. A. França, (Eds.), Alternative Criminologies. Abington, Oxford, UK: Routledge.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cyber crime scholarship. Deviant Behavior, 35, 20–40. doi:10.1080/01639625.2013.822209

Holt, T., & Bossler, A. M. (2016). Cyber crime in Progress: Theory and Prevention of Technology-enabled Offenses. Abingdon, Oxon: Routledge.

Holt, T., Bossler, A. M., & Spellar, S. K. (2015). Cyber crime and Digital Forensics. Abingdon, Oxon: Routledge.

Jaishankar K., (2008). Space transition theory of cyber crimes. In F. Schmallager and M. Pittaro (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

Jaishankar, K. (2007a). Cyber criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, 1(1), 1–6.

Jaishankar, K. (2007b). Establishing a theory of cyber crimes. International Journal of Cyber Criminology, 1(2), 7-9.

Jaishankar, K. (2010). The Future of Cyber Criminology: Challenges and Opportunities. International Journal of Cyber Criminology, 4(1&2), 26–31.

Jaishankar, K. (2011). Introduction / Conclusion. In K. Jaishankar (Ed.), Cyber criminology: Exploring Internet crimes and criminal behavior (pp. xxvii–xxxv and pp. 411-414). Boca Raton, FL: CRC Press.

Jaishankar (2017). Cyber Criminology: Evolution, Contribution and Impact. Module 2, e-Pathsala, University Grants Commission. Retrieved from http://epgp.inflibnet.ac.in/ahl.php?csrno=1608.

Jaishankar, K., & Chandra, R.R. (2017). Space Transition Theory of Cyber Crimes. Module 23, e-Pathsala, University Grants Commission. Retrieved from http://epgp.inflibnet.ac.in/ahl.php?csrno=1608.

Kethineni, S., Cao, Y., & Dodge, C. (2017). Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. American Journal of Criminal Justice. doi:10.1007/s12103-017-9394-6.

Kshetri, N. (2013). Cybercrime and cybersecurity in the global south. New York, NY: Palgrave MacMillan Publishers.

Maras, M. H. (2016). Cybercriminology. Oxford: Oxford University Press.

Moore, R. (2012). Cyber crime: Investigating High-Technology Computer Crime. Abingdon, Oxon: Routledge.

Ngo, F., & Jaishankar, K. (2017). Special article: Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. International Journal of Cyber Criminology, 11(1),

1–9. http://doi.org/10.5281/zenodo.495762.

Nhan, J., & Bachmann, M. (2010). Developments in cyber criminology. In M. Maguire & D. Okada (Eds.), Critical issues in crime and justice: Thought, policy, and practice (pp. 164–183). Thousand Oaks, CA: Sage.

Wada, F., Longe, & O. Danquah (2012). Action Speaks Louder than Words-Understanding Cyber Criminal Behavior Using Criminological Theories. Journal of Internet Banking and Commerce, 17(1), 1.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Malden, MA: Polity Press.

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), 407-427DOI: 10.1177/147737080556056.

Zhang, X. H. (2009). An Exploration of Student Teachers' Interaction with on-line activities, and their influence on their teaching topics such as netiquette and cyber-bullying: An Australian and Chinese Study. Doctoral Thesis submitted to the Griffith University, Australia. Retrieved from https://www120.secure.griffith.edu.au/rch/file/cf7a4f3e-5132-1570-f88e-8efd334cf8d1/1/Zhang_2001_02Thesis.pdf.

Infraction de distribution d'images intimes

Arias, E., Arce, R., & Vilariño, M. (2013). Batterer intervention programmes: A meta-analytic review of effectiveness. Psychosocial Intervention, 22(2), 153-160.

Citron, D. K., & Franks, M. A. (2014). Criminalising revenge porn. Wake Forest Law Review, 2014(1), 345–391.

Feder L., Austin S., & Wilson, D. (2008). Court-mandated interventions for individuals convicted of domestic violence. Campbell Systematic Reviews, 12(4), 1–46.

Eckhardt, C. I., Murphy, C. M., Whitaker, D. J., Sprunger, J., Dykstra, R., & Woodard, K. (2013). The effectiveness of intervention programs for perpetrators and victims of intimate partner violence. Partner Abuse, 4(2), 196-231.

Franks, M.A. (2016). Drafting an effective "revenge porn" Law: A guide for legislators. Cyber Civil Rights Initiative: https://www.cybercivilrights.org/guide-to-legislation/

Gilbert, J. (2013). Materialities of text: Between the codex and the net. New

Formations: A Journal of Culture/Theory/Politics, 78(1), 5–6.

Hall, M. & Hearn, J. (2017). Revenge pornography: Gender, sexuality and motivations. London: Routledge.

Hasinoff, A. A. (2015). Sexting panic: Rethinking criminalization, privacy, and consent. Champaign, IL: University of Illinois Press.

Hearn, J., & Parkin, W. (2001). Gender, sexuality and violence in organizations: The unspoken forces of organization violations. London: Sage.

Lacey, B. (2007). Social aggression: A study of internet harassment. Unpublished

Doctoral Dissertation, Long Island University.

Lundgren, R., & Amin, A. (2015). Addressing intimate partner violence and sexual violence among adolescents: emerging evidence of effectiveness. Journal of Adolescent Health, 56(1), S42-S50.

Match.com. (2012). More on sexting and texting from SIA 3. UpToDate. February 5. Retrieved February 15, 2016 from http://blog.match.com/2013/02/05/more-on-sexting-and-texting-from-sia-3

Penney, J. (2013). Deleting revenge porn. Policy Options Politiques. November. Retrieved August 21, 2015 from http://policyoptions.irpp.org/fr/issues/vive-montreal-libre/penney

Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in Human Behavior, 29(1), 26–32.

Smedslund, G., Dalsbø, T. K., Steiro, A., Winsvold, A., & Clench-Aas, J. (2007). Cognitive behavioural therapy for men who physically abuse their female partner (Review). Cochrane Database Systematic Review 3: CD006048.

Svoboda, E. (2014). Virtual assault. Scientific American Mind, 25(6), 46–53.

Topping, A. (2016). Facebook revenge pornography trial 'could open floodgates. The Guardian, October 9: https://www.theguardian.com/technology/2016/oct/09/facebook-revenge-pornography-case-could-open-floodgates

Tyler, M. (2016). All porn is revenge porn. Feminist Current, February 24: http://www.feministcurrent.com/2016/02/24/all-porn-is-revenge-porn/

Wathen, C. N., & MacMillan, H. L. (2003). Interventions for violence against women: scientific review. Journal of the American Medical Association, 289(5), 589–600.

Wellman, B. (2001). Physical space and cyberspace: the rise of personalized networking. International Journal of Urban and Regional Research, 25(2), 227–252.

Whisnant, R. (2010). From Jekyll to Hyde: The grooming of male pornography consumers. In K. Boyle (Ed.), Everyday pornography (pp. 114–133). London: Routledge.

Widup, S. (2014). Computer forensics and digital investigation with EnCase Forensic v7. McGraw-Hill Education Group.


PC Repair Utility
System Scan
scan & repair computer
Action Required
Scan Results
Unused file extension
Missing CLSID reference
Invalid registry key
Missing ProgID reference
Missing ProgID reference
Invalid registry key
Empty key

CHAPITRE 4

QUELLE PRÉVENTION POUR LA CYBERCRIMINALITÉ ?

Le cyberespace fait aujourd'hui l'objet d'une nouvelle discussion, tant théorique, que pratique, en matière de prévention de la criminalité. Plusieurs États utilisent les termes de cybersécurité et de cybercriminalité de façon interchangeable et dirigent leurs efforts vers la protection des infrastructures critiques de l'information, au détriment de la nécessaire réflexion entourant la prévention de la criminalité, dans le contexte du cyberespace. En commençant par bien différencier la cybersécurité et la cybercriminalité, tant au niveau conceptuel qu'opérationnel, ce quatrième chapitre a pour objectif de présenter les principales tendances en matière de prévention de la criminalité, les différentes mesures prises, dans l'objectif de prévenir certains des crimes les plus souvent cités dans les conventions internationales – soit la cyberintimidation, l'exploitation sexuelle des jeunes en ligne et la cyberfraude – ainsi que les difficultés à appliquer les théories classiques de prévention à la cybercriminalité.

Introduction

La prévention de la criminalité renvoie à la capacité d'appréhender les crimes avant qu'ils ne soient commis (Pelser, 2002). Autrement dit, la prévention réfère aux initiatives et aux stratégies cherchant à réduire les risques favorisant le développement de la criminalité (ONUDC, 2010). Comme nous l'avons vu dans le chapitre précèdent, il est encore difficile de bien cerner les facteurs de risque influant sur la cybercriminalité (Bossler & Holt, 2016). Ce manque de connaissances, accompagné de la quasi-absence de l'État dans le développement d'initiatives de prévention, provoque une abondance des opportunités criminelles et rend les entreprises privées et notamment les citoyens largement responsables de leur propre sécurité, faisant du cyberespace un nouveau Far West (Ghernaouti, 2013; Kigler, 2016; Williams & Levi, 2017). Non seulement les réponses se font attendre, mais le monde virtuel rend la commission de certains actes criminels traditionnels plus simple en raison de l'utilisation généralisée d'internet, notamment dans l'économie légale, de la vitesse, de la portée potentielle et de la décentralisation des interactions (Rivière & Didier, 2008) (voir chapitre 2).

Pourtant, les Principes directeurs applicables à la prévention du crime de l'ONU, rappellent clairement qu'il « incombe aux pouvoirs publics, à tous les niveaux, de créer, gérer et favoriser les conditions permettant aux institutions publiques concernées et à tous les secteurs de la société civile, y compris le secteur privé, de mieux jouer leur rôle dans la prévention du crime » (ONUDC, 2010, p. 29). Bien que les stratégies en cybersécurité incluent des aspects propres au domaine de la prévention, nous postulons ici que ces interventions sont insuffisantes face à l'ampleur du phénomène. En effet, les stratégies en cybersécurité, aujourd'hui de plus en plus nombreuses, se concentrent largement sur la protection des infrastructures technologiques de l'information ou encore, sur la criminalité organisée (Seger, 2012), au détriment des initiatives dites préventives.

Afin de vérifier cette hypothèse, ce chapitre entreprendra tout d'abord de définir clairement les différences entre cybersécurité et cybercriminalité. Cette première partie est capitale à la compréhension des enjeux entourant la création d'une réelle stratégie en prévention de la cybercriminalité. Ensuite, nous réaliserons un survol des principales conventions et stratégies internationales et régionales, dans le but de dresser un portrait des enjeux – en termes de criminalité ciblée par ces stratégies – et des principales recommandations soulevées par les organisations internationales et régionales concernées, en matière de sécurité et de prévention dans le cyberespace. À partir des enjeux identifiés dans ce survol, nous réaliserons une courte revue des mesures de prévention évaluées les plus souvent citées dans la littérature. Sur la base de ces mesures, nous porterons notre regard sur l'applicabilité des théories classiques de la prévention de la criminalité dans le contexte du cyberespace. L'objectif de cet exercice d'analyse et de synthèse est de dresser un portrait de l'état de la prévention dans le contexte du cyberespace, tant opérationnelle, que théorique, afin d'envisager des pistes de réflexions et de recommandations pour l'établissement d'une réelle stratégie de prévention de la cybercriminalité.

Première partie : cybercriminalité et cybersécurité

Les deux derniers chapitres nous ont permis de souligner comment la démocratisation de l'usage d'Internet a considérablement altéré les comportements traditionnels en société, notamment dans la façon dont on recherche et/ou partage l'information, affectant ainsi nos activités quotidiennes et nos relations interpersonnelles (Lewis & Lewis, 2011). Non seulement ce nouvel espace a transformé les normes entourant les interactions humaines, mais il amène aussi son lot de nouveaux risques, notamment en matière de sécurité.

La notion de cybercriminalité

La Convention de Budapest (Conseil de l'Europe, 2001) est l'une des seules conventions internationales juridiquement contraignantes s'intéressant directement à la sécurisation du cyberespace et à la prévention de la cybercriminalité (Jamil, 2014). Cette dernière définit la cybercriminalité de deux façons :

1. Les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques, c'est-à-dire contre les données et systèmes informatiques, y compris l'accès illégal, l'interception illégale, l'interférence des données et du système et l'utilisation abusive des dispositifs;
2. Les infractions commises au moyen de systèmes informatiques. Cette liste est limitée aux formes dites « traditionnelles » de criminalité, se différenciant par l'utilisation d'un ordinateur, à savoir la contrefaçon et la fraude informatiques, la pédopornographie et les infractions liées à la propriété intellectuelle et aux autres droits connexes.

Le chapitre précédent nous a aussi permis de constater que la définition de cybercriminalité reste un débat important, et que nous sommes encore loin d'avoir atteint consensus au niveau international, quant à cette définition. Cependant, pour les fins de ce chapitre, nous allons utiliser une définition opérationnelle - ainsi, les cybercrimes seront « compris comme étant des offenses contre des systèmes informatiques, ou à l'aide d'ordinateurs, causant des dommages » (Traduction libre de Seger, 2012, p. 21) » physiques et/ou économiques.

Malgré la place donnée à la criminalité traditionnelle dans la définition du Conseil de l'Europe, une part importante de la recherche, des stratégies nationales et, comme nous le verrons, des initiatives internationales et régionales, s'intéresse plutôt à la sécurité des infrastructures technologiques de l'information, l'autorégulation des citoyens, les réponses légales et la répression policière, et ce, au détriment de mesures concrètes en matière de prévention de la cybercriminalité (Seger, 2012). Ceci nous amène tout d'abord à faire une distinction entre les approches en cyber sécurité et les approches abordant le sujet de la cybercriminalité.

Les cyberattaques de 2007, en Estonie, représentent une conjoncture historique en matière de sécurisation du cyberespace. Elles ont influencé, au niveau mondial, la mise en place de stratégies axées sur la sécurité. En effet, depuis 2007, la cybersécurité occupe une part grandissante des agendas politiques à travers le monde. Les risques associés aux cyberattaques multiples, tout comme leurs cibles, sont régulièrement soulevés. Les concepts de cybersécurité, cybercriminalité et cyberdéfense sont présentement « employés de manière interdépendante sans que des définitions précises aient été consacrées par le droit » (Pereira, 2016, p.388). Pourtant, les objectifs de ces deux approches sont fondamentalement distincts et par conséquent, ne peuvent entraîner les mêmes résultats.

Encadré 4.1. **Les cyberattaques en Estonie en 2007**

En 2007, l'Estonie a subi une vague de cyberattaques affectant de nombreux serveurs commerciaux et gouvernementaux, mettant ainsi en péril la confidentialité, l'intégrité et l'accessibilité des données conservées sur ces serveurs. Près de 11 ans plus tard, aucun État ou groupe non-étatique n'a revendiqué ces attaques. Subséquemment, cette vague de cyberattaques sans précédent aura donné lieu à la création de nombreuses stratégies en cybersécurité à travers le monde (Haataja, 2017).

Les approches visant la cybersécurité

Les approches visant la cybersécurité, que nous appellerons dans ce chapitre **stratégies en cybersécurité**, ont pour objectif d'assurer la confidentialité, l'intégrité et la disponibilité des infrastructures de technologie de l'information. Ces stratégies ne visent donc pas l'intégralité des crimes commis dans le cyberespace, mais plutôt les questions liées à la protection des données personnelles et privées (Seger, 2012) (voir chapitre précédent) et la réduction des risques liés aux attaques cybernétiques commises par d'autres États ou des groupes non étatiques, ciblant leurs infrastructures essentielles de technologie de l'information (IETI). Étant donné que les stratégies en cybersécurité priorisent la sécurité des infrastructures critiques de l'information, celles-ci donnent une plus grande importance aux partenariats public-privé (Seger, 2012) (voir chapitre suivant). Enfin, ces stratégies sont normalement gérées, tant dans les opérations que la mise en œuvre, par les institutions publiques de la Défense ou de la Sécurité nationale, en partenariat avec le Ministère de la Justice (Seger, 2012).

Les approches en prévention de la cybercriminalité

Les stratégies en cybercriminalité, quant à elle, s'intéressent plutôt à la prévention de la criminalité et à la justice criminelle. La différence entre les deux types de stratégies reproduit ainsi la différence entre les approches sécuritaires et celles de prévention dans le contexte criminologique[24]. La criminalité traditionnelle fait donc l'objet de ces stratégies, que nous appellerons des **stratégies de prévention de la cybercriminalité[25].** Comme nous l'avons vu dans notre revue des initiatives, une part importante des mesures visant à prévenir la cybercriminalité reste dans le domaine des programmes de sensibilisation, des partenariats public-privé, de la coopération internationale et des approches dissuasives, consistant à appliquer des mesures punitives de plus en plus sévères (UIT, 2014). Bien que les mesures punitives ne mettent pas l'accent sur la prévention, mais la sanction (UIT, 2014), et qu'une part importante des incidents en cybercriminalité ne donnent pas lieu à des condamnations criminelles (Broadhurst, 2005), le consensus entourant les mesures préventives les plus appropriées dans le contexte du cyberespace reste encore très faible (Broadhurst, 2005). Ces mesures peuvent aller des solutions techniques, tels que les logiciels antivirus, au blocage de l'accès à des contenus illégaux (UIT, 2014).

Tableau 4.1. **La différence entre les stratégies de cybersécurité et celles associées à la cybercriminalité**

Stratégies en cybersécurité *Intérêts et sécurité nationale, confiance, résilience, fiabilité des technologies de l'information*		**Stratégies en cybercriminalité** *État de droit, droits humains, prévention de la criminalité et justice criminelle*	
Incidents de sécurité non-intentionnels	Attaques intentionnelles contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données	Infractions commises à l'aide d'un ordinateur et au contenu	Toute infraction impliquant des preuves électroniques

Source : Seger (2011)

Deuxième partie : les tendances en matière de prévention de la cybercriminalité

Dans cette partie, nous allons présenter les principales mesures mises en place pour prévenir la cybercriminalité en mettant l'accent sur les initiatives internationales, régionales ainsi que sur les programmes spécifiques de prévention.

Initiatives à l'échelle internationale

Lors du **12ème Congrès des Nations Unies pour la prévention de la criminalité et la justice pénale**, deux constats ont été fortement soulignés par les participants, soit l'importance des dommages économiques et humains causés par la commission d'actes criminels à l'aide des nouvelles technologies et la nature transfrontalière de cette criminalité. Afin de répondre à ces enjeux, deux recommandations ont été formulées; 1) la sensibilisation du public et la réaffirmation du rôle de l'école, ainsi que; 2) la coopération des instances répressives et pénales, au niveau international.

1. En effet, le **rôle des écoles** et des **campagnes de sensibilisation** a été soulevé comme étant des mesures peu coûteuses, permettant à la fois de traiter des enjeux de prévention et de justice pénale auprès des jeunes, notamment en ce qui a trait aux enjeux de la **cyberintimidation** et de sensibilisation de la population aux risques associés à l'utilisation des nouvelles technologies (CCPCJ, 2010).
2. D'autre part, plusieurs participants ont aussi soulevé l'importance de développer une plus grande **coopération internationale** pour lutter contre la cybercriminalité, notamment entre les **instances répressives et de justice pénale**. D'autres participants ont, quant à eux, soulevé l'importance de développer des partenariats avec le **secteur privé**, accompagné d'un plan d'action global pour le renforcement des capacités techniques en matière de prévention, de détection, d'investigation et de poursuite pénale des cyberdélinquants (CCPCJ, 2010).

Dans le même ordre d'idée, l'enquête de la **Commission pour la prévention de la criminalité et la justice pénale (CCJPC)** sur la problématique de la cybercriminalité et les réponses des États membres, de la communauté internationale et du secteur privé (2013), indique que la prévention de la cybercriminalité devrait impérativement passer par : a) la promulgation de lois pour réguler la problématique et encadrer les interventions; b) un leadership efficace; c) le développement et/ou le renforcement des capacités de la justice pénale et des forces de l'ordre; d) la sensibilisation du public et le renforcement du rôle de l'éducation dans la prévention; e) le développement d'une base de connaissances solide entourant les enjeux de la cybercriminalité; f) ainsi qu'une coopération accrue entre les gouvernements, les communautés, le secteur privé et l'international (ONUDC, 2013). Toujours selon l'enquête de la Commission, près de 70% des stratégies nationales rapportées indiquaient que la sensibilisation du public, la coopération internationale et le renforcement des capacités des forces de l'ordre étaient des composantes phares (ONUDC, 2013). Finalement, la commission souligne que

la sécurité des **jeunes**, des i**nfrastructures essentielles de technologie de l'information** (IETI) et des **données personnelles** étaient souvent au centre des préoccupations de ces stratégies (ONUDC, 2013).

La **Déclaration de Doha** (2015) appelle elle aussi au développement de mesures spéciales pour la prévention de certains crimes commis dans le cyberespace, tel que l'**exploitation en ligne des enfants**, notamment pour « identifier et protéger les victimes en retirant, entre autres, d'Internet tout matériel pornographique mettant en scène des enfants, en particulier toute image de maltraitance sexuelle d'enfants » (ONUDC, 2015). Pour atteindre cet objectif, la déclaration recommande le renforcement de la **coopération entre les instances répressives**, tant au niveau national, qu'international, ainsi qu'au **renforcement des capacités techniques** de ces mêmes acteurs (ONUDC, 2015). Comme nous l'avons vu dans le premier chapitre, la Déclaration de Doha va beaucoup plus loin que les enjeux propres au cyberespace. Sans nous y attarder trop longuement, nous tenons à indiquer que même si les recommandations de la déclaration ne s'intéressent pas toutes aux enjeux du cyberespace, cela ne veut pas dire qu'elles ne sont pas pertinentes à notre propos, nous verrons pourquoi plus tard.

Les récentes déclarations et rapports produits par les États membres et des groupes d'experts mandatés par l'ONU (CCPCJ, 2010 ; ONUDC, 2013, 2015) indiquent que la communauté internationale entend prévenir la cybercriminalité – principalement la cyberintimidation, l'exploitation sexuelle des enfants en ligne, la protection des IETI et des données personnelles – à l'aide de campagnes de sensibilisation, d'éducation, de partenariats avec le secteur privé, de coopération internationale entre les instances des forces de l'ordre et de la justice pénale et le renforcement des capacités, de ces mêmes acteurs. Afin d'approfondir notre compréhension du rôle que les États entendent jouer en matière de prévention de la cybercriminalité, notre revue des initiatives s'intéressera maintenant aux positions prises au niveau régional.

Autrement dit, nous nous intéresserons aux objectifs ciblés par les différentes déclarations/conventions/stratégies régionales en matière de prévention de la cybercriminalité.

Les initiatives régionales

Comme nous venons de le voir, la Convention de Budapest (Conseil de l'Europe, 2001) ou la Convention sur la cybercriminalité du Conseil de l'Europe, est le seul instrument international contraignant, en matière de cybercriminalité. Cette convention est aussi considérée comme un texte fondateur, sur lequel de nombreux pays se sont basés pour réaliser leurs propres stratégies nationales. Son objectif principal est de favoriser l'**harmonisation des cadres juridiques** nationaux autour de définitions légales visant à protéger la population contre la cybercriminalité et de développer la **coopération entre les pays**, à des fins d'investigation et de poursuites judiciaires, notamment au travers du partage de données criminelles pertinentes aux enquêtes (Conseil de l'Europe, 2001). Renforcée, en 2004, par le Protocole sur les actes xénophobes et racistes commis à l'aide d'un système informatique, la Convention traite principalement la **cyberfraude**, l'**exploitation sexuelle des jeunes en ligne**, les **cybercrimes haineux**, les **infractions à la propriété intellectuelle** et la **sécurité des réseaux informatiques** (Conseil de l'Europe, 2001, 2004).

En 2004, à Buenos Aires, les États membres de l'Organisation des États Américains ont, pour la première fois, communément reconnu l'ampleur des enjeux et menaces auxquels font face les infrastructures essentielles de technologie de l'information dans leurs pays respectifs et l'importance d'une action commune, faisant l'objet d'une coopération intersectorielle et internationale entre leurs différents gouvernements. Cette reconnaissance donna lieu à la création de la **Stratégie de sécurité cybernétique (2004 – Estrategia de Seguridad Cibernética)**, dans laquelle les États membres se sont entendus pour développer :

> « (…) une culture de cybersécurité dans les Amériques en adoptant des mesures de prévention efficaces pour prévoir, traiter et répondre aux cyberattaques, quelle que soit leur origine, en luttant contre les cybermenaces et la cybercriminalité, en caractérisant les attaques contre le cyberespace, en protégeant les infrastructures essentielles et en sécurisant les réseaux de systèmes informatiques. » (OEA, 2004, p.6). »

Pour ce faire, la déclaration commune (2003) encourage les États membres (OEA, 2004) :

a) à développer des partenariats public-privé dans le but d'accroître l'éducation et la sensibilisation du public ;

b) à identifier et évaluer les normes et les meilleures pratiques en matière de sécurité des infrastructures essentielles des technologies de l'information (IETI) ;

c) à promouvoir l'adoption de politiques et de lois visant à protéger les utilisateurs d'Internet et à décourager l'utilisation des réseaux informatiques à des fins illégales ;

d) et à la création d'équipes de réaction d'urgence informatique (CERT : Computer Emergency Response Teams) pour répondre rapidement aux incidents.

Le **Secrétariat du Commonwealth** encourage les États membres du Commonwealth à développer des réponses visant la sécurisation des IETI, la prévention, l'investigation et la poursuite pénale des cyberdélinquants. Le Secrétariat recommande aussi le développement de partenariats entre les secteurs public et privé, ainsi qu'entre les autres gouvernements du Commonwealth, notamment pour le renforcement des capacités et pour les meilleures pratiques entourant les poursuites et les investigations transfrontalières. Le Secrétariat recommande aussi le développement de stratégies nationales qui incluront des mesures spécifiques de prévention de la cybercriminalité, de sensibilisation grand public, de coordination entre les différentes agences gouvernementales, d'allocation de ressources

appropriées dans le domaine de la justice pénale, de la création de CERT nationaux et/ou régionaux, ainsi que de mécanismes et de protocoles pour la coopération avec les fournisseurs de service Internet et le secteur privé dans son ensemble. Enfin, une attention particulière est donnée à la coopération avec la société civile et le secteur privé pour développer des programmes de formations visant le renforcement des capacités techniques (Commonwealth Secretariat, 2014).

Consciente du manque de ressources (techniques et humaines) et d'harmonisation des cadres légaux en matière de cybercriminalité, la Communauté caribéenne a intégré dans sa Stratégie de sécurité et de lutte à la criminalité **(CCSS - 2013 – CARICOM Crime and Security Strategy)** une série de recommandations à l'attention de ses États membres concernant le phénomène de la cybercriminalité. Parmi celles-ci on retrouve aussi la création de CERT, le développement de campagnes de sensibilisation et de matériel éducatif concernant l'usage d'Internet, le renforcement des capacités des policiers, des juges, des procureurs et des intervenants du secteur médico-légal, ainsi que la création d'un centre régional et d'une unité spécialisée pour lutter contre la cybercriminalité et le développement de partenariats et de programmes avec le secteur privé (CARICOM, 2013).

Encadré 4.2. **Enjeux pour les petits États**

Dans son rapport, le Secrétariat du Commonwealth souligne que les petits pays sont moins susceptibles d'avoir l'expertise technique et politique permettant de développer des réponses efficaces et durables pour lutter contre la cybercriminalité. En effet, ces petits États font souvent face à un manque criant de ressources humaines qualifiées, tant au niveau administratif, académique, que privé, ainsi qu'à des infrastructures limitées. Ce faisant, les défis pour développer des initiatives de prévention sont multiples et nécessitent donc d'être répondus au travers d'une coopération internationale et/ou régionale plus accrue avec les États ayant la capacité technique et scientifique nécessaire (Commonwealth Secretariat, 2014).

La **Convention de l'Union africaine sur la cybersécurité et la protection de données à caractère personnel (2014)** appelle les États membres de l'Union à développer des stratégies nationales incluant des mesures permettant : a) la sensibilisation du public ; b) le développement des capacités ; c) la création de partenariats public-privé et internationaux ; d) ainsi que des mesures visant à limiter la cybercriminalité et favoriser la coopération en matière d'investigation, de poursuite et de justice réparatrice (Union africaine, 2014). La Convention engage aussi les États membres à promouvoir la culture de la sécurité chez toutes les parties prenantes – gouvernementales, entreprises privées et société civile – en mettant l'accent sur la sécurisation des infrastructures essentielles de technologies de l'information (IETI), les campagnes de sensibilisation auprès des petites entreprises, des écoles et des enfants, pour développer des comportements sécuritaires. En ce qui a trait au partage de l'information, la Convention suggère aux États membres la mise en œuvre de CERT ou de réaction aux incidents de sécurité informatique (CSIRTS : Computer Security Incident Response Teams).

Dans son rapport de Recommandations sur la cybersécurité et la lutte à la cybercriminalité au Moyen-Orient (2015), la **Commission économique et sociale pour l'Asie occidentale (CESAO)**, encourage les États de la région à développer des mesures de sensibilisation du grand public, la création d'instituts spécialisés, l'offre de cours techniques pour le renforcement des capacités des juges, des enquêteurs, des policiers et autres forces de l'ordre. La Commission reconnaît aussi l'importance de renforcer les coopérations régionales et internationales, et de mettre en œuvre des CERT pour protéger les IETI. Finalement, la Commission recommande aussi le développement de partenariats avec la société civile et le secteur privé, notamment pour le partage d'informations et des coûts financiers et le développement de solutions techniques (ESCWA, 2015).

La Déclaration de l'**Association des nations de l'Asie du Sud-Est (ASEAN) pour la prévention et la lutte contre la cybercriminalité (2017)**, quant à elle, vise en premier lieu l'harmonisation des cadres juridiques et de la collecte des éléments de preuves. La Déclaration appelle aussi les États membres à développer leurs propres plans d'action nationaux et à coopérer entre eux pour l'échange d'expertise technique, d'information, de bonnes pratiques et de renforcement des capacités techniques des intervenants du milieu de l'éducation et des secteurs administratifs du gouvernement. En dernier lieu, la Déclaration recommande aussi le développement de programmes d'éducation et de sensibilisation des communautés quant aux risques du cyberespace (ASEAN, 2017).

Comme nous venons de le voir, les **campagnes de sensibilisation** semblent être l'un des outils de prévention les plus utilisés par les États, et ce, malgré les connaissances limitées que nous avons entourant leur impact réel (Williams & Levi, 2017). On constate aussi la place importante accordée au développement de **partenariats public-privé**, au niveau national, et entre les **instances de répression**, au niveau international. Autre constat, la place accordée à l'harmonisation des cadres légaux et au développement des capacités techniques, principalement pour la détection, l'investigation et les poursuites pénales. À cet égard, l'Union Internationale des Télécommunications (UIT) indique qu'une part importante des initiatives, mises de l'avant dans les stratégies nationales, se bornent au domaine des approches dissuasives, consistant à appliquer des mesures, d'une part, punitives et de plus en plus sévères (UIT, 2014) ainsi que, d'autre part, des mesures visant la réduction des opportunités (Reyns, Randa, & Henson, 2016). Enfin, le rôle que peut jouer les **CERT** est aussi mis de l'avant dans la plupart des recommandations, au niveau régional.

Prévention de la cyberintimidation, de l'exploitation sexuelle des jeunes en ligne et de la cyberfraude

Dans cette partie, nous allons aborder des mesures spécifiques concernant la prévention de la cybercriminalité, notamment celles contre les personnes. Dans le chapitre précédent, nous avons spécifiquement mentionné trois types de cybercrimes : le piratage informatique, la cyberfraude et la cyberviolence. Cependant, en raison du fait que nous avons choisi de nous intéresser à une approche de cybercriminalité plutôt que de cybersécurité, cette section ne développera pas le sujet du piratage informatique qui est traité à partir d'approches sécuritaires.

Ainsi, nous nous arrêterons sur trois types de cybercrimes : a) la cyberintimidation, b) l'exploitation sexuelle des jeunes en ligne, ainsi que certains crimes économiques, notamment c) la cyberfraude. Comme nous l'avons vu précédemment, c'est pour contrer ces trois types de crimes que la communauté internationale encourage des mesures préventives (CCPCJ, 2010; ONUDC, 2013, 2015).

a. Prévention de la cyberintimidation

Comme nous l'expliquions en introduction, le cyberespace offre une relative impression d'anonymat, favorisant le développement de comportements violents à l'égard d'autrui, sans craindre des représailles immédiates d'une personne tierce (Notar, Padgett, & Roden, 2013; Snakenborg, Van Acker, & Gable, 2011). La cyberintimidation renvoie à l'usage d'un médium de communication digitale par des groupes ou un individu cherchant à partager des informations jugées, par une personne raisonnable, comme étant blessantes, vulgaires, menaçantes, embarrassantes, effrayantes, etc.

Les réponses internationales et nationales suggèrent, généralement, une prévention de type universelle ou primaire. Plus précisément, il s'agit surtout dans ces réponses, de sensibilisation des parents, des intervenants scolaires et des étudiants visant une utilisation plus sécuritaire d'internet. Williams et Pearson (2016) rapportent que de nombreuses organisations américaines et britanniques recommandent aux jeunes utilisateurs d'internet d'utiliser les paramètres de confidentialité à leurs disponibilités, le signalement des incidents à des adultes, de conserver les preuves d'actes de cyber-intimidation, au lieu de les effacer, puis d'éviter de répondre ou de réagir à ces actes. Dans le même ordre d'idées, les auteurs encouragent les adultes à signaler ces actes auprès des fournisseurs internet, les écoles et les médias sociaux concernés (Williams & Pearson, 2016).

Les écoles sont de plus en plus nombreuses à développer des initiatives en prévention de la cyberintimidation. Toutefois, la plupart d'entre elles ont tendance à se résumer à la dispense d'activités de sensibilisation à l'aide de vidéos pédagogiques, ou à l'élaboration de code de vie visant à favoriser le vivre-ensemble et les relations non conflictuelles (Snakenborg et al., 2011). Par contre, d'autres approches en milieu scolaire, basées sur des données probantes, vont beaucoup plus loin, telles que a) iSAFE, aux États-Unis; b) KiVa en Finlande; le c) ConRed (Programme connaissance, construction et vivre-ensemble sur l'internet) en Espagne; le d) No Trap en Italie; et finalement, le e) ViSC, en Autriche. Ces pratiques sont fréquemment mentionnées dans la littérature pour leurs résultats positifs (Chisholm, 2014; Espelage & Hong, 2016; Notar et al., 2013; Slonje, Smith, & Frisen, 2013; Snakenborg et al., 2011).

a) Le programme iSAFE peut être offert à l'attention des élèves en dernière année du secondaire, des parents, des enseignants ou encore, des leaders communautaires (Snakenborg et al., 2011). Le cursus comprend 5 ateliers de 60 minutes, qui aborderont les thèmes de la sécurité en ligne, la citoyenneté dans le cyberespace, la sécurité personnelle, la propriété intellectuelle et l'application de la loi dans l'environnement virtuel (Espelage & Hong, 2016).

b) KiVa est un programme scolaire holistique, combinant prévention développementale universelle et indiquée, à l'attention des enfants de 7 à 15 ans. Ce programme requiert la participation des professeurs, des parents, des leaders du milieu et des étudiants (Espelage & Hong, 2016). Les enseignants disposent d'un guide d'instruction, complété par un jeu vidéo à l'attention des jeunes du primaire et d'un forum internet pour les jeunes du niveau secondaire (Espelage & Hong, 2016). Un des objectifs des outils proposés consiste à sensibiliser les jeunes sur les conséquences de la cyberintimidation et de venir en soutien aux jeunes victimes d'intimidation (Slonje et al., 2013). Le programme a démontré des résultats positifs lors d'une étude à grande échelle (avec un groupe contrôle) déployée dans près de 90% des écoles du réseau scolaire finlandais. Sur la base de ses résultats, KiVa a démontré l'importance du rôle joué par les témoins dans le processus d'intimidation (Hutchings & Clarkson, 2015).

c) Le ConRed est un programme d'intervention basé sur des données probantes, mettant l'emphase sur l'anonymat des agresseurs, la portée des agressions et la souffrance des victimes (Ortega-Ruiz, Del Rey, & Casas, 2012). La démarche d'Ortega et al (2012) se décline de quatre façons : 1) le développement de pratiques, de procédures et de stratégies proactives de prévention, dont l'objectif est la mise en œuvre d'un plan d'action spécifique visant à lutter contre les risques entourant l'usage d'internet et des réseaux sociaux, à renforcer les capacités des intervenants et à développer des techniques d'autorégulation ; 2) le développement des connaissances et des compétences du milieu de l'éducation, à l'aide de mécanismes permettant de développer les compétences nécessaires à l'identification, la prévention et l'intervention ; 3) le développement d'un environnement scolaire sécuritaire facilitant la communication entre les étudiants, fomentant en eux une culture de soutien et de respect mutuel et d'empathie avec les plus vulnérables ; 4) enfin, le développement de partenariats école-famille-communauté, ayant pour objectif de promouvoir la collaboration entre les intervenants scolaires, les parents et les organismes du milieu, dans une optique de réduction des comportements problématiques.

d) Le No Trap ou le Let's not fall into the trap! est un programme visant à prévenir et lutter à la fois contre l'intimidation et la cyberintimidation. Lancé en 2008, le programme se réalise en deux étapes distinctes, la première étant gérée par des chercheurs en psychologie, puis la deuxième par un groupe d'étudiants qui agissent à titre de leaders positifs. Ces derniers reçoivent une formation leur permettant d'agir à titre d'acteur de changement dans le monde virtuel à l'aide d'outils de sensibilisation, ainsi qu'à titre d'acteur de soutien auprès des collègues de leur classe, dans un contexte de personne à personne. Plus précisément, ces leaders tiendront des activités coopératives avec d'autres jeunes de leur classe, en mettant l'emphase sur l'empathie, la résolution de problèmes et les responsabilités des témoins. Les auteurs des programmes suggèrent de réaliser ce type de programme auprès des 14-15 ans, puisque cette tranche d'âge représenterait, selon eux, un groupe beaucoup plus à risque de décrochage, que les autres (Palladino, B.E., Nocentini, A. et Menesini, E. 2016).

e) Finalement, le ViSC, est un programme visant à prévenir la violence et favoriser le développement d'habiletés sociales dans les écoles secondaires. Le programme envisage trois niveaux d'interventions : l'école, la classe et le jeune. Ce modèle, dit en cascade, demande donc à l'entraîneur ou l'intervenant d'appliquer le programme en fonction du niveau d'intervention. Les intervenants ciblés par le programme sont ici les enseignants et les psychologues en milieu scolaire. De 2008 à 2011, trente-six (36) intervenants autrichiens ont été formés. L'évaluation réalisée en 2012 par Strohmeier et ses collègues démontre que des effets positifs ont été observés dans le groupe testé, comparativement au groupe contrôle (Spiel, C., Wagner, S., et Strohmeier, D., 2012).

Encadré 4.3. **Le rôle des intervenants de la santé**

La cyberintimidation est souvent considérée comme une problématique de justice criminelle et d'éducation (Moreno & Vaillancourt, 2016). Toutefois, les intervenants du milieu de la santé sont de plus en plus sollicités afin de participer aux interventions visant la prévention de la cyberintimidation (Espelage & Hong, 2016). En effet, de par leur rôle, les médecins, les infirmiers, les psychologues et les travailleurs sociaux sont en mesure d'être plus actifs en ce qui a trait à l'identification et la prévention de la cyberintimidation (Dale, Russel, & Wolke, 2014). Certains chercheurs vont même jusqu'à affirmer que les intervenants de la santé devraient directement demander aux jeunes si ceux-ci sont victimes d'intimidation, et si oui, depuis combien de temps, à quel endroit, et de quelle façon cela affecte la vie quotidienne du jeune (Espelage & Hong, 2016). Par ailleurs, ces interventions mériteraient alors d'être réfléchies à l'intérieur du cadre plus large des initiatives en santé publique (Dale et al., 2014), en partenariat avec les intervenants du milieu scolaire (Moreno & Vaillancourt, 2016).

b. Prévention de l'exploitation sexuelle des enfants en ligne

L'exploitation sexuelle des enfants est un crime contre l'intégrité de la personne, englobant tout ce qui a trait aux abus sexuels, à la violence et l'exploitation des enfants, à des fins sexuelles ou financières (IHE, 2010). Par ailleurs, ce symptôme serait alimenté par les représentations stéréotypées que renvoient les médias, tels que la sexualisation et la soumission des enfants et des femmes, notamment dans les jeux vidéo, les publicités, et les émissions télévisées, mais aussi par la pornographie légale, se nourrissant de ces mêmes stéréotypes (Prevention Institute, 2009).

Le UK Council for Child Internet Safety recommande, dans son rapport Child Safety Online (2015), une meilleure gestion du contenu personnel publié sur les réseaux sociaux, le renforcement des paramètres de sécurité et confidentialité, ainsi que l'ajustement des contrôles parentaux, afin d'éviter que des mineurs soient en contact avec du contenu illégal. En cas de diffusion d'images non-consensuelles, offrir le support d'une équipe spécialisée à la victime, envisager l'utilisation de technologies telles que PhotoDNA et les acteurs pertinents comme l'Internet Watch Foundation afin de faciliter le retrait de contenus illégaux. Enfin, le Conseil recommande aussi de sensibiliser à la fois les parents et les intervenants en milieu scolaire et de développer ces campagnes de sensibilisation avec le soutien d'experts afin de rejoindre différentes communautés (Williams & Pearson, 2016).

Lutter contre ces crimes demande une approche intégrée, soutenue par différents cadres légaux nationaux et internationaux (ICMEC & UNICEF, 2016). Une approche intégrée signifie que les stratégies développées à chacun des niveaux de gouvernement se doivent d'être multisectorielles et multidisciplinaires. Autrement dit, la littérature recommande que ces stratégies soient menées à la fois par le système de justice criminelle, la protection de la jeunesse, l'industrie des technologies de l'information et qu'elles nécessitent la mise en œuvre de mesures de prévention développementale, environnementale et partenariale (ICMEC & UNICEF, 2016; IHE, 2010; LIBE, 2015).

Dans le contexte de l'exploitation sexuelle, les mesures développementales se rapportent surtout aux activités de sensibilisation, de renforcement des capacités et des programmes de soutien aux victimes d'actes criminels, ainsi que des programmes de prévention de la récidive. Pour ce qui est des mesures dites environnementales, la littérature fait notamment référence à la fermeture ou au blocage des sites hébergeant des contenus illégaux, et aux contrôles parentaux. Finalement, en ce qui a trait à la prévention partenariale, il est plutôt question de développer des programmes cherchant à répondre aux facteurs de risque propres à l'exploitation sexuelle, et de rendre imputable l'industrie pornographique, ainsi que les hébergeurs.

Sensibilisation des jeunes, des parents et des acteurs concernés

Tout d'abord, la sensibilisation vis-à-vis des enjeux de l'exploitation sexuelle auprès des jeunes, des parents et des acteurs

concernés, notamment les intervenants en milieu scolaire, les hébergeurs, les fournisseurs d'accès internet et les représentants du milieu des médias (LIBE, 2015), est une des recommandations de base que l'on retrouve dans la majorité des conventions internationales, jusqu'à ce jour (ICMEC & UNICEF, 2016). Ces activités de sensibilisation visent principalement à favoriser un usage responsable d'internet, notamment en informant sur les facteurs permettant de repérer des situations d'exploitation (Simantiri, 2017), en permettant aux usagers de développer des techniques d'autorégulation, enfin, en rappelant les responsabilités propres à chaque usager (LIBE, 2015). À titre d'exemple, le Centre canadien de protection de l'enfance enseigne aux enfants et aux adolescents comment développer des comportements sécuritaires en ligne, en réduisant leur vulnérabilité et en renforçant leur résilience. Le programme s'appuie sur des données probantes et comporte des informations sur les relations amoureuses, les risques liés à l'utilisation d'internet et à la mise en ligne de contenu personnel (IHE, 2010).

Développement de programmes sur mesure, à l'attention des victimes et des délinquants

L'identification des victimes est aussi recommandée par le Comité des libertés civiles, de la justice et des affaires intérieures du Parlement européen (2015). En effet, ce comité précise que l'identification des victimes, ou des victimes potentielles, permettrait aux décideurs publics et aux organismes concernés de développer des programmes de soutien sur mesure (LIBE, 2015). Dans le même ordre d'idées, au-delà des sanctions pénales, est aussi mis en avant le développement nécessaire de programmes de soutien à l'attention des délinquants (Simantiri, 2017) et des individus ayant verbalisé leurs désirs avant le passage à l'acte, tel que suggéré par la Directive 93 de l'Union européenne (2011) :

> Afin de prévenir les abus sexuels et l'exploitation sexuelle des enfants, des programmes ou des mesures d'intervention visant les délinquants sexuels devraient être proposés à ces derniers. Ces programmes ou mesures d'intervention devraient s'inscrire dans une approche large et souple, axée sur les aspects médicaux et psychosociaux et revêtir un caractère facultatif. Ces programmes ou mesures d'intervention s'entendent sans préjudice des programmes ou mesures imposés par les autorités judiciaires compétentes (Directive 2011/93/UE, no.37).

À titre d'exemple, il existe en Autriche des centres de suivi pour les hommes craignant de commettre des crimes sexuels sur un mineur. D'autres programmes, tels que LIMES, offre du dépistage, des thérapies individuelles et de groupe, ainsi que des services psychologiques pour les hommes n'ayant jamais commis de crimes sexuels envers des mineurs, mais en exprimant le désir. Dans le même ordre d'idées, la fondation Sexpo, en Finlande, offre un programme de prévention pour les personnes ayant commis ou ayant peur de commettre des crimes sexuels sur mineurs, incluant une ligne téléphonique gratuite et des suivis thérapeutiques (LIBE, 2015).

Contrôle parental, autorégulation et fermeture des sites hébergeant du contenu illégal

Dans une optique de prévention environnementale, la théorie des opportunités nous invite à réfléchir aux différents mécanismes qui nous permettraient de rendre les contenus illégaux inaccessibles au grand public, du moins, jusqu'à ce que ceux-ci soient définitivement supprimés (Prevention Institute, 2009), tel que le recommande l'Union européenne :

> La lutte contre ce phénomène exige de réduire la diffusion du matériel relatif à des abus sexuels d'enfants en rendant la mise à disposition du public en ligne de ce contenu plus difficile pour les auteurs d'infractions. Il convient donc de supprimer le contenu et d'appréhender les personnes qui se rendent coupables de production, de diffusion ou de téléchargement d'images d'abus sexuels d'enfants (Directive 2011/93/UE, no.46).

Les contrôles parentaux, tout comme les paramètres de confidentialité adaptés en fonction de l'âge des publics, sont des outils technologiques pouvant améliorer la sécurité des jeunes dans le cyberespace (LIBE, 2015).

Rôle de l'industrie, des fournisseurs d'accès internet et des hébergeurs

Le rôle de l'industrie pornographique, tout comme des médias, est aujourd'hui largement reconnu dans la banalisation des violences sexuelles et de l'exploitation sexuelle (MacKinnon, 2005; Prevention Institute, 2009; Sun, Bridges, Johnson, & Ezzell, 2016). À cet égard, le Prevention Institute (2009) recommande à l'industrie pornographique de mettre fin à l'objectification sexuelle des adolescents et des enfants, et recommande aux médias de mettre fin aux publicités mettant en scène des jeunes sexualisés.

Dans le même ordre d'idées, l'Union internationale des télécommunications recommande aux gouvernements d'élargir le mandat et la portée de leurs agences régulatrices en matière de technologie de l'information et de la communication (TIC). Notamment en ce qui a trait à la protection des consommateurs, la cybersécurité et leur participation dans le développement et la mise en œuvre de politiques publiques adaptés au cyberespace (UIT, 2014).

c. Prévention de la cyberfraude

Comme nous l'avons expliqué au chapitre précédent, la fraude est un phénomène protéiforme, que nous pourrions désigner comme étant « une sollicitation sous de faux prétextes pour obtenir de l'argent (Prates, Gaudreau, & Dupont, 2013) » et/ou des biens matériels. Encore une fois, la recherche entourant les modes de prévention concerne surtout les théoriciens des activités routinières et du choix rationnel. Par conséquent, la plupart des mesures de prévention proposées jusqu'à aujourd'hui concernent la prévention situationnelle. À cet égard, Gupta et Sherman (2011) ont développé trois types de prévention situationnelle propres au cyberespace : la **prévention active**, qui

demande aux usagers de modifier sur une base régulière leurs paramètres de sécurité et leurs mots de passe; la **prévention par l'évitement**, qui demande aux usagers d'utiliser moins fréquemment l'internet pour leurs transactions bancaires et l'achat de biens; et enfin, la **prévention passive**, qui demande aux usagers de refuser les courriels de sources inconnues, d'installer et mettre à jour leurs logiciels antivirus et de ne visiter que des sites de confiance. Selon les auteurs, l'application de ces trois types de prévention permettrait de réduire fortement le risque de victimisation individuelle (Williams & Levi, 2017, p. 459-460) .

Il est certain que le manque de renseignements fiables sur la cybercriminalité, notamment économique, est vu comme un obstacle majeur à l'élaboration de stratégies de prévention du crime portant sur la cybercriminalité (Smyth & Carleton, 2011). Malgré l'ampleur qu'a pris aujourd'hui la cyberfraude, et bien qu'il y ait des millions de dollars en jeu chaque année, la prévention entourant ce cybercrime reste tout à fait partielle.

Encadré 4.4. **Rôle des forces de l'ordre dans la prévention de la cyberfraude**

Les forces de police ont développé des techniques d'investigation clandestine sur internet (Chu et al., 2010; Franklin et al., 2007; Hinduja, 2007; Poulsen, 2012; Jenkins, 2001; Wolak, Finkelhor, & Mitchell, 2012; Holt & Lampke, 2010; Peretti, 2009). De nombreuses agences de forces de l'ordre ont ainsi infiltré des forums et des canaux de discussion en ligne, notamment pour perturber des marchés. Ces approches sont vues comme ayant un effet dissuasif, réduisant les gains potentiels et augmentant les risques pour les criminels. Plusieurs opérations ont notamment amené des agents des forces de l'ordre à prendre le contrôle de ce type de sites pour arrêter leurs membres (ex: Mills, 2009). Ce genre d'action permet à la fois de rassembler le plus de preuves possible contre les personnes arrêtées, mais aussi de saper la confiance entre divers acteurs du marché. Toutefois, certaines études indiquent que les cybercriminels arrêtés recevraient des sanctions insuffisamment élevées par rapport à leurs actes, ce qui pourrait fortement remettre en question l'effet dissuasif de telles actions (Holt, 2013; Wall, 2007).

Troisième partie : les difficultés à appliquer les théories classiques de prévention à la cybercriminalité

Depuis plus d'une trentaine d'années, les théories de la prévention de la criminalité se sont développées autour de la compréhension des comportements des victimes et des motivations criminelles potentielles (Lewis & Lewis, 2011). Graduellement, le concept de la prévention de la criminalité est devenu une importante composante des stratégies nationales, régionales et locales en sécurité publique (voir chapitre 1). La prévention de la criminalité postule que le crime est associé à une série de facteurs de risque sous-jacents et que, par conséquent, c'est en identifiant ces facteurs que nous arrivons à développer des stratégies de prévention efficaces. Comme nous l'avons vu dans le chapitre précédent, l'identification de ces facteurs dépend en grande partie de l'approche criminologique appliquée à la problématique criminelle. À cet égard de l'identification des facteurs de risque, le cyberespace soulève de nombreux enjeux, dus entre autres, comme susmentionnés, à la relative impression d'anonymat des usagers, du faible contrôle social exercé sur les réseaux sociaux, des caractéristiques spatio-temporelles propres au monde virtuel, de la multiplication des interactions, ou encore de la portée des actes. Nous chercherons par conséquent à établir les principaux constats de la littérature quant à l'applicabilité des approches de la prévention de la criminalité les plus souvent utilisées, soit : a) la prévention développementale; et b) la prévention environnementale.

Prévention développementale

Tout d'abord, il est important de rappeler que les crimes contre l'intégrité de la personne représentent des enjeux importants de santé publique, associés à des conséquences très négatives en matière de santé mentale, de développement social et de dommages tels que la marginalisation sociale et économique, la dépression, ou encore le suicide (Chisholm, 2014; Espelage & Hong, 2016; Kowalski, Limber, & Agoston, 2008; Notar et al., 2013). Selon Patchin & Hinduja (2012), Espelage & Hong (2017), la démocratisation rapide de l'usage d'internet et des nouvelles technologies de l'information aurait provoqué une dilution des frontières entre sphères privée et publique, faisant d'internet une extension du monde réel, plutôt qu'un complément, avec ses spécificités propres (Berguer, 2015). Selon Collier (2010), ce constat est primordial dans la compréhension du phénomène de la violence dans le cyberespace, puisqu'il amène l'idée que la technologie ne serait « ni le problème ni la solution (Collier & Nigam, 2010, p. 10) ». Par conséquent, la prévention des cyberviolences devrait, avant tout, être comprise comme une question sociale et non technologique, sans quoi toute stratégie de prévention pourrait s'avérer inefficace. C'est pour cette raison que la prévention développementale reste encore pertinente dans le contexte de la cybercriminalité visant l'intégrité des personnes.

Encadré 4.5. **L'approche développementale**

La prévention de criminalité dans une perspective développementale prend racine dans l'idée que la criminalité est en grande partie liée à des facteurs de risques sociaux et environnementaux ayant affecté le développement de l'individu (Tilley, 2005 ; Tremblay & Craig, 1995). Elle découle principalement des théories comportementales et sociologiques, des années 60 et 70, analysant les différents comportements criminels tant pour en faire des typologies que des trajectoires criminelles (Tremblay & Craig, 1995). Selon les principes directeurs de l'ONU, la prévention développementale vise à « favoriser le bien-être des populations et à encourager un comportement sociable par l'application de mesures sociales, économiques, sanitaires et éducatives, en privilégiant en particulier les enfants et les jeunes et en mettant l'accent sur les facteurs de risque et de protection associés à la criminalité et à la victimisation » (ONUDC, 2010, p. 13).

Alors que les intervenants de première ligne et les chercheurs s'intéressent de plus en plus à la prévention développementale dans le cadre de leurs activités, celle-ci occupe une place encore très marginale dans la littérature sur la cybercriminalité, ainsi que dans les différentes stratégies nationales de prévention mises en œuvre au cours des dernières décennies (Bossler & Holt, 2016 ; EUCPN, 2017 ; Seger, 2012 ; Williams & Levi, 2017). En effet, outre les campagnes de sensibilisation sur l'intimidation en ligne, la protection des données personnelles, tel que recommandés par les lignes directrices de l'ONU (ONUDC, 2013), ou encore, la dispense d'ateliers pédagogiques en milieu scolaire, tel que iSAFE, très peu de programmes « sur mesure » visant à réduire ou atténuer les facteurs de risques propres à la cybercriminalité, tels que KiVa et ConRed, ont été développés. Plusieurs raisons permettent d'expliquer cette lacune, notamment le peu d'études portant sur les facteurs de risque propres à la cybercriminalité jusqu'à ce jour, à l'exception de la cyberintimidation et de l'exploitation sexuelle en ligne (Lewis & Lewis, 2011), mais aussi, l'importance qu'a prise la protection des infrastructures critiques de l'information, suite aux cyberattaques de 2007.

Les deux chapitres précédents ont bien montré que l'état actuel des recherches sur la cybercriminalité ne permet pas, pour l'instant, d'établir de corrélations directes entre des facteurs de risque de type « macro » (sociaux, économiques et d'inégalités, entre autres) et les processus de criminalité ou de victimisation.

Malgré la difficulté évidente à utiliser ce modèle de prévention, nous pouvons envisager au moins deux facteurs qui peuvent servir à aborder cette problématique : les normes sociales et le contrôle social. Les valeurs et les normes sociales semblent en effet avoir un lien effectif avec le développement ou non d'activités illégales dans le cyberespace. Sur ce point, deux éléments sont à souligner sous un angle situationnel. Premièrement, les normes sociales se construisent selon plusieurs formes dans le cyberespace, dont deux particulièrement nous intéressent du point de vue de la prévention de la cybercriminalité. Tout d'abord, les valeurs sociales qui existent dans le monde dit « réel » sont modifiées dans le cyberespace. Par exemple, la gravité perçue des acteurs cybercriminels tend à montrer une plus grande acceptation des activités illégales dans le cyberespace que dans le monde dit « réel ». Ceci a été montré par plusieurs études, portant notamment sur les phénomènes de cyberharcèlement et de cyberviolences contre les femmes (Herring, 2002; Dunn, Lalonde, & Bailey, 2017; West, 2014), ainsi que sur des études sur la perception de délits comme le piratage en ligne (Chaudhry, Chaudhry, Stumpf, & Sudler, 2011; Krawczyk, Kukla-Gryz, & Tyrowicz, 2015). Ces normes sociales se (re)construisent également en fonction des conditions intrinsèques du cyberespace, notamment, entre autres, des dimensions d'anonymat et de dépersonnalisation des interactions (Koops, 2010). Ainsi, on ne peut compter seulement sur les campagnes de sensibilisation et la répression si nous voulons réellement endiguer les problèmes de cyberintimidation et d'exploitation sexuelle en ligne. S'il faut développer une culture de cybersécurité, comme le stipule la Stratégie en sécurité cybernétique de l'OEA, il importe de développer une culture de prévention des actes répréhensibles visant l'intégrité de la personne, ayant pour objectif de changer les normes sociales vis à vis de la banalisation de ce type de crime, entre autres.

Dans le même ordre d'idées, le contrôle social, qui agit comme un puissant facteur de protection dans le monde dit « réel », se trouve considérablement relativisé dans le cyberespace. Dès lors, la redéfinition des normes sociales, ainsi que les caractéristiques environnementales telles que l'anonymat ou la dépersonnalisation, viennent modifier la manière dont la collectivité agit comme un facteur de régulation des comportements individuels: d'une part, la déconnexion physique et l'anonymat tendent à affaiblir la possibilité de contrôle social ; d'autre part, la capacité de mobilisation à vaste échelle, notamment à travers les réseaux sociaux, contribue à renforcer ce même contrôle social. Cette tendance a notamment été illustrée par le mouvement Me too / Moi aussi.

Enfin, un élément trop souvent écarté de la littérature en prévention de la criminalité est le **principe de différenciation**. Plus précisément, le principe de différenciation demande aux parties prenantes de réfléchir aux enjeux des cyberviolences sous un angle différencié selon le genre, le sexe, l'orientation sexuelle, la religion, etc. L'adaptation des stratégies de prévention aux différents groupes d'individus auxquelles elles sont proposées est un principe absolument central dans la prévention classique. Si la cybercriminalité, quant à elle, s'inscrit aussi dans un contexte différencié (pour les auteurs comme pour les victimes), la différenciation des stratégies de prévention y revêt des dimensions distinctes : tous les types de délits commis sur Internet ne se prêtent pas à une approche différenciée. Ang et Goh (2010) abondent en ce sens dans le contexte de la cyberintimidation, stipulant que les initiatives en prévention devraient systématiquement inclure

des formations sur l'empathie, mettant l'accent sur l'empathie cognitive chez les garçons et l'empathie affective chez les filles (Chisholm, 2014).

Prévention environnementale

La prévention environnementale comprend à la fois la prévention situationnelle et la prévention par l'aménagement du territoire. Principalement développée au courant des années 70 par le Home Office britannique (Tilley, 2005), la prévention environnementale de la criminalité vise à limiter les opportunités criminelles, augmenter le risque associé à la commission d'un crime et réduire les avantages que pourrait en tirer le délinquant (ONUDC, 2010). Cette approche découle principalement des théories du choix rationnel (Clarke & Cornish, 1985), de l'activité routinière (Cohen & Felson, 1979) et des motivations criminelles (Brantingham & Brantingham, 2008), aussi appelées les théories de l'opportunité (Sutton, Cherney, & White, 2008; Tilley, 2005). Newman et Clarke (2003) stipulent que « la criminalité suit l'opportunité, lorsqu'il y a, au même moment, dans un lieu donné, présence de motivations criminelles, de facteurs d'attractions et de cibles intéressantes dénuées de protection effective (Broadhurst, 2005, p.7) ». De nos jours, la prévention situationnelle est devenue, en quelque sorte, un synonyme de la réduction des opportunités. Par conséquent, ce type d'approche se traduit souvent par des patrouilles policières ciblées, des activités de médiation sociale dans les parcs et les transports publics, ou encore la pose de caméras (Sutton et al., 2008).

Les mesures préventives les plus souvent soulevées dans la littérature portant sur la cybercriminalité nous renvoient aux approches de prévention dite situationnelle, généralement sous l'angle de la théorie des activités routinières (Cobb, 2014; Dashora, 2011; Leukfeldt & Majid, 2016; Williams & Levi, 2017; Poonia, Bhardwaj, & Dangayach, 2011). Ces approches mettent l'emphase sur la réduction des opportunités criminelles au travers des changements de comportements des usagers et de la modification des caractéristiques environnementales favorisant le développement de ces opportunités (Cornish & Clarke, 2003; EUCPN, 2017; Sutton et al., 2008).

Plus précisément, Bossler et Holt (2016) envisagent quatre catégories d'intervention situationnelle dans le cadre de la prévention de la cybercriminalité: (1) accroître la difficulté de commettre un crime; (2) augmenter les risques liés au délit; (3) créer des mécanismes réduisant la récompense liée à l'acte cybercriminel ; et finalement (4), éliminer les excuses pour les auteurs, afin qu'ils ne cherchent pas justifier leurs actes par des phénomènes extérieurs (Bossler & Holt, 2016, p. 137). On peut penser ici à l'utilisation de logiciels antivirus et/ou de bloqueurs de publicité afin de se protéger de logiciels malveillants (Ngo & Paternoster, 2011) ou des vols d'identités (Bossler & Holt, 2016). Toutefois, leur efficacité n'est pas toujours garantie (Ngo & Paternoster, 2011). En ce qui a trait aux logiciels de contrôle parental, ceux-ci auraient un impact minimal sur le risque d'intimidation, de harcèlement et d'avances sexuelles que les jeunes pourraient subir sur internet (Jones et al., 2006; Marcum, 2013).

Toujours dans l'optique de limiter les opportunités criminelles, Ngo et Paternoster (2011) proposent une vision nouvelle des patrouilles policières dans le contexte du cyberespace. Conscients du fait que le concept ne peut s'appliquer de la même façon dans le cadre du monde virtuel, les auteurs s'en inspirent afin de développer leur concept de stratégie policière distribuée. Au lieu de reposer d'abord sur la police puis sur les citoyens, cette stratégie argumente que le cyberespace demanderait une inversion des rôles. Puisque, dans ce cadre, le fait qu'une personne ne prendrait pas en main sa propre sécurité pourrait permettre la victimisation d'une autre personne (Ngo & Paternoster, 2011). Dans le même ordre d'idée, Garland (2001) argumente que l'application de la loi dans le monde virtuel doit aussi passer par la responsabilisation des entreprises privées et de la société civile (Williams & Levi, 2017).

Bien que le concept d'opportunité permette à la prévention environnementale d'identifier les lieux propices à la commission d'actes criminels, cette approche ne permet pas d'expliquer les causes de la criminalité (Cobb, 2014; Tilley, 2005). Ainsi, n'agissant pas directement sur les causes de la criminalité, la PSC n'engage que très rarement des changements à long terme. Par ailleurs, dans une optique de choix rationnel, la prévention environnementale peut aussi avoir pour simple effet le déplacement de la problématique criminelle (Cobb, 2014). Ainsi, la présence de mesures développées à partir de l'approche environnementale pourrait aussi avoir un effet néfaste sur le sentiment d'insécurité de la part du public qui en est témoin (Cobb, 2014).

Vers une prévention partenariale dans le cyberespace

La prévention de la cybercriminalité fait appel à des structures de gouvernance radicalement différentes de celles du monde dit réel, et qui s'organisent sous forme de réseaux. Afin d'opérationnaliser ces réseaux, il est nécessaire de former des partenariats et des mécanismes de coopération, dont nous distinguerons ici deux types : le premier concerne l'harmonisation des cadres juridiques et la coopération internationale des systèmes de justice et des services de police, tandis que le second se penche sur la coopération des différents types d'acteurs, dans une perspective de gouvernance nodale.

Comme l'ont souligné les deux précédents chapitres, une des difficultés majeures qui se pose dans le cadre de la lutte contre la cybercriminalité réside en la nature même du cyberespace et des activités qui s'y déroulent : leur (relative) déconnexion des territoires physiques. Déconnexion, car les caractéristiques principales qui régissent la manière dont la criminalité est envisagée reposent sur leur localisation : localisation de l'auteur, de la victime et de l'acte, qui s'inscrivent dans une certaine unité. C'est donc cette unité qui vole en éclat avec la cybercriminalité : la victime et l'auteur peuvent se trouver dans des pays différents, et l'acte en tant que tel peut faire intervenir d'autres localisations physiques, par exemple celle des serveurs piratés et qui stockaient la donnée volée.

Ceci implique que la gouvernance physiquement fragmentée que l'on connaît, et la manière dont elle aborde la criminalité (sous la forme d'institutions de police et de justice, de cadres juridiques et législatifs géographiquement limités) ne permettent pas de répondre efficacement à la cybercriminalité. La collaboration étroite des acteurs au niveau international, ainsi que l'harmonisation des cadres régulateurs, constitue alors les conditions essentielles de lutte contre la cybercriminalité. À ce sujet, Dupont (2016) observe que les pratiques coopératives existantes indiquent l'émergence d'un nouveau modèle de gouvernance, qu'il nomme polycentrique, et qui se caractérise par un fonctionnement en réseaux multiacteurs concrétisés sous forme de partenariats. L'auteur souligne en outre que l'étude de ces réseaux montre une plus grande adaptabilité que ce que les conceptions généralement admises tendent à véhiculer, notamment en ce qui a trait aux institutions gouvernementales, tout particulièrement celles des systèmes police-justice.

Encadré 4.6. **Les réseaux informels de police**

Une prévention holistique de la cybercriminalité demande des ressources spécialisées, en mesure de prendre en charge des problématiques complexes. Ce faisant, de nombreuses organisations policières n'arrivent pas à répondre adéquatement aux enjeux de la cybercriminalité, entre autres, par manque de connaissances adéquates ou de personnel qualifié. Ainsi, le réseautage entre les différents services de police peut s'avérer une solution peu coûteuse et efficace pour répondre à ces enjeux. Dans le même ordre d'idées, Bayer (2010), dans une revue de littérature substantielle, complétée par de nombreux entretiens avec différents services de police et agences de renseignement, stipule que les réseaux policiers traditionnels sont généralement critiqués comme étant inefficaces et coûteux, dû à l'importance de la bureaucratie impliquée dans ces processus de réseautage. C'est pourquoi certains auteurs, tels que Eskola (2012), recommandent la formation de réseaux informels de partage de pratiques, de connaissances et d'expertise technique, afin d'éviter d'alourdir les processus des différentes agences d'application de la loi concernées (Eskola, 2012).

Nhan et Huey (2008) identifient quatre « grappes nodales » (nodal clusters), des pôles d'acteurs essentiels qui conforment les réseaux : les gouvernements (incluant l'ensemble des institutions gouvernementales ou multigouvernementales, nationales et internationales, en dehors de celles conformant les systèmes de justice criminelle), les systèmes de justice criminelle (c'est-à-dire la continuité des acteurs Police-Justice), le secteur privé à toutes les échelles, et enfin le public des usagers (incluant également les organisations de la société civile en ligne et dans le monde réel). Quéro et Dupont (2017) distinguent cinq types de capital qui conforment les caractéristiques spécifiques des nœuds dans les relations avec d'autres types d'acteurs : 1) le capital social désigne la capacité d'un nœud à créer et maintenir des relations de bénéfice mutuel avec d'autres nœuds ; 2) le capital culturel, lié à la connaissance d'un nœud en termes de cybercriminalité et de cybersécurité, connaissance pouvant constituer une ressource pour d'autres ; 3) le capital politique qui s'attache à l'aptitude d'un nœud à comprendre les dynamiques liées aux structures politiques, gouvernementales et aux institutions publiques à toutes les échelles ; 4) le capital économique, quant à lui associé à la compréhension, par un nœud, des dynamiques de marchés et des structures de l'économie, ici aussi à toutes les échelles, ainsi qu'à son pouvoir économique et ; 5) le capital symbolique qui englobe l'ensemble des facteurs contribuant à la légitimité organisationnelle d'un nœud.

Ainsi, pour que ces réseaux se forment et que leurs différentes grappes nodales coopèrent de manière efficace, il est nécessaire de développer plusieurs types de mécanismes : 1) l'harmonisation des cadres de régulation, 2) la coopération des différents acteurs de police et de justice agissant dans des juridictions distinctes et 3) les partenariats de collaboration incluant l'ensemble des catégories d'acteurs.

Compte tenu de la multitude de facteurs de risque, du faible contrôle social et de l'abondance des opportunités criminelles, Williams et Levi (2017) affirment qu'il est primordial d'envisager toutes initiatives de prévention de la cybercriminalité dans une optique partenariale. La prévention communautaire ou partenariale se fonde sur la notion qu'il est possible d'influer positivement sur les comportements criminels en modifiant l'organisation physique et sociale d'un milieu donné (Tonry & Farrington, 1995). Les initiatives de prévention résultant de ce type d'approche sont informées par l'expertise des participants et les données probantes entourant la problématique (Tilley, 2005). « Les experts en prévention de la criminalité soutiennent que les initiatives en prévention efficaces sont fondées sur la connaissance scientifique entourant la nature et les causes de la criminalité, ainsi que sur les exemples réussis » (Rosenbaum & Schuck, 2012, p.1). Afin de bien informer ces initiatives et d'assurer une mise en œuvre efficace et durable, il est nécessaire d'obtenir la participation du secteur de la santé, du développement social et de la planification urbaine, des services d'aide en recherche d'emploi, des loisirs, du milieu scolaire, du système de justice, des services sociaux, du secteur privé (Crawford, 1999), ainsi que des fournisseurs d'accès internet et des hébergeurs de contenu en ligne, dans le cas qui nous intéresse. En effet, ces deux derniers sont particulièrement bien situés lorsque vient le temps d'informer et d'élaborer des initiatives en prévention de la cybercriminalité, puisqu'ils ont les capacités techniques pour observer les comportements problématiques des usagers, d'interdire l'accès à des contenus illégaux, d'assurer l'application des lois, de faciliter les investigations criminelles et d'intervenir lorsque des individus sont victimes d'actes criminels (ONUDC, 2013).

La gouvernance du cyberespace est multipolaire et essentielle-

ment articulée autour des acteurs privés gérant les infrastructures, l'accès et l'hébergement de contenu d'Internet, un point développé dans le chapitre 2. Ainsi, ce premier principe d'un leadership centré sur les pouvoirs publics ne peut pas être appliqué à la prévention des activités criminelles dans le cyberespace, ouvrant la nécessité d'un modèle adapté, fondé sur le partenariat et la coopération plutôt que sur le leadership d'une seule catégorie d'acteurs.

Du point de vue des pouvoirs publics, la préoccupation pour les activités criminelles commises dans le cyberespace trouve son point de départ dans le monde post 11 septembre 2001 et s'est imposée comme une priorité avant tout sécuritaire face à la menace terroriste (Fratianni & Savona, 2005). S'éloignant du modèle a-gouvernemental à l'origine de la création et du développement d'Internet, ainsi que d'une gouvernance absolument multiacteurs et centrée sur le privé, de nombreux États, aux régimes aussi bien démocratiques qu'autoritaires, se dirige vers un renforcement de leur contrôle sur le cyberespace à travers des régulations et un encadrement plus strict (Deibert & Crete-Nishihata, 2002).

À ce sujet, soulignent Tilley et Sidebottom (2017), les responsabilités liées à la sécurité se sont diluées, dans le cyberespace, entre les acteurs et les usagers organisés sous forme de réseaux (Tilley & Sidebottom, 2017). Wall préconise donc que le leadership développé par les pouvoirs publics dans le cyberespace soit celui d'un facilitateur, encourageant de nouvelles relations entre les différents nœuds des réseaux à la base de la cybersécurité (Wall, 2007).

De fait, la question des responsabilités de chacun des acteurs quant à la sécurité et la prévention de la cybercriminalité est au cœur de la (re)définition de la gouvernance du cyberespace. De la même manière que les pouvoirs publics ne peuvent constituer l'unique régulateur et l'unique entité responsable, le secteur privé, malgré son rôle absolument central dans la cybergouvernance, ne peut assumer l'ensemble de ces responsabilités. À l'heure actuelle, le flou qui entoure les responsabilités de chacun au sein du cyberespace impacte d'abord et avant tout les victimes de la cybercriminalité : ainsi, les victimes de fraude ou de vol d'identité ont généralement peu de recours à leur disposition, et nombre de ces crimes sont de facto traités et considérés comme des conséquences néfastes, mais irrémédiables de l'âge numérique.

En conséquence, une des pistes de réflexion qui s'impose à la suite de ces constats est la nécessité de redéfinir la gouvernance du cyberespace dans une perspective de prévention de la cybercriminalité intégrant un point de vue centré sur les victimes. Ainsi, la question se pose de définir les responsabilités de chacun des acteurs, les régulations, les normes et standards encadrant les accès, les activités et les usages du cyberespace. Cette question constitue une priorité essentielle dans la lutte contre la cybercriminalité et implique des problématiques cœur telles que la question de la privauté, de la collecte, la protection et l'usage des données personnelles, de l'adaptation des systèmes de police et justice aux nouvelles contraintes imposées par le cyberespace. Du point de vue des victimes, cela soulève la question de l'attribution des responsabilités encadrant la sécurité des usagers et de leurs données personnelles.

Enfin, un autre aspect de la prévention partenariale renvoie au principe d'interdépendance, appliqué à la criminalité dite « classique », faisant référence à l'imbrication des échelles et l'importance de trouver, dans les stratégies de prévention, une cohérence scalaire : en bref, la stratégie nationale et les initiatives locales doivent concourir à des objectifs communs et s'articuler de manière complémentaire.

Encore une fois, ce principe se transforme radicalement dans le cadre de la prévention dans le cyberespace. Premièrement, la nature même d'échelle d'action ou de politique prend un sens particulier. En effet, si des niveaux de gouvernance différents peuvent être impliqués dans la prévention de la cybercriminalité, ils s'appliquent tous à un objet a-scalaire et global. Il s'agit donc d'une interdépendance des niveaux d'acteurs exclusivement.

À cette interdépendance d'échelles de gouvernance, nous pouvons associer, dans le cas de ces gouvernances multipolaires et multiacteurs, une interdépendance des grappes nodales : ainsi, les actions et initiatives menées par tel ou tel groupe d'acteurs doivent, au même titre, concourir à des objectifs communs, d'une manière complémentaire.

Conclusion : recommandations

Si la prévention est par définition une action qui s'inscrit dans le moyen à long terme, ce principe se voit opposé au contexte du cyberespace, caractérisé par un rythme de changements très soutenu et des évolutions extrêmement rapides. Ainsi, lorsqu'on souhaite ouvrir une réflexion sur la prévention des diverses formes de violences et de criminalité sur le cyberespace, il est nécessaire d'intégrer ces évolutions rapides au sein d'une approche durable. La question se pose alors de savoir comment construire des perspectives de prévention très adaptables et capables de conserver leur pertinence et leur efficacité dans des conditions changeantes.

Tout d'abord, comme nous venons de le proposer, l'approche partenariale est centrale à la prévention de la cybercriminalité. C'est pourquoi la question des responsabilités nécessite de construire des initiatives de prévention transparentes, qui définissent clairement les rôles et fonctions des différentes parties prenantes et qui font l'objet d'évaluations rigoureuses. Encore une fois, la gouvernance multiacteurs et multipolaire du cyberespace complexifie beaucoup la manière dont les initiatives sont développées et mises en œuvre :

1) Le leadership, traditionnellement attribué aux autorités publiques, devient plus problématique et sujet à des luttes de pouvoir et d'influence.

2) Dès lors, les questions de mise en œuvre, de gestion et de financement impliquent une capacité accrue de consensus et de collaboration entre les différents acteurs centraux afin de trouver un équilibre des intérêts, notamment dans le cas où ces initiatives impliquent un cofinancement et une cogestion par des groupes d'acteurs très différents.

Logiquement, la dissolution du leadership, et le partage des responsabilités et des rôles entre des groupes d'acteurs de différents types complexifient la recherche de processus transparents, basés sur une reddition de comptes accrue. Cet aspect a été largement documenté par la littérature (notamment dans le secteur de la gestion de l'environnement et des Partenariats Public-Privé), qui montre bien la difficulté à construire une gouvernance multiacteurs efficace, ainsi que les bénéfices qui lui sont associés en termes de transparence et de reddition de compte (Brinkerhoff & Brinkerhoff, 2011) (voir chapitre précédent). Ainsi, la prévention de la criminalité ne peut relever d'un seul acteur ou encore, d'un petit groupe d'acteurs. Les initiatives, à tous les niveaux, doivent considérer la prévention de la cybercriminalité sous la forme d'une démarche intégrée ou holistique, réunissant les acteurs du système de justice criminelle, de la protection de la jeunesse, de l'industrie des technologies de l'information, du milieu scolaire, du secteur de la santé et des services de police, dans une perspective de prévention développementale et environnementale, dans le respect du principe d'interdépendance, de clarté des rôles, des droits humains et de la culture de légalité.

Par ailleurs, compte tenu du niveau encore embryonnaire de notre connaissance de la cybercriminalité, il reste difficile alors de fonder une approche préventive basée sur un corpus scientifique fourni, comme c'est le cas pour la criminalité traditionnelle, ce que les chapitres 2 et 3 ont déjà décrit. Ainsi, du point de vue du preneur de décision, il est impératif de réfléchir à de nouvelles avenues en matière de prévention. Deuxièmement, l'évaluation des programmes de prévention de la cybercriminalité fait face à deux contraintes majeures. Tout d'abord, celle d'évaluer la prévention, qui, en soi, constitue un défi : la prévention, notamment sociale, s'attachant à des facteurs de risque dits « macro ». Elle produit un effet systémique, difficile à mesurer. Ensuite, lorsqu'elle s'attache au cyberespace, cette prévention se heurte à la faible connaissance que nous avons, aujourd'hui, des processus de criminalité, de victimisation sur Internet, et des facteurs correspondants (voir chapitre précédent).

Cela représente, pour des institutions comme le Centre international pour la prévention de la criminalité, un défi majeur : comment développer des outils qui permettent une prise de décision informée et qui ne soit pas centrée sur la connaissance scientifique, mais qui pallient à cette insuffisance par des approches complémentaires ?

Contribution

Chercher à répondre aux enjeux de la criminalité numérique

Jérôme BARLATIER, Ph. D
Chef d'escadron
Service central de renseignement criminel (SCRC), France

La dimension numérique s'impose aux forces de l'ordre comme une évidence qui n'épargne aucune de leurs activités. Dans le domaine judiciaire, elle constitue une opportunité pour le criminel en créant des circonstances qu'il peut mettre à profit pour faire évoluer ses modes opératoires ou en créer de nouveaux. Elle constitue également des potentialités accrues ou inédites pour des enquêteurs qui se trouvent toujours à l'aise dans un monde où le criminel peut être pisté par les traces qu'il génère. Ni zone de non droit, ni big brother, l'Internet renouvelle simplement les enjeux du rapport entre le criminel et le policier.

Le présent article propose d'exposer la stratégie du centre de lutte contre les criminalités numériques (C3N) du service central de renseignement criminel (SCRC) de la gendarmerie nationale.

Une organisation fondée sur la complémentarité et la subsidiarité

La gendarmerie nationale française a accompagné dès l'origine les développements de l'Internet. Elle se prépare désormais aux enjeux futurs de la numérisation de la société.

Partant d'une identité fondée sur la proximité territoriale et la polyvalence de ses agents, elle tente d'investir au mieux le caractère immatériel du cyberespace avec des moyens de plus en plus spécialisés.

La conciliation de ce qui pourrait sembler être un paradoxe repose sur un double principe:

- la subsidiarité entre, d'une part, la démocratisation des savoirs et des outils qui permet de répondre à l'omniprésence du numérique dans les enquêtes courantes et, d'autre part, la spécialisation qui permet le traitement des affaires de cyberdélinquance les plus complexes;
- la complémentarité au sein d'une police judiciaire qui marche sur ses deux pieds : une chaîne d'investigation (articulant l'action d'unités généralistes et de services spécialisées) et une chaîne d'appui (mettant notamment en oeuvre des compétences en terme de criminalistique et de renseignement criminel).

La gendarmerie nationale conjugue ces deux aspects au sein de la chaîne Cybergend, un réseau de 4.400 militaires échelonné en trois niveaux de compétence (application, maîtrise et expertise). Elle se trouve ainsi en mesure de procéder à un large spectre d'investigations répondant aux spécificités de la délinquance sur Internet, à savoir :

- 70 % d'escroqueries,
- 10 % d'atteintes aux systèmes de traitement automatisé de données,
- 10 % d'atteintes à la réputation,
- et 10 % d'autres infractions.

Le C3N se situe au sommet de cet édifice opérationnel de lutte contre la cybercriminalité. Dans un positionnement particulièrement original, il est tout à la fois :

- une unité d'investigation de haut niveau,
- un échelon d'animation du réseau Cybergend,
- un service national de rapprochement judiciaire et de veille numérique,
- un contributeur au renseignement stratégique, opérationnel et tactique,
- un laboratoire de recherche.

La diversité de ces missions représente un véritable atout dans le développement d'une police judiciaire à la fois stratégique et exploratoire.

Une police judiciaire stratégique et exploratoire

Dans un environnement judiciaire concurrentiel, les services d'investigation doivent chercher le positionnement adapté qui signe leur plus-value.

Le C3N concentre ainsi son effort sur le traitement d'un contentieux stratégique qui ne pourrait être efficacement abordé à un autre niveau. La délinquance sur Internet s'affranchit des règles de la territorialité. Le cyberespace est une étendue sans frontière. Il constitue un contexte criminogène particulièrement propice au délinquant qui peut atteindre de façon massive les victimes au sein de l'intimité de leur domicile. Internet crée les conditions favorables à l'anonymat des malfaiteurs et à la dépersonnalisation des victimes. Il facilite le passage à l'acte en évitant leur confrontation directe. En quelques clics, un seul individu ou un groupe astucieux peut atteindre une population considérable et générer des préjudices importants. Dans ces circonstances, le C3N cherche à neutraliser les auteurs prolifiques par une détection appropriée des patterns criminels récurrents. L'ouverture d'enquêtes ciblées permet un travail d'investigation par rapprochement fondé sur la collecte d'une masse critique d'information judiciaire de nature à favoriser le rassemblement des preuves et l'identification des auteurs.

Les poursuites judiciaires ne sont pas le seul aboutissement de ce travail. Le développement d'un partenariat dense, fondé sur la confiance d'acteurs publics et privés, permet également de trouver des solutions non contentieuses propres à endiguer certains phénomènes.

Le C3N s'oriente également sur le traitement d'un contentieux exploratoire. Il tente ainsi de mettre à profit sa capacité

de renseignement stratégique afin d'anticiper la menace et de comprendre les enjeux à venir dans le domaine numérique. Hissés à un haut niveau de compétence judiciaire et technique, ses agents doivent être aptes à déployer des méthodes d'investigation innovantes dans des domaines inexplorés. Les enquêtes sur les crypto-monnaies et sur le darkweb furent les enjeux des années passées. Une fois démontrée la faisabilité de telles investigations, les unités de recherche de la gendarmerie ont pu métaboliser ces savoirs-faire. Les années à venir consisteront probablement à maîtriser l'Internet des objets (IoT), à faire face aux enjeux du big data et à mettre à profit les potentialités de l'intelligence artificielle.

L'ambition de cette police judiciaire stratégique et exploratoire n'est rendue possible qu'éclairée par le renseignement et la recherche.

Une action opérationnelle guidée par le renseignement et la recherche

Les criminologues s'attachent traditionnellement à décrire le travail de l'enquêteur comme bureaucratique, réactif et routinier (Cf. notamment Greenwood Chaiken et Petersilia 1976 confirmé par une littérature constante recensée par Barlatier 2017). Deux mouvements de politique policière envisagent de faire évoluer ces modes d'action.

En premier lieu, l'intelligence-led policing (ILP) propose le modèle d'une police dont l'activité opérationnelle est orientée en amont par sa connaissance des phénomènes et des populations criminelles (Ratcliffe 2016). Le renseignement devient alors discernement. Il permet au gendarme de contrôler de façon appropriée les lieux de concentration de délinquance (hot spot) et les individus à risque (prolific offenders). Dans cette perspective, le savoir accumulé par les forces de police n'est rien s'il n'est employé en vue de l'action.

La lutte contre la cybercriminalité se prête relativement bien aux pratiques de l'ILP. En lieu et place d'une prise de plainte systématique et judiciairement stérile au niveau d'unités locales démunies face au traitement d'un contentieux de masse pour lesquels elles ne disposent pas des moyens d'action efficients, un système de plate-formes de signalement émerge progressivement. Ce dispositif propose aux victimes de décrire en ligne les faits qu'elles ont subi. Cette démarche n'emporte pas pour autant une ouverture d'enquête systématique. Elle permet, en revanche, de collecter massivement du renseignement, de l'organiser et de l'analyser en vue, le cas échéant, de générer une enquête judiciaire ou de recourir à d'autres mesures de remédiation. En agissant avec discernement, le gendarme espère ainsi agir utile.

En 2018, le SCRC déploiera la plate-forme PERCEVAL destinée au signalement des fraudes en ligne à la carte bancaire qui représentent moins de 10.000 dépôts de plainte chaque année, alors que le phénomène est évalué à 1,9 millions de faits par le secteur bancaire et les e-commerçants. Enrichies par d'autres sources et soumises à un mode de traitement adapté, les informations fournies par les particuliers feront l'objet de rapprochements en vue de la détection de séries criminelles. S'opère ainsi un renversement de logique où le gendarme n'agit plus en réaction des informations du citoyen, mais où le citoyen vient enrichir le savoir du gendarme en vue d'une action pro-active, rationnelle et efficiente.

En second lieu, l'evidence-based policing (EBP) envisage une police guidée par les éléments probants de la recherche (Sherman 1998). Il propose de surmonter l'indifférence réciproque que se portent souvent le policier et le chercheur à partir d'un double constat :

- l'activité policière est un terreau fertile pour la recherche empirique ;
- le savoir généré par celle-ci peut s'avérer, en retour, particulièrement utile au praticien.

Le SCRC pilote une politique de recherche et de développement constituée de deux cercles :

- des projets de court à moyen terme, au plus proches des préoccupations opérationnelles, pilotés par des chercheurs affectés au sein du service ;
- des projets de moyen à long terme, portant sur des concepts et des outils utiles à l'activité d'enquête ou de renseignement, initiés dans le cadre de partenariats avec des centres de recherche publics ou privés.

Dans ce cadre, le groupe R&D du C3N se montre particulièrement dynamique par son appui direct aux enquêteurs (e.g., développement de scripts facilitant le recueil et la gestion de masses importantes de données collectées sur le Web) et le développement d'outils susceptibles d'êtres mis en production au profit d'un public plus large (e.g., applications de veille ou de recherche sur Internet, moyens de recueil et d'analyse des traces numériques, reconnaissance et exploitation d'images par l'intelligence artificielle).

Loin de prétendre à constituer un modèle, l'exemple du SCRC/C3N illustre ainsi une volonté pragmatique de répondre aux enjeux de l'enquête judiciaire dans le cyberespace. Respectant les modes d'action traditionnels de la gendarmerie nationale, son dispositif repose néanmoins sur un nécessaire changement de paradigme et un utile décloisonnement des approches.

Contribution

Réponses des États pour prévenir la cybercriminalité ?

Cécile Doutriaux
Avocate
Membre de la Chaire Cyberdéfense des écoles de Saint-Cyr, France

> « Les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars[26]»

Ces propos illustrent la préoccupation des États face à la cybercriminalité[27] car depuis plus d'une vingtaine d'années, de multiples attaques informatiques sont perpétrées au niveau mondial par des cybercriminels[28].

La menace informatique est protéiforme (hameçonnage[29], rançongiciel[30], sabotage informatique[31], attaque par déni de service[32], par défiguration[33], usurpation d'identité numérique...) et les victimes diversifiées : États, collectivités territoriales, entreprises, particuliers.

Les cyberdélinquants exploitent la rapidité et l'anonymat des technologies modernes pour commettre des infractions et défier les frontières terrestres, les réseaux numériques étant accessibles au niveau planétaire.

Ils ont ainsi la possibilité de commettre des attaques dans un pays où la législation est moins répressive ou inexistante, ce qui rend les poursuites pénales difficiles et les investigations nécessaires à l'interpellation des auteurs complexes.

Ainsi, pour que les infractions commises dans le cyberespace ne demeurent pas impunies, l'action individuelle de chaque État ne suffit pas et tous les pays doivent coopérer pleinement.

Pourtant, si de nombreux moyens ont été mis en place au niveau européen et international, certains s'avèrent plus limités que d'autres, ce qui remet en question leur caractère dissuasif et leur faculté à prévenir la cybercriminalité.

Au niveau international

Plusieurs initiatives ont été prises par les organisations internationales pour prévenir les cyberattaques.

a) L'O.N.U.

L'Organisation des Nations unies[34] a ainsi chargé l'UIT[35] d'élaborer un cadre international pour réglementer le cyberespace.

Un Groupe d'experts gouvernementaux (GGE), nommé par Le secrétaire général de l'ONU, a proposé une série de normes adoptées ensuite par le G20, ce qui a conduit à reconnaître l'applicabilité du droit international au cyberespace, et notamment la Charte des Nations Unies, la Déclaration universelle des droits de l'Homme, le droit des conflits armés et le droit de la responsabilité internationale des États.

En 2010, lors du Forum économique mondial de Davos, l'UIT a suggéré l'adoption d'un traité international sur la cybersécurité, axé autour de trois principes : la mise en place d'une politique de cyberdéfense par État, l'interdiction d'abriter des cybercriminels et le renoncement à toute action offensive contre un autre État. "

La multiplication des SMSI[36] ainsi que des Forum sur la Gouvernance de l'Internet, initiés par l'ONU, a renforcé le dialogue entre les États.

Toutefois, même si les États ont admis le principe de prévention, de coopération et de non-prolifération dans le cyberespace en 2013 et ont adopté des engagements volontaires de « bonne conduite » dans le cyberespace en 2015, ils ne sont pas parvenus à un véritable consensus sur la règlementation relative à l'espace numérique.

En effet, plusieurs États, et notamment les États-Unis, sont réticents lorsqu'il s'agit de renoncer à leur pouvoir régulateur de l'Internet au profit des Nations Unies.

L'ONU reste par conséquent impuissante dans le domaine de la sécurisation cybernétique au niveau mondial, en raison des nombreuses divergences politiques nationales qui limitent la coopération.

b) L'OTAN

Dès 2002, l'0TAN a souhaité renforcer ses défenses contre les cyberattaques et se doter d'une structure spécifique : le centre technique de la capacité OTAN de réaction aux incidents informatiques[37]. Ce centre gère l'ensemble des systèmes d'information de l'OTAN et les cyberattaques perpétrées à son encontre.

En 2008, l'OTAN a également créé un centre d'excellence de cyberdéfense, situé à Tallinn en Estonie, pour préparer les travaux portant sur les enjeux et les perspectives des attaques informatiques tout en organisant des formations, des tests de vulnérabilité et des exercices communs afin de renforcer les capacités de réponse des États.

Au sommet de Varsovie, en 2016, les Alliés de l'OTAN ont pris l'engagement de renforcer et d'améliorer la sécurisation des infrastructures et des réseaux nationaux.

De plus, l'OTAN travaille en partenariat avec l'Union européenne (UE), l'Organisation des Nations Unies (ONU) et l'Organisation pour la sécurité et la coopération en Europe (OSCE) dans un esprit de complémentarité, pour aboutir à une meilleure sécurisation du cyberespace.

Toutefois, malgré les efforts déployés par cette organisation, plusieurs attaques attribuées au groupe Anonymous ont visé l'OTAN en avril 2010, ce qui a eu pour effet de décrédibiliser cette organisation et de démontrer que la sécurité des systèmes informatiques est loin d'être acquise.

Les organisations internationales ayant montré leurs limites en matière de prévention contre les cyberattaques, les États privilégient en réalité les coopérations limitées à un nombre de partenaires plus restreints pour rendre la lutte plus efficace.

Au niveau européen

a) L'E.N.I.S.A.

L'Agence européenne chargée de la sécurité des réseaux et de l'information (E.N.I.S.A.), créée en 2004, est un centre d'expertise en matière de cybersécurité en Europe. Elle aide les États membres à prévenir et à détecter les problèmes de sécurité de l'information et y répondre.

En septembre 2017, la Commission Européenne a décidé de renforcer ses prérogatives. Ainsi, il a été décidé que cette agence deviendra « l'Agence de cybersécurité de l'UE » et que son mandat sera permanent pour aider les États membres, les institutions et les entreprises de l'UE à contrer les cyberattaques.

Une équipe permanente d'intervention en cas d'urgence informatique (CERT-UE) pour les institutions, organes et agences de l'Union européenne, a également été créée afin de répondre de manière coordonnée aux cyberattaques visant les États membres de l'UE.

Cette agence sera aussi chargée de mettre en application de la directive sur la sécurité des réseaux et des systèmes d'information (SRI), adoptée en 2016, pour intensifier la coopération entre les États membres. Elle prévoit l'obligation pour chaque pays de l'UE de désigner une autorité nationale et de se doter d'une stratégie pour lutter contre la cyber-menace.

Il est enfin prévu qu'elle travaillera en étroite collaboration avec les équipes de sécurité informatique des institutions de l'UE et des États membres, mais également qu'elle coopérera avec l'OTAN.

b) Le Conseil de l'Europe

Convention de Budapest sur la cybercriminalité du 23 novembre 2001[38] qui vise à harmoniser les infractions pénales nationales en matière de cybercriminalité entre les États et à mettre en place un régime rapide et efficace de coopération internationale.[39]

Cette Convention a aussi pour but « de rendre plus efficaces les enquêtes et procédures pénales portant sur des infractions en relation avec des systèmes et données informatiques et de permettre la collecte des preuves électroniques d'une infraction pénale ».[40]

Ainsi, un État peut, sur la base de cette convention, obtenir la conservation rapide de données informatiques stockées sur le territoire d'un autre État pour identifier l'agresseur numérique et établir la preuve de ses agissements.

La coopération transfrontière entre les services répressifs des États est réalisée avec l'aide de l'Office européen de police (Europol)[41] et de l'unité de coopération judiciaire de l'Union européenne (Eurojust)[42], lesquels harmonisent leurs pratiques et procèdent à des échanges d'informations en matière d'infractions numériques.

Au niveau opérationnel, les États de l'UE collaborent étroitement avec le Centre européen de lutte contre la cybercriminalité (EC3) créé en 2013 au sein d'Europol et avec Eurojust pour aligner les approches politiques et pratiques des États en matière de lutte contre la cybercriminalité.

Cette coopération entre les États est efficace puisqu'une enquête menée avec le soutien d'Europol et Eurojust, a conduit à l'arrestation d'un groupe de 20 hackers ayant falsifié les courriels des autorités fiscales pour escroquer les clients des banques en Italie et en Roumanie pour un million d'euros le 28 mars 2018.

De plus, le 26 mars 2018, Europol révélait avoir réussi à appréhender en Espagne un groupe criminels qui avait infiltré 100 institutions financières dans 40 pays au moyen de logiciels malveillants Carbanak et Cobaltl[43], après une enquête menée par la police nationale espagnole, avec le soutien d'Europol, du FBI américain, des autorités roumaines, moldaves, biélorusses et taiwanaise et des sociétés privées de cybersécurité.

Conclusion

Le contrôle des technologies de l'information représente un enjeu majeur et de nombreux États sont réticents à l'idée d'abandonner une part de leur souveraineté au profit d'une coopération pleine et entière en matière de lutte contre la cybercriminalité.

Dans un contexte mondialisé de tensions internationales et de retour à un certain protectionnisme, il est difficile d'envisager une coopération internationale renforcée, même si tous les États y gagneraient.

Par conséquent, la solution, pour prévenir plus efficacement la cybercriminalité, est manifestement de privilégier une coopération ponctuelle et limitée à un nombre plus restreint d'États, exclusivement dans un contexte criminel et économique, en dehors de toutes considérations politiques.

Une autre solution consisterait également à développer des solutions techniques nationales, telles que le déréférencement et l'indisponibilité des réseaux, ce que plusieurs Etats ont d'ores et déjà mis en œuvre.

Contribution

Le rôle de l'élaboration d'une stratégie de cybersécurité dans la mise en place d'un cadre de lutte contre la cybercriminalité[44]

Belisario Contreras
Responsable de programme cybersecurité
Organisation des États Américains, États-Unis

Kerry-Ann Barrett
Spécialiste en politique de cybersécurité
Organisation des États Américains, États-Unis

Introduction

Avec l'augmentation de la connectivité à internet, le monde n'a jamais été aussi petit. Le tout internet a changé la façon dont les gens, les entreprises et les gouvernements interagissent les uns avec les autres. Avec plus de 3 milliards d'utilisateurs d'internet, représentant un peu plus de la moitié de la population mondiale et rien qu'en Amérique latine et dans les Caraïbes environ 417 940 160 internautes[45], de plus en plus de gens prennent conscience tant des avantages que des risques d'être en ligne.

L'Amérique latine et les Caraïbes représentent actuellement l'une des populations qui, sur internet, croît le plus rapidement dans le monde, ce qui entraine un certain nombre de défis importants en matière de cybersécurité, notamment concernant la protection des infrastructures critiques et l'augmentation des activités malveillantes menées sur le web. Avec cette augmentation de l'utilisation d'internet, la différence entre le monde réel et le monde numérique disparaît rapidement. En conséquence, les cyber-infractions à motivation criminelle sont devenues une menace considérable et préjudiciable, qui exige que les gouvernements, les organisations internationales, le secteur privé et la société civile travaillent ensemble en reconnaissant que les menaces à la cybersécurité concernent tout un chacun.

Cybersécurité et cybercrime

Le lien entre cybersécurité et cybercrime est parfois flou, et il arrive que les praticiens en cybersécurité et ceux qui travaillent sur la cybercriminalité au sein du système de justice pénale délibèrent afin de déterminer où le rôle de l'un s'achève et l'autre commence. Le présent article part du principe que la cybersécurité et la cybercriminalité, bien qu'elles soient étroitement liées, sont des disciplines distinctes. En outre, il est proposé que les mesures de cybersécurité puissent fournir un cadre qui contribue à l'atténuation de la cybercriminalité et/ou à fournir des mécanismes de résolution de ses effets.

La cybercriminalité peut être définie comme l'utilisation malveillante d'internet ou de systèmes informatiques pour commettre un crime, ou la commission d'un crime dirigé contre un système informatique. La cybersécurité désigne quant à elle les mesures pratiques qui sont prises dans le but de s'assurer que les systèmes de communication de l'information restent opérationnels, sans interférence. Dans une perspective plus large, cela inclut non seulement les mesures prises pour maintenir les systèmes disponibles et sans interférence, mais également un écosystème plus large qui touche l'application de mesures techniques telles que les lois, les règlements, les politiques et les pratiques. Cet écosystème plus vaste fournit le cadre permettant aux acteurs nationaux, régionaux et internationaux d'identifier et de réagir à un incident cybernétique, et de prendre davantage de mesures s'il est identifié comme un crime. En tant que telle, la cybersécurité implique également une approche multipartite pour développer et mettre en œuvre ces mesures de protection des réseaux.

Pour lutter contre la cybercriminalité, de nombreux éléments contingents doivent être instaurés, comme le requiert la conduite d'enquêtes, de poursuites, et un partage des preuves impliquant souvent d'autres États et acteurs étatiques. Certaines des questions qu'il convient de se poser sont les suivantes : existe-t-il une législation en place qui identifie les éléments du crime ? La législation exige-t-elle qu'il y ait une victime ou qu'il soit prouvé que des dommages ont été causés ? Le tribunal est-il compétent pour juger l'accusé (en particulier lorsque le crime est commis dans une juridiction mais que l'auteur présumé réside dans une autre) ? De plus, les enquêteurs et les procureurs possèdent-ils les capacités nécessaires pour enquêter et poursuivre l'affaire ?

Les différences entre cybercriminalité et cybersécurité sont également visibles chez les personnes qui travaillent dans ces domaines. Il est préférable de confier les enquêtes et les poursuites en matière de cybercriminalité au secteur de la justice pénale – services de détection et de répression, analystes, procureurs, magistrats et juges. En revanche, la cybersécurité est en grande partie assurée par des spécialistes des technologies de l'information et des communications (TIC) – tels que les développeurs de logiciels, les ingénieurs réseaux et systèmes, et les analystes des risques cybernétiques – et par les internautes avertis.

Lorsqu'ils formulent une stratégie de cybersécurité, les décideurs doivent reconnaître ces distinctions, c'est-à-dire entre la lutte contre la cybercriminalité et la gestion de la cybersécurité. Ils doivent également comprendre comment la cybercriminalité s'inscrit dans l'écosystème plus large de la cybersécurité.

L'écosystème plus large de la cybersécurité

En tenant compte de la distinction entre la cybersécurité et la cybercriminalité, il faut prendre en considération les autres domaines qui ont un impact sur la cybercriminalité et son enquête. Il s'agit notamment des efforts déployés aux niveaux national et international pour mettre en œuvre des mesures qui, en fin de compte, ne peuvent conduire qu'à l'amélioration de la coopération d'État à État au cours des enquêtes. C'est ce que nous décrivons comme l'écosystème au sens large (voir Fig. 1), qui facilite

les enquêtes et les poursuites en matière de cybercriminalité, et qui comprend :

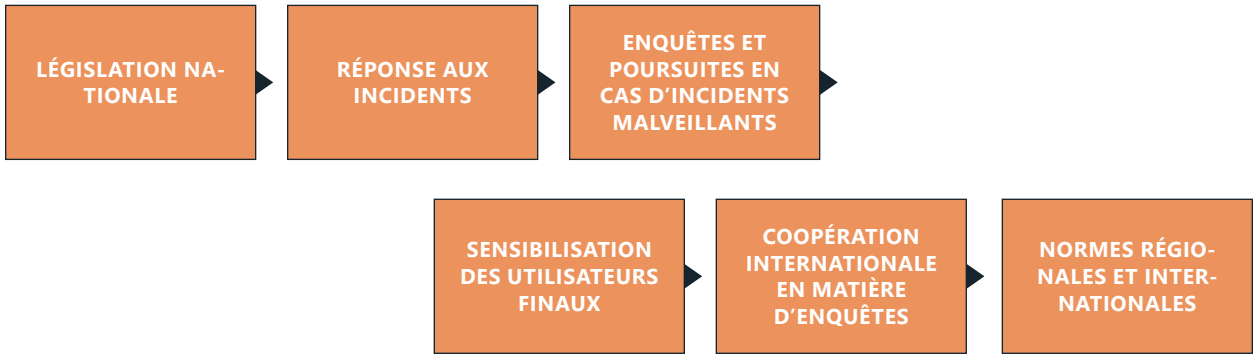
1. **La législation nationale** qui, une fois en vigueur, fournit la base sur laquelle les cybercrimes peuvent faire l'objet d'enquêtes et de poursuites. Elle assure également, entre autres, des pouvoirs d'enquête et des outils à l'intention des autorités chargées de l'application de la loi ;
2. **La réponse aux incidents** facilite la récupération et la continuité des réseaux. Toutefois, s'il y a lieu, les éléments de preuve recueillis peuvent également être utilisés pour les enquêtes et les poursuites de cybercrimes dans le cadre de lignes directrices et de procédures bien établies ;
3. **Les enquêtes et les poursuites relatives aux incidents d'origine malveillante** contribuent à assurer la sécurité publique en décourageant, en identifiant et en minimisant les acteurs malveillants en ligne et en renforçant la confiance des utilisateurs finaux dans l'utilisation des services en ligne;
4. **La sensibilisation des utilisateurs finaux** fournit les outils dont les citoyens ont besoin pour ne pas être victimes d'une cybercriminalité et, s'ils le sont, quelles mesures ils pourraient prendre et à qui et où le signaler ;
5. **La coopération internationale** comprend non seulement les mécanismes internationaux de cybersécurité, mais également les mécanismes de lutte contre la cybercriminalité, comme la GEI de l'ONUDC sur la cybercriminalité[46] et la convention de Budapest[47], qui vise à lutter contre la cybercriminalité. Ceux-ci contribuent également à l'établissement d'une réciprocité et des enquêtes transfrontalières ;
6. **Les normes régionales et internationales**[48] contribuent au débat plus large sur la coopération d'État à État, et peuvent fournir aux États des orientations sur leur comportement dans le traitement des questions liées à la cybersécurité et à la cybercriminalité.

C'est dans ce contexte que nous aimerions souligner les moyens très pratiques par lesquels l'élaboration d'une stratégie nationale de cybersécurité peut appuyer le développement d'un cadre solide pour lutter contre la cybercriminalité. Une stratégie nationale de cybersécurité (SNC) est un plan d'action conçu pour améliorer la sécurité et la résilience des infrastructures et des services nationaux. Il s'agit d'une approche verticale de haut niveau de la cybersécurité, qui établit une série de priorités et d'objectifs nationaux à atteindre dans un délai précis[49]. Afin d'aborder la question de manière holistique, il est recommandé que les pays considèrent leur stratégie nationale de cybersécurité comme un cadre qui peut soutenir les efforts d'un pays pour protéger les ordinateurs, les réseaux et les données de son gouvernement, de ses entreprises et de sa population. Une composante de toute stratégie devrait porter sur la prévention, les enquêtes et les poursuites en matière de cybercriminalité. Les domaines à prendre en considération sont les suivants :

1) La coordination nationale réduit les réponses ad hoc aux cyberincidents et la duplication des efforts des organismes responsables à l'intérieur d'un pays et devrait inclure :
   a. la définition des rôles et responsabilités des organismes responsables et des parties prenantes nationales, y compris l'autorité nationale de coordination, les autorités chargées de la cybersécurité (comme les CSIRT, les ministères des TIC, etc.) et les autorités du secteur de la justice pénale (tels que les forces de l'ordre, les procureurs, les magistrats, les juges) ;
   b. l'identification des points de contact pour la coordination ;
   c. la coordination des parties prenantes nationales pour l'élaboration de la politique et pour la réponse aux incidents.

2) L'allocation de ressources stratégiques et adéquates garantit qu'il existe la capacité technique nécessaire pour réagir de manière appropriée aux cyber-menaces, et devrait inclure :

Figure 4.1. **Écosystème élargi en cybersécurité**



Source : élaboration personnelle

a. un budget alloué aux efforts menés en matière de cybersécurité ;
b. une répartition adéquate du personnel ;
c. une formation continue des responsables de la cybersécurité ;
d. des experts disponibles 24 heures sur 24 pour la coordination des interventions en cas d'incident ;
e. des experts dédiés aux enquêtes sur la cybercriminalité.

3) Un cadre législatif qui s'attaque à la cybercriminalité et fournit les outils nécessaires à l'application de la loi :

a. une législation qui criminalise les cybercrimes ;
b. des mesures qui appuient la capacité de recueillir, préserver et de partager les données probantes.

4) La coopération et la collaboration internationales qui tiennent compte de la nature sans frontières des crimes liés à la cybercriminalité et qui inclut :

a. une participation au dialogue international sur les problématiques cyber (comme la cybercriminalité) ;
b. une disposition de « double incrimination » en droit interne ;
c. la conclusion d'accords bilatéraux et multilatéraux d'entraide juridique (comme par exemple le Traité de l'OEA[50]).

Élaboration de stratégies nationales de cybersécurité

Compte tenu de ce qui précède et des menaces en constante évolution qui affectent le cyberespace, chaque pays peut considérer les domaines identifiés dans la section précédente et trouver une approche stratégique adaptée à ses besoins. Les meilleures stratégies sont celles qui favorisent une étude adéquate des risques et des menaces, tiennent compte des mesures d'atténuation des risques, sont adaptées aux besoins nationaux individuels et font participer toutes les parties prenantes concernées au processus de prise de décision et de mise en œuvre. À cet égard, il est reconnu qu'il est nécessaire de disposer d'une directive nationale de haut niveau sur la cybersécurité, assortie d'un plan d'action stratégique pour atteindre les objectifs de celle-ci. Le processus d'élaboration devrait toujours impliquer l'ensemble des parties prenantes concernées (le gouvernement – y compris les forces de l'ordre –, le secteur privé, la société civile, le monde universitaire et autres), et aboutir à un document au champ d'application bien défini, qui traite des menaces nationales spécifiques et énonce clairement les buts, les objectifs ainsi que les étapes nécessaires pour les atteindre, à la lumière de priorités identifiées. Concernant sa mise en œuvre, une fois approuvés, les coûts associés et les ressources disponibles doivent être identifiés et inclus dans les budgets des organismes ou entités chargés de son exécution.

Il convient de noter que le Secrétariat du Comité interaméricain contre le terrorisme (CICTE) du Secrétariat général de l'OEA (OEA/GS), par le biais de son programme de cybersécurité, travaille depuis plus d'une décennie avec les États-membres pour renforcer les capacités nationales de cybersécurité dans le cadre de la mise en œuvre de la Stratégie globale interaméricaine de cybersécurité, adoptée par les États-membres de l'OEA en 2004. En Amérique latine et dans les Caraïbes, l'importance d'avoir une cybersécurité nationale est de plus en plus évidente, plusieurs pays ayant récemment publié des stratégies dans le domaine : Colombie (2011 et 2016)[51], Panama (2013)[52], Trinité-et-Tobago (2013)[53], Jamaïque (2015)[54], Chili (2017), Paraguay (2017) et Costa Rica (2017)[55].

Conclusion

L'interaction entre cybersécurité et cybercriminalité ne peut que bénéficier de l'élaboration d'une stratégie nationale de cybersécurité. Les stratégies nationales de cybersécurité établissent un cadre dans lequel tous les acteurs peuvent travailler ensemble, y compris sur la définition des rôles et des responsabilités. Le processus d'élaboration et de mise en œuvre exige l'engagement de hauts fonctionnaires, ainsi que la coopération et la participation de diverses parties prenantes nationales. La mise en œuvre des objectifs définis dans le présent document aidera un pays à améliorer ses capacités en matière de cybersécurité et, en fin de compte, à faire preuve d'une plus grande souplesse dans la lutte contre les cybercrimes lorsqu'ils se produisent.

Notes

24 Voir par exemple la différence entre les approches sécuritaires de contre-terrorisme et celles de prévention de la radicalisation dans l'introduction de notre étude « Comment prévenir la radicalisation : une revue systématique » (CIPC, 2015).

25 Étant donné la difficulté à accorder une définition à la cybercriminalité, le terme « cybercriminalité » dans ce texte inclura également les concepts de criminalité informatique ou encore de criminalité dans le cyberespace.

26 Pour Jean-Claude Juncker, président de la Commission européenne (discours sur l'état de l'Union, septembre 2017).

27 La cybercriminalité désigne « tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique ».

28 Au niveau mondial on évalue l'impact économique des attaques à 400 milliards d'euros par an et en 2016, 80% des entreprises européennes ont connu un incident informatique selon la Commission Européenne.

29 L'hameçonnage ou phishing est une technique dont l'objectif est d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel.

30 Les rançongiciels sont des programmes informatiques malveillants (ex : Locky, TeslaCrypt, Cryptolocker, WannaCry etc.) chiffrant des données pour les rendre indisponibles.

31 Le sabotage informatique est le fait de rendre inopérant tout ou partie d'un système d'information via une attaque informatique.

32 Le déni de service a pour effet de rendre un site internet indisponible par l'envoi de multiples requêtes.

33 L'Attaque par défiguration modifie l'apparence ou le contenu d'un site internet et altère l'intégrité des données.

34 L'Organisation des Nations unies (ONU) est une organisation internationale créée le 24 octobre 1945 qui comprend 193 Etats membres, ayant pour objectifs de faciliter la coopération en droit international, la sécurité internationale, le développement économique, le progrès social, pour favoriser la paix mondiale.

35 L'Union internationale des télécommunications (UIT) est l'agence des Nations unies chargée de développer les technologies de l'information et de la communication entre les États et le secteur privé.

36 Le Sommet mondial sur la société de l'information est un forum mondial organisé par l'Union internationale des télécommunications, une agence de l'Organisation des Nations unies.

37 « Nato computer incident response capability » ou NCIRC.

38 Ouverte à la signature le 23 Novembre 2001, à l'occasion de la Conférence internationale sur la Cybercriminalité, la Convention de Budapest est entrée en vigueur le ler Juillet 2004, et constitue le premier traité international sur les infractions pénales commises via l'Internet et d'autres réseaux informatique.

39 Source : Conseil de l'Europe, Rapport explicatif de la Convention sur la cybercriminalité, Budapest, [2001],STE n°185, p. 4. Au 25/03/2018, 56 Etats ont adhéré à la Convention de Budapest. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=FRE.

40 Conseil de l'Europe, « Convention sur la cybercriminalité », op. cit., Ch. II, Titre 4, art. 10.

41 Europol (European Union Law Enforcement Organisation) est l'Office européen de police créé en 1995 pour faciliter les opérations de lutte contre la grande criminalité internationale avec 28 États membres et plusieurs pays partenaires non membres de l'Union européenne. Il facilite l'échange de renseignements entre polices nationales en matière de cybercriminalité.

42 Eurojust est un organe de l'Union européenne institué en 2002 afin d'améliorer la coordination des enquêtes et des poursuites judiciaires entre les Etats membres de l'Union chargées de traiter les affaires de criminalité organisée transfrontalière.

43 Les criminels enverraient aux employés de la banque des courriels de phishing avec une pièce jointe malveillante imitant des compagnies légitimes. Une fois téléchargé, le logiciel malveillant permettait aux criminels de contrôler à distance les machines infectées des victimes, leur donnant accès au réseau bancaire interne et infectant les serveurs contrôlant les guichets automatiques.

44 AVERTISSEMENT : les opinions exprimées dans ce document ne reflètent pas nécessairement les vues du Secrétariat général de l'Organisation des États américains ou des gouvernements de ses États-membres, mais représentent celle des auteurs.

45 Utilisation d'internet dans le monde et statistiques démographiques – Décembre 2017 – Mis à jour, consulté à l'adresse suivante : https://www.internetworldstats.com/stats10.htm.

46 Réunion intergouvernementale d'experts à composition non limitée sur la cybercriminalité - https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-meeting-on-cybercrime.html.

47 Convention sur la cybercriminalité - https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

48 Par exemple, au niveau régional, l'Organisation des Etats américains a adopté la Stratégie interaméricaine globale de lutte contre les menaces à la cybersécurité : une approche multidimensionnelle et multidisciplinaire pour créer une culture de la cybersécurité, dans laquelle les Etats membres ont convenu de coordonner leurs efforts pour renforcer la cybersécurité (http://www.oas.org/en/sms/cicte/Documents/OAS_AG/AG-RES_2004_(XXXIV-O-04)_EN.pdf). Au niveau international, le rapport consensuel du groupe d'experts gouvernementaux des Nations Unies sur le développement dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, adopté en juillet 2015, recommande aux Etats d'envisager la norme suivante de comportement responsable : « Les Etats devraient réfléchir à la meilleure façon de coopérer pour échanger des informations, s'entraider, poursuivre les terroristes et les criminels qui utilisent les TIC et mettre en œuvre d'autres mesures de coopération pour faire face à ce menaces ». Rapport, paragraphe 13(d) - http://undocs.org/A/70/174.

49 ENISA- https://www.enisa.europa.eu/topics/national-cyber-security-strategies

50 http://www.oas.org/juridico/english/treaties/a-55.html

51 https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

52 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/panama-national-cybersecurity-strategy

53 https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf

54 https://www.sites.oas.org/cyber/Documents/Jamaica%20National%20Cyber%20Security%20Strategy.pdf

55 http://ciberseguridad.interior.gob.cl/media/2017/04/NCSP-ENG.pdf

Références

Chapitre 4 : Quelle prévention pour la cybercriminalité ?

ASEAN. (2017). Declaration to Prevent and Combat Cybercrime, adopted by the Heads of State/Government of the Association of Southeast Asian Nations, in Manila, the Philippines, 13 November 2017, available at: http://www.asean2017.ph/wp-content/uploads/13-ASEAN-Declaration-to-Combat-Cybercrime.pdf [accessed 23 April 2018].

Bayer, M. D. (2010). The blue planet: Informal international police networks and national intelligence. Washington, DC: United States Department of Defense, National Defense Intelligence College Press.

Berguer, A. (2015). Patchin J. W., Hinduja S., Cyberbullying Prevention and Response, Expert Perspectives. New York, Routledge, 2012, 204 pages. Cyberviolence et école, 33.

Bossler, A. M., & Holt, T. J. (2016). Cybercrime in Progress: Theory and prevention of technology-enabled offenses. London: Routledge. ISBN: 9781317688990

Brantingham, P., & Brantingham, P. (2008). Crime Pattern Theory. In Environmental Criminology and Crime Analysis. London: Willan.

Brinkerhoff, D. W., & Brinkerhoff, J. M. (2011). Public–private partnerships: Perspectives on purposes, publicness, and good governance. Public Administration and Development, 31(1), 2-14. https://doi.org/10.1002/pad.584

Broadhurst, R. G. (2005). Workshop 6: Measures to Combat Computer Related Crime. In 11th UN Congress on Crime Prevention and Criminal Justice (p. 1-12). Bangkok: Commission on Crime Prevention and Criminal Justice.

CARICOM (2013) Crime and Security Strategy: Securing the Region. Adopted at the Twenty-Fourth Inter-Sessional Meeting of the Conference of Heads of Government of CARICOM, 18-19 February 2013, Port-au-Prince, Republic of Haiti, available at: https://www.state.gov/documents/organization/210844.pdf [accessed 19 April 2018].

CCPCJ. (2010). Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador: United Nations Congress on Crime Prevention and Criminal Justice.

Chaudhry, P. E., Chaudhry, S. S., Stumpf, S. A., & Sudler, H. (2011). Piracy in cyber space: consumer complicity, pirates and enterprise enforcement. Enterprise Information Systems, 5(2), 255-271. https://doi.org/10.1080/17517575.2010.524942

Chisholm, J. F. (2014). Review of the Status of Cyberbullying and Cyberbullying Prevention. Journal of Information Systems Education, 25(1).

CIPC. (2015). Comment prévenir la radicalisation: une revue systématique. Montréal: Centre International pour la prévention de la Criminalité. Consulté à l'adresse http://www.crime-prevention-intl.org/fr/publications/report/report/article/etude-comparative-internationale-sur-la-prevention-de-la-radicalisation-1.html

Clarke, R. V., & Cornish, D. B. (1985). Modeling Offenders Decisions: A Framework for Research and Policy. Crime and Justice: An Annual Review of Research, 6, 313.

Cobb, S. (2014). The main problem with Situational Crime Prevention is that it fails to address the root causes of crime : a critical discussion. University of Leicester, available at: http://cobbsblog.com/sc/cybercrime-situational-crime-prevention.pdf [accessed 5 April 2018].

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rates: A Routine Activity Approach. American Sociological Review, (44), 588-608.

Collier, A., & Nigam, H. (2010). Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group. Washington: Online Safety and Technology Working Group.

Commonwealth Secretariat. (2014). Report of the Commonwealth Working Group of Experts on Cybercrime. Commonwealth Law Bulletin.

Conseil de l'Europe (2001) Convention on Cybercrime, European Series Treaty, Pub. L. No. 185, adopted in Budapest, 23.XI.2001, available at: https://rm.coe.int/1680081561 [accessed 10 April 2018].

Conseil de l'Europe (2004) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Strasbourg: European Treaty Series – No. 189

Cornish, D., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions. Crime prevention studies, 16, 41-96.

Crawford, A. (1999) The Genesis of the Partnership Approach and Appeals to Community in Crime Control. Oxford: Oxford University Press.

Dale, J., Russel, R., & Wolke, D. (2014). Intervening in primary care against childhood bullying: an increasingly pressing public health need. Journal of the Royal Society of Medicine, 107(6), 219-223.

Dashora, K. (2011). Cyber Crime in the Society: Problems and Preventions. Journal of Alternative Perspectives in the Social Sciences, 3(1), 240-259.

Deibert, R., & Crete-Nishihata, M. (2002). Global Governance and the Spread of Cyberspace Controls. Global Governance, 18, 339-361.

Dunn, S., Lalonde, J. S., & Bailey, J. (2017). Girlhood Studies, 10(2), 80-96. https://doi.org/10.3167/ghs.2017.100207

Dupont, B. (2016). La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale. Cultures & Conflits, (102), 95-120.

ESCWA. (2015). Policy Recommendations on Cybersafety and Combating Cybercrime in the Arab Region. New York: Economic and Social Commission for Western Asia.

Espelage, D. L., & Hong, J. S. (2016). Cyberbullying Prevention and Intervention Efforts: Current Knowledge and Future Directions. The Canadian Journal of Psychiatry, 62(6), 374-380.

Eskola, M. (2012) From Risk Society to Network Security: Preventing Cybercrimes in the 21st Century. Journal of Applied Security Research, 7:1, 122-150.

EUCPN. (2017). Cyber Safety: A theorical insight (Theorical Paper). Brussels: European Crime Prevention Network.

Fratianni, M., & Savona, P. (2005). New Perspectives on Global Governance: Why America Needs the G8. Routledge.

Ghernaouti, S. (2013). Cyber Power: Crime, conflict and security in cyberspace. Boca Raton: Taylor & Francis Group. ISBN : 9781466573048.

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. Law, Innovation and Technology, 9(2), 159-189.

Herring, S. (2002). Cyber Violence: Recognizing and Resisting Abuse in Online Environments. Asian Women, 14 (Summer), 187-212.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. Social Science Computer Review, 31, 165-177.

Hutchings, J., & Clarkson, S. (2015). Introducing and piloting the KiVa bullying prevention programme in the UK. Educational & Child Psychology, 32(1).

ICMEC & UNICEF. (2016). Online Child Sexual Abuse and Exploitation: Guidelines for the Adoption of National Legislation in Latin America. Alexandria: International Centre for Missing & Exploited Children and the United Nations Children's Fund, Latin America and Caribbean Regional Office.

IHE. (2010). Sexual Exploitation of Children and Youth Over the Internet: A Rapid Review of the Scientific Literature. Edmonton: Institute of Health Economics - Alberta Canada.

Jamil, Z. (2014). Cybercrime Model Laws. Discussion paper prepared for the Cybercrime Convention Committee (T-CY). Strasbourg: Council of Europe.

Jones, L. M., Mitchell, K. J., & Walsh, W. A. (2014). A Content Analysis of Youth Internet Safety Programs: Are Effective Prevention Strategies Being Used? Crime Against Children Research Center.

Kigler, M. (2016). Interventions, Policies, and Future Research Directions in Cybercrime. In The Wiley Handbook on the Psychology of Violence (1st éd., p. 604-622). San Antonio: John Wiley & Sons.

Koops, B.-J. (2010). The Internet and its Opportunities for Cybercrime (SSRN Scholarly Paper No. ID 1738223). Rochester, NY: Social Science Research Network. Consulté à l'adresse https://papers.ssrn.com/abstract=1738223

Kowalski, R. M., Limber, S. P., & Agoston, P. W. (2008). Cyber Bullying: Bullying in the Digital Age. Malden: Blackwell Publishing.

Krawczyk, M., Kukla-Gryz, A., & Tyrowicz, J. (2015). Digital Piracy and the Perception of price Fairness. Varsovie: Université de Varsovie.

Leukfeldt, E. R., & Majid, Y. (2016). Applying Routine Activity Theory to Cybercrime: A theorical and Empirical Analysis. Deviant Behavior, 3(37), 263-280.

Lewis, S., & Lewis, D. A. (2011). Digitalizing Crime Prevention Theories: How technology Affects Victim and Offender Behavior. International Journal of Criminology and Sociological Theory, 4(2), 756-769.

LIBE. (2015). Combatting child sexual abuse online. Luxembourg: European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE).

MacKinnon, C. A. (2005). Pornography as Trafficking. Michigan Journal of International Law, 26(4).

Marcum, C. D. (2013). Cyber Crime. Aspen College Series. ISBN: 9781454820338.

Moreno, M. A., & Vaillancourt, T. (2016). The Role of Health Care Providers in Cyberbullying. The Canadian Journal of Psychiatry, 62(6), 364-367.

Nhan, J., & Huey, L. (2008). Policing through nodes, clusters and bandwidth. In S. Leman-Langlois (Éd.), Technocrime: Technology, Crime and Social Control. Portland, OR: Willan.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. International Journal of Cyber Criminology, 5(1), 773-793.

Notar, C. E., Padgett, S., & Roden, J. (2013). Cyberbullying: Resources for Intervention and Prevention. Universal Journal of Educational Research, 1(3), 133-145.

OEA. (2004) Estrategia Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética, aprobada en la cuarta sesión plenaria, celebrada el 8 de junio de 2004, en Washington, available at:

https://www.sites.oas.org/cyber/Documents/Estrategia-seguridad-cibernetica-resolucion.pdf [accessed 15 April 2018].

OMS. (2002). Rapport mondial sur la violence et la santé. Genève: Organisation mondiale de la santé.

ONUDC. (2010). Principes directeurs applicables à la prévention du crime: Manuel d'application pratique. Vienne : Office des Nations Unies contre la drogue et le crime.

ONUDC. (2013). Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face. Vienne : Office des Nations Unies contre la drogue et le crime.

ONUDC. (2015). Déclaration de Doha sur l'intégration de la prévention de la criminalité et la justice pénale dans le programme d'action plus large de l'Organisation des Nations Unies visant à faire face aux problèmes sociaux et économiques et à promouvoir l'État de droit aux niveaux national et international et la participation du public. Vienne : Office des Nations Unies contre la drogue et le crime.

Ortega-Ruiz, R., Del Rey, R., & Casas, J. A. (2012). Knowing, Building and Living Together on Internet and Social Networks: The ConRed Cyberbullying Prevention Program. International Journal of Conflict and Violence, 6(2).

Pelser, E. (2002). Crime prevention partnerships: Lessons from pratice. Pretoria: Institute for Security Studies. ISBN: 1919913076 9781919913070.

Pereira, B. (2016). La lutte contre la cybercriminalité: de l'abondance de la norme à sa perfectibilité. Revue internationale de droit économique, 387-409.

Poonia, A. S., Bhardwaj, A., & Dangayach, G. S. (2011). Cyber Crime: Practices and Policies for its Prevention. The First International Conference on Interdisciplinary Research and Development.

Prates, F., Gaudreau, F., & Dupont, B. (2013). La cybercriminalité: état des lieux et perspectives d'avenir. Institut Canadien d'Études Juridiques Supérieures, 415-442.

Prevention Institute. (2009). Transforming Communities to Prevent Child Sexual Abuse and Exploitation: A Primary Prevention Approach. Oakland: Prevention Institute.

Quéro, Y.-C., & Dupont, B. (2017). Nodal governance: toward a better understanding of node relationships in local security governance. Policing and Society, 0(0), 1-19. https://doi.org/10.1080/10439463.2017.1391808

Reyns, B. W., Randa, R., & Henson, R. (2016). Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. Crime Prevention and Community Safety, 18(1), 33-59.

Rivière, J., & Lucas, D. (2008). Criminalité et internet, une arnaque à bon marché. Sécurité globale, (6), 67-82.

Rosenbaum, D. P., & Schuck, A. M. (2012). Comprehensive Community Partnership for Preventing Crime. In The Oxford Handbook of Crime Prevention (Oxford Handbooks Online). Oxford: David P Farrington et Brandon C. Welsh. ISBN: 9780195398823.

Seger, A. (2012). Cybercrime strategies (Discussion paper). Strasbourg: Conseil de l'Europe.

Simantiri, N. L. (2017). Abus et exploitation sexuels des enfanst en ligne: Formes actuelles et bonnes pratiques pour la prévention et la protetion. Luxembourg: ECPAT France & Luxembourg.

Slonje, R., Smith, P. K., & Frisen, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in Human Behaviour, (29), 26-32.

Smith, R. G., Cheung, C.-C., & Chung-Lau, L.-Y. (2015). Cybercrime Risks and Responses: Eastern and Western Perspectives. New York: Palgrave Macmillan. ISBN : 9781137474162.

Smyth, S. M., & Carleton, R. (2011). Évaluation de l'ampleur de la cyberfraude : document de travail sur les méthodes potentielles et les sources de données. Ottawa: Division de la recherche et de la coordination nationale sur le crime organisé, Secteur de la police et de l'application de la loi, Sécurité publique Canada.

Snakenborg, J., Van Acker, R., & Gable, R. A. (2011). Cyberbullying: Prevention and Intervention to Protect Our Children and Youth. Prventing School Failure: Alternative Education for Children and Youth, 55(2), 88-95.

Spiel, C., Wagner, S., et Strohmeier, D. (2012) Violence Prevention in Austrian Schools: Implementation and Evaluation of a National Strategy. Vienna: International Journal of Conflict and Violence: Vol. 6 (2), p.176-186.

Sun, C., Bridges, A., Johnson, J. A., & Ezzell, M. B. (2016). Pornography and the Male Sexual Script: An Analysis of Consumption and Sexual Relations. Archives of Sexual Behaviour, 45(4), 983-994.

Sutton, A., Cherney, A., & White, R. (2008). Crime Prevention: Principles, perspectives and practices. Cambridge: Cambridge University Press.

Tilley, N. (2005). Handbook of Crime Prevention and Community Safety. Portland: Willan Publishing. ISBN: 1843921464.

Tilley, N., & Sidebottom, A. (2017). Handbook of Crime Prevention and Community Safety (2e éd.). New York: Routledge. ISBN : 9781138851054.

Tonry, M., & Farrington, D. P. (1995). Strategic Approaches to

Crime Prevention. Crime and Justice, 19, 1-20.

Tremblay, R. E., & Craig, W. M. (1995). Developmental Crime Prevention. The University of Chicago Press Journals, 19, 151-236.

UIT. (2014). Comprendre la cybercriminalité : Phénomène, difficultés et réponses juridiques. Genève : Union internationale des télécommunications.

Union africaine (2014) Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel. Adopté par la 23ème Session Ordinaire de la Conférence de l'Union à Malabo, le 27 juin 2014, available at: https://www.afapdp.org/wp-content/uploads/2014/07/CONV-UA-CYBER-PDP-2014.pdf, [accessed 10 April 2018]

Wall, D. S. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. Police Practice & Research: An International Journal, 8(2), 183-205.

Welsh, B. C., & Farrington, D. P. (2010). The Future of Crime Prevention: Developmental and Situational Strategies. National Institute for Justice.

West, J. (2014). Cyber-Violence against Women. Vancouver, Canada: Battered Women's Support Service.

Williams, M. L., & Levi, M. (2017). Cybercrime prevention. In Handbook of crime prevention and community safety (2e éd., p. 454-469). London; New York: Routledge, Taylor & Francis Group.

Williams, M. & Pearson, O. (2016) Hate Crime and Bullying in the Age of Social Media – Conference report. Cardiff: Cardiff University.

Contribution

Chercher à répondre aux enjeux de la criminalité numérique

Barlatier, J. (2017). Management de l'enquête et ingénierie judiciaire, recherche relative à l'évaluation des processus d'investigation criminelle (Thèse de doctorat). Université de Lausanne, École des sciences criminelles. doi: 10.13140/RG.2.2.31577.42089

Chaiken, J.M., Greenwood, P., Petersilia, J. (1976). The criminal Investigation Process. A Summary Report. The Rand Paper Series. Santa Monica: The Rand Corporation.

Ratcliffe, J. H. (2016). Intelligence-led policing (2nde éd.). New York : Routledge.

Sherman, L. (1998). Evidence-based policing. Police Foundation


Security

CHAPITRE 5

LES PARTENARIATS PUBLIC-PRIVÉ EN PRÉVENTION DE LA CYBERCRIMINALITÉ

Ce cinquième et dernier chapitre aborde la question des partenariats public-privé en cybersécurité, et plus spécifiquement la manière dont ils abordent la prévention de la cybercriminalité. En guise d'introduction à la thématique, la première partie a pour objet de définir en quoi consiste un partenariat public-privé, pour ensuite s'attarder sur son émergence en prévention de la criminalité. La seconde partie dresse un portrait des partenariats public-privé en prévention de la cybercriminalité. Une description des acteurs impliqués dans ces partenariats est présentée, suivie des approches de mise en œuvre et de développement des partenariats, ainsi que leurs composantes. La troisième partie présente un aperçu de partenariats public-privé internationaux et stratégies nationales axés sur la prévention de la cybercriminalité. La quatrième partie se rapporte aux principaux enjeux rencontrés dans le cadre de ces partenariats, et pour conclure la cinquième partie présentent quelques recommandations.

Introduction

Depuis la fin du vingtième siècle, le secteur privé a commencé à jouer un rôle de plus en plus prédominant dans plusieurs secteurs en lien avec la sécurité nationale, notamment la protection des infrastructures critiques, la cybersécurité, la sécurité des ports et la gestion de l'énergie (Busch & Givens, 2012). Une des raisons de cette importance accrue du rôle du secteur privé dans ces domaines sont les développements technologiques, qui ont permis d'intensifier deux tendances : une internationalisation et une privatisation croissantes. Ces deux tendances diminuent l'importance de l'État et ont toutes deux des implications pour la sécurité (Dunn Cavelty & Brunner, 2007). L'importance croissante du secteur privé a donc favorisé la prolifération de partenariats public-privé, impliquant une collaboration accrue entre les deux secteurs (Busch & Givens, 2012).

Toutefois, un enjeu important est le fait qu'assurer la sécurité des citoyennes et citoyens demeure une des tâches fondamentales du gouvernement. En effet, l'État tel qu'il est perçu aujourd'hui est souvent considéré comme étant responsable de l'octroi de services de sécurité, tout comme la sécurité est considérée comme étant sa plus importante responsabilité (Etzioni, 2017). Octroyer une quelconque responsabilité en ce domaine au secteur privé peut donc s'avérer une opération très délicate (Dunn Cavelty & Suter, 2009).

En parallèle, comme nous allons le voir, le secteur privé est, depuis les années 1980, de plus en plus impliqué dans la prévention de la criminalité. En effet, pour beaucoup, dont l'ONU (CIPC, World Bank Sustainable Development Department for Latin America and the Caribbean, Chambre de commerce de Bogotá, & Instituto Sou da Paz, 2011), la prévention de la criminalité nécessite des partenariats entre une multitude d'acteurs, notamment entre le privé et le public. De la même manière, ce même constat est souvent fait quand il s'agit de cybercriminalité. Le but de ce chapitre sera donc d'étudier les partenariats public-privé notamment en cybersécurité de façon à en faire ressortir certaines caractéristiques et enjeux, mais également d'en présenter des exemples concrets. Tandis que le chapitre précédent distinguait les approches de cybersécurité liées à la protection de l'infrastructure numérique et les approches de cybercriminalité, le manque d'informations disponibles rend difficile la recherche en matière de modèles de partenariats public-privés axés exclusivement sur la cybercriminalité. Il convient donc de se concentrer sur ces premières approches, tout en essayant dans la mesure du possible de fournir quelques exemples de partenariats public-privés.

Qu'est-ce qu'un partenariat public-privé?

Le recours à des partenariats public-privé se serait intensifié depuis les années 1990, en raison d'une privatisation croissante des infrastructures critiques, perçue par les gouvernements comme étant plus avantageuse d'un point de vue économique (Carr, 2016; Forrer, Kee, Newcomer, & Boyer, 2010; Manley, 2015). Les partenariats public-privé (PPP) ne sont évidemment pas uniques à la cybersécurité et la prévention de la cybercriminalité; ces arrangements sont mobilisés dans de nombreux contextes pour la gestion de différents enjeux, y compris ceux en lien avec la sécurité et la prévention de la criminalité. Bien qu'ils soient de plus en plus utilisés à travers le monde en guise de solutions à différentes problématiques gouvernementales, une certaine ambiguïté demeure par rapport à la signification exacte d'un partenariat public-privé (Weihe, 2005). En effet, les définitions des partenariats public-privé sont multiples et variées.

Par exemple, l'Agence européenne chargée de la sécurité des réseaux et de l'information [European Union Agency for Network and Information Security], ENISA selon l'acronyme en anglais, qui sera décrite de manière détaillée plus loin dans ce chapitre, définit un partenariat public-privé comme étant « une relation organisée entre des organisations publiques et privées qui établit un champ d'application et des objectifs communs, et qui utilisent des rôles et une méthodologie de travail définis pour atteindre ces objectifs partagés » (ENISA, 2011a, p. 10).

Le Conseil canadien pour les partenariats public-privé (CCPPP), pour sa part, propose la définition suivante d'un partenariat public-privé : « Un projet de coopération entre les secteurs public et privé, fondé sur l'expertise de chaque partenaire, qui répond au mieux aux besoins clairement définis du public à travers l'allocation des ressources, risques et rétributions. » (Le Conseil canadien pour les partenariats public-privé, 2016). Le Conseil national pour les partenariats public-privé des États-Unis offre une définition similaire :

> « Un accord contractuel entre un organisme public (fédéral, étatique ou local) et une entité du secteur privé. Grâce à cet accord, les compétences et les atouts de chaque secteur (public et privé) sont partagés dans la prestation d'un service ou d'une installation à l'usage du grand public. En plus du partage des ressources, chaque partie partage les risques et les bénéfices potentiels de la prestation du service et/ou de l'installation. » (Bechkoum, Thomas, Campbell, & Brown, 2017, p. 8).

Ces définitions démontrent que les partenariats public-privé se distinguent des ententes contractuelles dans lesquelles le secteur public, autrement dit le gouvernement, sous-traite une compagnie privée pour la réalisation d'un produit spécifique (par exemple pour la construction d'un pont ou d'un édifice). La différence se situe au niveau de ce qui va être partagé entre les partenaires : les ressources (les biens, les compétences, l'expertise, le financement), les risques et les bénéfices (Bechkoum et al., 2017).

Bien que les définitions des partenariats public-privé soient diverses, elles possèdent généralement des critères communs. Li et Akintoye (2003) et Forrer et ses collègues (2010) indiquent premièrement que la relation établie entre les partenaires doit être stable, durable et continuelle; les partenariats public-privé se distinguent de simples transactions sporadiques et ponctuelles. Deuxièmement, un aspect crucial des partenariats public-privé est le partage des responsabilités en matière de résultats et d'activités. Ce type de relation diffère donc des échanges au cours desquels le gouvernement consulte le secteur privé afin d'obtenir des conseils et des recommandations par rapport à des politiques qui demeurent sous son contrôle. Ce partage des responsabilités engendre néanmoins des enjeux importants en termes d'imputabilité, qui seront abordés plus loin dans ce chapitre. Li et Akintoye ajoutent également que le partenariat doit comprendre au moins deux acteurs, avec minimalement un acteur en provenance du secteur public et un acteur issu du secteur privé. Chaque participant doit également être en mesure de négocier en son nom propre, sans devoir faire appel à d'autres sources d'autorité. Finalement, Forrer et ses collègues soutiennent que le secteur privé doit participer aux processus de prise de décision, non seulement en termes de développement des biens et services, mais également par rapport à la meilleure façon de les offrir au public.

Manley (2015) ajoute également deux aboutissements souhaitables d'un partenariat public-privé. Premièrement, la collaboration et le partage de différents types de ressources devraient permettre de pouvoir libérer une synergie entre les acteurs impliqués. De plus, une ou plusieurs organisations prenant part au partenariat devraient se voir transformer par ce dernier.

Les secteurs public et privé sont fréquemment considérés comme deux entités séparées et fondamentalement différentes. Cette dichotomie est d'autant plus accentuée par le fait que l'on attribue à l'un et à l'autre des valeurs qui se veulent contradictoires. L'un des deux secteurs est considéré comme étant vertueux par certains, et l'autre comme étant corrompu par d'autres; l'un valoriserait la communauté et la solidarité, alors que l'autre prioriserait l'individu et les intérêts personnels (Etzioni, 2017). Cette vision des secteurs public et privé peut évidemment varier d'un pays à un autre en fonction de son organisation; par exemple, une séparation très distincte entre le privé et le public est particulièrement présente aux États-Unis, et serait à la base de la pensée juridique américaine (Etzioni, 2017). Cette vision dichotomique des deux secteurs ne fait pourtant pas l'unanimité. En sciences sociales, plusieurs experts indiquent que la distinction entre le public et le privé est plus floue que ne le laisse croire le discours public, et les organisations publiques et privées devraient être représentées sous la forme d'un continuum plutôt que d'une dichotomie (Etzioni, 2017).

Les partenariats public-privé en prévention de la criminalité

Cette section vise à brièvement présenter l'émergence des partenariats public-privé en prévention de la criminalité.

Tel que souligné dans les principes directeurs de l'ONU sur la prévention de la criminalité, une prévention efficace doit s'appuyer sur des partenariats établis entre une multiplicité d'acteurs : les institutions et ministères gouvernementaux, le milieu associatif, les organisations non gouvernementales, la société civile et les entreprises (ONUDC, 2011). Pourtant, alors que la mobilisation de la société civile en prévention de la criminalité et promotion de la sécurité publique s'effectue depuis de nombreuses années déjà, l'implication du secteur privé à ce sujet est plus récente et toujours en croissance (CIPC, 2011).

Au cours des années 1980 et 1990, les partenariats public-privé en prévention de la criminalité se traduisaient principalement par des mesures pour la protection de propriétés commerciales, d'ensembles résidentiels protégés et de domiciles privés (CIPC, 2011). Ces mesures adoptaient une approche de prévention situationnelle, ayant pour objectifs de maximiser les risques et minimiser les bénéfices d'un acte criminel sans pour autant s'attaquer aux causes profondes de la criminalité. D'ailleurs, le privé s'intéresse généralement moins aux interventions visant les causes sociales de la criminalité; tel que le rapporte Capobianco : « Les entreprises privées, qui carburent aux objectifs mesurables et aux solutions concrètes, sont moins sensibles aux projets de développement social dont les avantages sont plus théoriques, plus difficiles à mesurer ou trop longs à se matérialiser » (2005, p. 17). Ainsi, les partenariats public-privé en prévention de la criminalité avaient tendance à préconiser les initiatives dont l'approche de prévention est situationnelle, aux dépens d'autres types de prévention.

Pourtant, on commence à noter graduellement l'émergence d'une deuxième génération de partenariats public-privé qui,

cette fois, adoptent une approche davantage sociale et communautaire. Les initiatives réalisées dans le cadre de ces partenariats seront par exemple de soutenir des projets pilotes de prévention ou d'effectuer des recherches pour le développement de mesures de prévention de la criminalité (CIPC, 2011).

Mobiliser le secteur privé afin qu'il contribue à la prévention de la criminalité n'est toutefois pas chose facile. Premièrement, en matière de sécurité, la prévention (à l'inverse de la répression) est rarement une priorité gouvernementale; un faible engagement de la part du secteur public n'est pas propice à une forte mobilisation de la part du secteur privé, qui lui-même ne considérera pas la prévention comme une priorité (Avina, 2011; CIPC ,2011). De plus, des entreprises peuvent être réticentes à l'idée d'être associées à des initiatives en lien avec des thématiques criminelles par crainte des répercussions que pourrait engendrer cette association sur leur réputation. Elles peuvent par exemple craindre que leur implication dans des initiatives de prévention de la criminalité paraisse comme des tentatives de corriger des erreurs passées, ou encore que cette implication associe publiquement leur gouvernement à un enjeu qui porte atteinte à la réputation nationale (Gardiner, 2009).

La mobilisation du secteur privé sera d'autant plus ardue si celui-ci ne voit pas les bénéfices de s'investir dans un partenariat qui vise la prévention de la criminalité. Toutefois, la cybercriminalité apporte ici une nuance importante : il s'agit d'un type de criminalité qui non seulement peut porter directement atteinte à la sécurité d'une entreprise, mais qui inévitablement se réalise par l'intermédiaire de réseaux et systèmes dont le secteur privé est propriétaire. Ainsi, le rôle du privé en prévention de la criminalité se voit invariablement transformé par une forme de criminalité qui le mobilise directement.

Les partenariats public-privé en cybersécurité

Au cours des dernières années, les approches en cybersécurité ont largement été basées sur l'idée qu'il est nécessaire de reconnaître le rôle du secteur privé en matière de sécurité des réseaux de l'information et d'établir des partenariats entre les secteurs public et privé (Tropina, 2015). Tel que le stipule Germano (2014), la nature multiforme des enjeux en matière de cybersécurité a considérablement influencé les modes d'interaction entre les gouvernements et le secteur privé. Bien que le point de vue partagé soit que les gouvernements ne sont pas en mesure de lutter contre la cybercriminalité sans impliquer le secteur privé, plusieurs questions demeurent : quels devraient être les rôles respectifs de chaque entité ? Quelle forme devrait prendre la coopération entre les deux secteurs ? L'intervention gouvernementale devrait-elle être minime, ou cela risquerait-il d'engendrer des dérives de la part du privé ? Quelles approches devraient être préconisées pour le développement et la mise en œuvre de partenariats public-privé en prévention de la cybersécurité ? Cette section va s'attarder à ces questions et poser un regard sur les partenariats public-privé tels qu'actuellement développés à ce sujet.

Qu'est-ce qu'un partenariat public-privé en cybersécurité ?

Dans le cadre de ce chapitre, nous adopterons la définition d'un partenariat public-privé en cybersécurité telle que présentée par Bechkoum et ses collègues :

> « une entente de collaboration par laquelle le gouvernement ou des organisations publiques s'engagent dans des projets de coopération avec les milieux industriels ou académiques pour atténuer les risques envers la cybersécurité à travers l'amélioration des capacités de cyberdéfense, de coopération et de partage d'informations. » (2017, p. 8).

Les acteurs impliqués dans un partenariat public-privé en cybersécurité

a) Description des acteurs

Une simple dichotomie entre le secteur public et le secteur privé ne reflète pas adéquatement la complexité et la diversité des acteurs impliqués dans des partenariats public-privé, et particulièrement lorsqu'il est question de cybersécurité. Tel que le souligne Carr :

> « Il est important de noter que le partenariat public-privé en cybersécurité nationale est multidimensionnel. Les gouvernements entretiennent des relations variées avec des fournisseurs de services Internet […], des sociétés multinationales d'information (Google, Facebook, etc.), des entreprises privées de cybersécurité, des organismes défendeurs de droits humains et civils, les forces de l'ordre et la société civile. » (2016, p. 45).

L'Agence européenne chargée de la sécurité des réseaux et de l'information, ou ENISA, mentionnée au début de ce chapitre, est une agence de l'Union européenne créée en 2004 avec pour mandat d'assurer un niveau élevé de sécurité des réseaux et de l'information. Elle agit en tant que centre d'expertise pour l'Union européenne, ses États membres, ses citoyens, et le secteur privé. L'ENISA travaille avec ces différents acteurs dans le but de développer des conseils et des recommandations sur les bonnes pratiques en matière de sécurité de l'information. Notamment, l'Agence aide les États membres de l'Union européenne à mettre en œuvre la législation pertinente de l'Union européenne et cherche à améliorer la résilience des infrastructures et des réseaux d'information critique de l'Europe (ENISA, 2017b).

Dans le cadre de ses activités, l'ENISA a réalisé en 2017 une étude portant sur les partenariats public-privé en cybersécurité actuellement mis en œuvre en Europe afin

d'identifier les enjeux communs entre États membres et dégager des meilleures pratiques (ENISA, 2017b). À partir d'une recherche documentaire et d'entretiens réalisés auprès d'acteurs des secteurs privé et public de douze États membres de l'Union européenne, les auteurs du rapport ont pu identifier les différents types d'acteurs généralement impliqués dans des partenariats public-privé en cybersécurité :

- Des opérateurs privés de services;
- Des agences de cybersécurité;
- Des organismes de recherche;
- Des autorités nationales compétentes;
- Des forces de l'ordre;
- Des opérateurs publics de services;
- D'autres types d'organisations;
- Des services nationaux de renseignement.

Selon l'étude de l'ENISA, les opérateurs privés de service étaient les acteurs les plus fréquemment impliqués dans des partenariats, suivis des agences de cybersécurité, des organismes de recherche, et des autorités nationales compétentes. Les types d'acteurs sollicités pour participer au partenariat vont bien évidemment dépendre largement des objectifs de ce dernier et des domaines dans lesquels le partenariat souhaite intervenir. Par exemple, la Coalition financière européenne contre l'exploitation sexuelle commerciale des enfants en ligne (European Financial Coalition against Commercial Sexual Exploitation of Children Online, ou EFC selon l'acronyme en anglais), l'un des rares exemples de partenariat public privé en cybercriminalité, regroupe différents corps policiers européens : la police italienne, suédoise, suisse, et danoise notamment[56]. L'implication des organisations non gouvernementales (ONG) est également une tendance notable, que Dupont (2016) avait remarquée dans le cadre de son étude d'initiatives internationales de coopération pour lutter contre la cybercriminalité. En effet, les ONG étaient à l'origine de 33 pour cent des 51 initiatives analysées, et parmi les principaux groupes d'acteurs représentés dans la catégorie des ONG, se trouvaient les associations de protection des droits des enfants (2016).

Ainsi, il importe de se rappeler la pluralité d'acteurs pouvant être impliqués dans les termes plus génériques de « secteur public » et « secteur privé ». Par souci de simplicité, ces termes seront tout de même utilisés dans le cadre de ce chapitre.

b) Les motivations pour développer ou se joindre à un partenariat public-privé

Les secteurs privé et public possèdent leurs raisons respectives qui les poussent à rejoindre ou développer un partenariat public-privé axé sur la cybersécurité. Cela dit, certains facteurs sont également communs aux deux secteurs.

Nous allons premièrement nous pencher sur les motivations du secteur public pour mettre en place ou rejoindre un partenariat public-privé, suivi des motivations du secteur privé, puis des motivations communes aux deux secteurs.

Les motivations du secteur public

Une première motivation du secteur public de mettre en œuvre ou prendre part à un partenariat public-privé est de **faciliter la mise en œuvre d'une stratégie nationale de cybersécurité** (ENISA, 2011b). La stratégie nationale peut, par exemple, exiger la mise en place d'un mécanisme qui permette de partager des informations avec le secteur privé. Ce mécanisme peut être mis en place au moyen d'un partenariat public-privé. Le gouvernement peut également se retrouver dans une situation où ses moyens sont trop limités pour pouvoir mettre en œuvre à lui seul la stratégie nationale : un partenariat avec le secteur privé faciliterait ainsi la mise en œuvre de la stratégie et lui permettrait d'accéder à différentes ressources.

Au-delà du cadre d'une stratégie nationale de cybersécurité, le secteur public peut également envisager un partenariat public-privé comme un moyen **d'assurer la participation du secteur privé en cybersécurité** de manière plus générale. Le gouvernement est responsable d'assurer la protection des infrastructures critiques (voir Encadré 5.1) : or, dans plusieurs pays industrialisés, les systèmes d'infrastructures critiques sont privatisés, le secteur privé étant ainsi le principal propriétaire et exploitant de ces systèmes (Carr, 2016). Il est donc essentiel pour le gouvernement d'instaurer un mécanisme qui assure l'implication du secteur privé dans la protection des infrastructures critiques, et le partenariat public-privé permet de faciliter cette implication.

Encadré 5.1. **La protection des infrastructures critiques : un élément incontournable de la cybersécurité**

Sécurité publique Canada définit les infrastructures critiques, ou infrastructures essentielles, comme étant :

> « [...] les processus, les systèmes, les installations, les technologies, les réseaux, les biens et les services qui sont essentiels à la santé, à la sécurité ou au bien-être économique des Canadiens et des Canadiennes, ainsi qu'au fonctionnement efficace du gouvernement. Les infrastructures essentielles peuvent être autonomes ou interconnectées et interdépendantes dans les administrations provinciales, territoriales ou nationales ou entre celles-ci. La perturbation de ces infrastructures essentielles pourrait se traduire en pertes de vie et en effets économiques néfastes, et pourrait considérablement ébranler la confiance du grand public. » (Sécurité publique Canada, 2017)

Les États-Unis et le Royaume-Uni possèdent des définitions semblables, celles-ci indiquant que compromettre, endommager ou détruire des systèmes d'infrastructure critique aurait un impact sévère sur la sécurité nationale, la sécurité économique nationale, la santé publique, ou toute combinaison de ces enjeux (Carr, 2016).

La protection des infrastructures critiques est donc au cœur des débats en matière de cybersécurité depuis de nombreuses années déjà. Celle-ci est d'ailleurs l'un des domaines clés ciblés par les stratégies nationales de cybersécurité des États-Unis et du Royaume-Uni, le second domaine étant l'économie (Carr, 2016).

Tel que l'explique Carr (2016), le gouvernement est considéré responsable d'assurer la sécurité, en particulier la sécurité de la nation. La protection des infrastructures critiques est donc perçue comme faisant intégralement partie du mandat du gouvernement en termes de sécurité nationale. En effet, une cyberattaque de grande envergure envers les infrastructures critiques du pays pourrait avoir des conséquences tellement dévastatrices que le gouvernement ne peut que reconnaître sa responsabilité d'en assurer la protection. Ainsi, selon Carr, la protection des infrastructures critiques est au cœur des stratégies nationales de cybersécurité; alors que bon nombre d'aspects en lien avec la cybersécurité sont liés aux intérêts de la nation, la protection des infrastructures critiques est fondamentalement liée à la sécurité nationale (2016).

Or, au cours des dernières années, de nombreux pays industrialisés ont vu leurs systèmes d'infrastructure critique – tels que les systèmes d'approvisionnement en eau et de traitement des eaux usées, d'électricité, financiers, des communications et du transport – se privatiser. Ainsi, le gouvernement se voit dans l'obligation d'établir une relation avec le secteur privé, propriétaire et exploitant de ces systèmes, afin de pouvoir en assurer la sécurité. Dunn-Cavelty et Suter déclarent d'ailleurs que la coopération entre le gouvernement et le secteur privé en protection des infrastructures critiques est non seulement utile, mais désormais inévitable (2009).

Ainsi, la protection des infrastructures critiques est devenue un enjeu clé de la cybersécurité pour bon nombre de gouvernements, et les partenariats public-privé le moyen de prédilection pour faciliter cette protection. Carr explique d'ailleurs, dans son étude de stratégies nationales de cybersécurité (2016), que dans les pays où des systèmes d'infrastructure critique sont privatisés, la stratégie nationale de cybersécurité accordera une place prépondérante aux partenariats public-privé comme mécanisme permettant de limiter les attaques.

Le secteur public peut également juger pertinent de développer ou rejoindre un partenariat public-privé afin de **coordonner différentes initiatives** qui visent la lutte contre la cybercriminalité. Un partenariat public-privé offre notamment la possibilité de développer des synergies entre différentes initiatives du secteur privé, qui autrement pourraient travailler indépendamment les unes des autres (ENISA, 2017b).

Finalement, le secteur public peut décider de développer un partenariat public-privé afin d'**aider le secteur privé à mettre en application de nouvelles régulations** qui lui sont imposées. Par exemple, dans le cadre de l'étude de l'ENISA portant sur les partenariats public-privé européens en cybersécurité (2017b), certains experts européens interviewés ont mentionné le fait que de nouvelles réglementations européennes – telles que la directive sur la sécurité des réseaux et des systèmes d'information, connue sous l'appellation « directive NIS », adoptée par le Parlement européen et le Conseil de l'Union européenne le 6 juillet 2016 (ANSSI, 2016), ou encore le règlement général sur la protection des données (RGPD) adopté par le Parlement européen le 14 avril 2016 – imposaient des obligations particulières au secteur privé. Ainsi, des gouvernements ont décidé de créer des partenariats dans l'optique d'aider le secteur privé à mettre en œuvre ces nouvelles régulations.

Les motivations du secteur privé

Une motivation propre au secteur privé de vouloir participer ou développer un partenariat public-privé est d'**exercer une influence sur le cadre réglementaire**, que ce soit au niveau des politiques publiques ou des législations qui concernent la cybersécurité. Un partenariat avec le secteur public peut permettre au secteur privé d'influencer les futures stratégies nationales de sécurité et autres politiques et lois se rapportant à la cybersécurité. Le partenariat public-privé peut également servir de mécanisme de rétroaction, offrant la possibilité au secteur privé de signaler au gouvernement les obligations lui paraissant contraignantes, inappropriées, ou irréalistes (ENISA, 2011b). Les intérêts économiques du secteur privé sont fréquemment au cœur de ce désir d'implication, celui-ci souhaitant protéger ses intérêts commerciaux et éviter des obligations coûteuses imposées par des législations (ENISA, 2017b).

Une organisation privée peut également faire face à un problème en lien avec sa cybersécurité dont la solution ou l'impact dépasse ses limites organisationnelles (ENISA, 2011b). La participation d'autres acteurs lui paraît donc nécessaire et lui permet d'**outrepasser ses limitations**.

Le secteur privé peut également considérer comme avantageux de se joindre à un partenariat afin de faire avancer ses intérêts privés. Dupont note, par exemple, que dans le domaine de la coopération policière internationale contre la cybercriminalité, des entreprises telles que Microsoft, Symantec et Telefonica :

> « […] n'hésitent pas à déployer leurs capacités techniques et juridiques de manière plus ou moins coordonnée avec certaines institutions policières nationales et internationales afin de faire avancer leurs intérêts privés, qu'il s'agisse de maintenir la confiance des consommateurs dans leurs produits ou de les convaincre de la supériorité de leurs solutions sur celles de leurs compétiteurs. » (2016, p. 117).

Les motivations communes aux deux secteurs

Accéder à des ressources est une motivation fréquente, autant de la part du secteur privé que public (ENISA, 2011b). Pour le secteur privé, le partenariat public-privé permet d'accéder à des fonds publics ou encore à des informations privilégiées du secteur public telles que des informations confidentielles. Alors que le secteur privé est souvent considéré comme un acteur pouvant contribuer de manière importante à un partenariat en cybersécurité, notamment en termes de ressources (techniques, financières) et d'expertise, Germano (2014) rappelle que le secteur public possède également de nombreuses forces à ne pas négliger. Le secteur public peut, quant à lui, procéder à des enquêtes, des arrestations et des poursuites de cybercriminels; recueillir des renseignements étrangers concernant des cybermenaces; offrir, dans certains cas, des protections statutaires à des entreprises qui partagent des informations avec le gouvernement; analyser des informations provenant de sources domestiques et étrangères avant que ces informations ne soient accessibles au secteur privé, ainsi que récolter et diffuser des informations à différentes industries et entreprises. Par le biais de ces différentes possibilités, le gouvernement est en mesure d'enrichir la compréhension d'une menace, facilitant ainsi le développement de mesures d'atténuation des risques et de protection des victimes potentielles (Germano, 2014). En ce qui concerne le secteur public, les ressources qui lui sont accessibles par l'entremise d'un partenariat public-privé sont notamment une expertise qui facilite le développement de standards et de bonnes pratiques, ainsi que des informations qui lui permettent d'acquérir une meilleure compréhension des mesures de Protection de l'Information sur les Infrastructures Critiques (PIIC) mises en place par le secteur privé (ENISA, 2011b). Les partenariats permettent également à chaque secteur d'obtenir des contacts crédibles et directs avec d'autres organisations, sources d'expériences et connaissances. Le secteur public peut également ne pas posséder suffisamment de ressources pour mobiliser ou motiver l'ensemble des parties prenantes plus petites, mais pertinentes au développement d'un environnement cyber sécuritaire, par exemple les petites et moyennes entreprises. Les ressources du secteur privé, financières ou autres, lui permettent donc de rejoindre un plus large éventail d'acteurs.

En plus du partage des ressources, **le partage des risques et des coûts** associés à l'offre d'un service aux citoyennes et citoyens est une motivation importante autant pour le secteur privé que public (Kaijankoski, 2015).

Dans certains cas, des partenariats public-privé peuvent devoir être créés dans le cadre de **nouvelles réglementations.** Il peut s'agir d'une loi pour laquelle l'administration publique considère qu'un partenariat public-privé en facilitera la réalisation. Ces lois peuvent notamment porter sur la gestion de crise ou d'urgences. Il peut également être question d'une loi spécifique aux partenariats public-privé, qui dicte précisément en quoi consistera le cadre de coopération et collaboration. Ces lois sont généralement consacrées aux partenariats public-privé en général, et non uniquement à ceux portant sur la cybersécurité. Finalement, certaines lois ou législations exigent d'une organisation du secteur privé qu'elle fasse partie d'un partenariat public-privé (ENISA, 2011b).

Un partenariat public-privé peut également être mis sur pied dans l'optique d'**améliorer la coordination** entre différents secteurs. Des organisations publiques et privées peuvent reconnaître que le partage d'informations est insuffisant entre ces secteurs, ou encore qu'il y a un dédoublement d'efforts qui pourrait être pallié au moyen d'un partenariat. La coordination entre des secteurs tels que celui des communications et celui des technologies de l'information s'avère également essentielle, les frontières entre ces deux secteurs devenant de plus en plus perméables (ENISA, 2011b). De plus, il peut parfois régner un climat de méfiance entre différents compétiteurs d'un même territoire ou secteur; le partenariat public-privé facilite donc le recours à un médiateur externe qui puisse assurer une coordination entre des acteurs qui seraient autrement peu disposés à coopérer.

L'intérêt de développer un partenariat public-privé peut être de **s'assurer que la cybersécurité soit considérée comme un enjeu important dans l'agenda collectif**, autant pour le gouvernement que le secteur privé, afin de générer une certaine mobilisation de la part des différents acteurs et d'en faire la promotion (ENISA, 2017b).

Les partenariats public-privé sont également un moyen de **s'adapter à la nature changeante des menaces**, qui prennent entre autres de nouvelles formes (par exemple le cyberterrorisme) ou encore une ampleur de plus en plus internationale (ENISA, 2011b). Tel que le souligne Germano, « le secteur privé requiert fréquemment l'assistance du gouvernement pour transcender les frontières et développer des solutions internationales pour le suivi, l'identification, et l'atténuation des cybermenaces » (2014, p. 2).

Finalement, les partenariats public-privés permettent également aux secteurs public et privé de **réduire leurs vulnérabilités** à la suite d'attaques dont ils auraient été les cibles (ENISA, 2011b).

L'ENISA (2017b) rappelle que de manière générale, des partenariats public-privé sont développés en réponse à différents motifs, et non pour une seule raison spécifique.

La mise en œuvre et le développement d'un partenariat public-privé en cybersécurité

Différentes approches peuvent être adoptées pour mettre en œuvre et développer un partenariat public-privé. L'ENISA (2017b) a notamment identifié différentes combinaisons possibles dans un contexte de cybersécurité, à la fois en matière de mise en œuvre et de développement.

a) Approches de mise en œuvre du partenariat public-privé

En termes de mise en œuvre, les deux approches principalement adoptées sont une approche top-down et une approche bottom-up. Lorsqu'un partenariat public-privé est mis en œuvre à partir d'une **approche** top-down, celui-ci a généralement été créé à la suite d'une directive ou d'un plan d'action gouvernemental requérant la création d'un partenariat public-privé. À l'inverse, un partenariat issu d'une **approche** bottom-up est habituellement le résultat d'un besoin identifié par une communauté, qui s'est mobilisée afin de créer un partenariat qui puisse combler ce besoin. Les différents acteurs interviewés par l'ENISA dans le cadre de son étude (2017b) ont d'ailleurs spécifié qu'il était plus probable qu'un partenariat public-privé en cybersécurité mis en œuvre afin de répondre à des besoins identifiés par le secteur privé – autrement dit mis en œuvre à partir d'une approche bottom-up – soit dynamique et garant de succès.

b) Approches de développement du partenariat public-privé

Le partenariat public-privé peut par la suite se développer de différentes manières. Dans le cadre d'un partenariat mis en œuvre de manière top-down, le gouvernement peut s'être chargé de recruter des membres par lui-même. Toutefois, dans certains cas, le développement du partenariat se réalise plutôt de manière bottom-up ; la création du partenariat a été imposée par le gouvernement, mais les décisions en termes de responsables et membres du partenariat n'ont pas été prises exclusivement par le secteur public. Le secteur privé a été largement impliqué dans cette prise de décision et le développement du partenariat. Cette **combinaison d'une mise en œuvre** top-down **et d'un développement** bottom-up est d'ailleurs à l'origine de plus des deux tiers des partenariats public-privé en cybersécurité analysés par l'ENISA dans le cadre de son étude (2017b). Une combinaison inverse est également possible : un groupe d'acteurs peut avoir identifié un besoin, mis en œuvre un partenariat pour répondre à ce besoin, et par la suite approché une autorité gouvernementale afin que celle-ci cautionne l'initiative. Afin que le partenariat se développe, le gouvernement peut y apporter des contributions financières ou encore y assurer une certaine autorité. Il s'agit ainsi d'une **combinaison d'une mise en œuvre** bottom-up **et d'un développement** top-down.

Le partenariat public-privé peut également se développer indépendamment de la structure l'ayant créé. Tel que l'explique l'ENISA :

> « Un organisme central, souvent dirigé par le gouvernement, crée une structure de partenariat, en promeut l'utilisation, mais une fois les partenariats créés, ils sont autonomes. Un kit de démarrage peut être fourni, pouvant inclure des outils et la possibilité d'acheter ou de s'inscrire à des services tels que des avertissements ou des alarmes [en cas de cyberattaques]. » (2017b, p. 17)

Finalement, au fur et à mesure qu'il se développe, le partenariat public-privé peut nécessiter une certaine restructuration afin de favoriser son efficacité. Ainsi, il peut se fractionner en différents sous-groupes possédant chacun une spécialisation ou un objectif précis. L'information récoltée par ces sous-groupes est donc généralement plus spécifique, et la taille réduite du groupe a l'avantage de faciliter le développement de relations de confiance entre ses membres – un aspect crucial pour assurer la réussite d'un partenariat public-privé, qui sera analysé de manière détaillée plus loin dans ce chapitre. La situation inverse peut également se produire : il peut s'avérer plus judicieux pour différents partenariats public-privé de fusionner, notamment lorsque ceux-ci partagent des thématiques, compétences, ou objectifs communs.

Les composantes des partenariats public-privé en cybersécurité

L'ENISA a publié en 2011 un premier rapport et guide de bonnes pratiques sur les modèles de coopération pour des partenariats public-privé en cybersécurité efficaces. À partir des différents partenariats public-privé étudiés, l'ENISA a été en mesure de développer une taxonomie des partenariats public-privé comprenant sept composantes :

- **La structure de gouvernance.** Cette composante fait référence à la manière dont le partenariat public-privé est organisé, la manière dont les partenaires travaillent ensemble, ses règlements et ses sources de financement.
- **Les objectifs.** Cette composante fait référence aux aspects de sécurité et résilience sur lesquels le partenariat cherche à intervenir. Les objectifs du partenariat détermineront les services offerts par celui-ci, et permettront ainsi de situer ses activités en fonction des étapes d'un cycle de cybersécurité, qui seront décrites plus loin. Autrement dit, les objectifs du partenariat permettent de déterminer s'il cherche à prévenir des cyberattaques, à réagir à celles-ci, ou les deux.
- **Les services.** Il s'agit des services offerts par le partenariat afin de répondre à ses objectifs. Il peut s'agir, notamment, de partager des informations, ou de réaliser des exercices de simulation d'une cyberattaque auprès des différents partenaires.
- **Les menaces.** Cette composante comprend les types de menaces envers la sécurité que le partenariat prend en considération.
- **L'étendue.** Cette composante fait premièrement référence à l'étendue géographique couverte par le partenariat; autrement dit, à la localisation géographique des partenaires impliqués, soit au niveau national, régional, ou international. Elle fait également référence à l'étendue des secteurs impliqués : s'agit-il d'une thématique particulière, d'un secteur entier (par exemple le domaine financier), ou d'une envergure intersectorielle?
- **Le développement.** Cette composante comprend la manière dont le partenariat a été établi, son évolution, ainsi que les incitations employées pour encourager et maintenir un certain niveau de participation de la part des différents partenaires.

- **Les liens.** Cette dernière composante fait référence aux liens établis entre le partenariat et d'autres partenariats public-privé, ainsi qu'avec d'autres organisations.

Nous allons nous pencher plus spécifiquement sur les deuxième et troisième composantes, soit les objectifs du partenariat et les services qu'il offre. Tel que nous pourrons le constater, ces deux composantes, et plus particulièrement les objectifs, vont déterminer si le partenariat adopte une approche préventive en matière de cybersécurité.

a) Les objectifs d'un partenariat public-privé en cybersécurité

Tel que vu précédemment, les objectifs de sécurité du partenariat vont s'inscrire dans l'une ou l'autre des étapes du cycle de cybersécurité. Ces étapes sont les suivantes :

- **La dissuasion.** Un partenariat public-privé ayant pour objectif la dissuasion va chercher à décourager la réalisation d'une attaque par des cybercriminels. Les services offerts par le partenariat peuvent être de l'ordre de la sensibilisation par rapport à la cybersécurité et aux conséquences d'une attaque pour les cybercriminels, ou encore des mesures des forces de l'ordre.
- **La protection.** Afin de développer la protection des systèmes, les partenariats public-privé ayant cet objectif vont chercher à développer des standards de protection et des communautés de partage d'informations. Pour ce faire, ils vont recueillir les informations les plus récentes au sujet des nouvelles menaces envers la cybersécurité ainsi que des mécanismes de protection.
- **La détection.** Les partenariats public-privé ayant pour objectif la détection vont chercher à comprendre les nouvelles menaces informatiques pour mieux y répondre. Ils feront donc appel au partage d'informations et aux systèmes d'alerte rapide pour y parvenir.
- **L'intervention.** Un partenariat public-privé axé sur l'intervention aura pour objectif de développer la capacité des partenaires à réagir à l'impact initial d'une attaque ou d'une urgence. Les services offerts dans le cadre de cet objectif seront par exemple des simulations d'attaques afin que les partenaires puissent pratiquer leurs réactions, le développement de plans d'action en cas d'urgences, et la gestion de crise.
- **La récupération.** Un partenariat public-privé ciblant davantage la récupération va chercher à développer la capacité de ses membres à se remettre d'une attaque et effectuer les réparations nécessaires. La récupération implique donc de travailler à ce que les systèmes retrouvent leur fonctionnalité initiale.

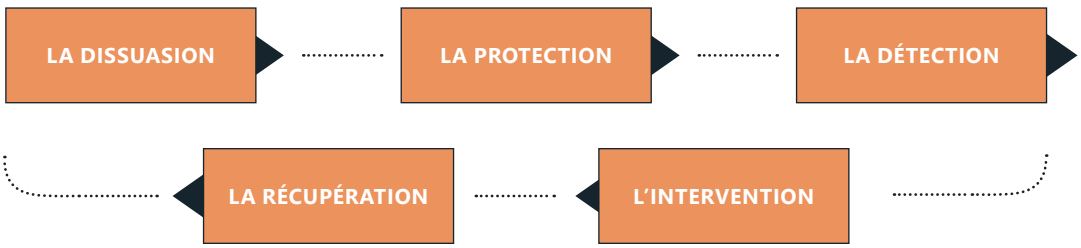
b) Les services offerts par un partenariat public-privé en cybersécurité

Les partenariats public-privé en cybersécurité peuvent offrir une grande diversité de services à leurs membres. L'ENISA (2017b) identifie entre autres les services suivants : la gestion de crise et le traitement des incidents; la recherche et l'analyse (par exemple des études pour développer des nouvelles technologies plus sécuritaires); le développement de guides de bonnes pratiques et lignes d'action; le partage d'informations; le signalement rapide en cas de menaces; les exercices et simulations afin que les membres du partenariat puissent pratiquer leurs réactions face à une attaque éventuelle; la sensibilisation; l'évaluation technique; l'établissement de standards155; la planification en matière de stratégie, d'urgences ou de résilience; l'analyse des risques. Ces différents services seront de toute évidence déterminés en fonction des objectifs établis par le partenariat.

c) Les principaux types de partenariats public-privé en cybersécurité

L'ENISA a pu établir une typologie des partenariats public-privé en fonction des étapes du cycle de cybersécurité auxquelles le partenariat souhaite intervenir; autrement dit, les objectifs du partenariat sont au cœur de cette typologie. Les trois principaux types identifiés sont les suivants : les partenariats public-privé axés sur la prévention, les partenariats axés sur l'intervention,

Figure 5.1. **Les étapes du cycle de cybersécurité**



et les partenariats axés sur l'ensemble des étapes du cycle de cybersécurité. Tel que l'explique l'ENISA (2011b), les différents partenariats public-privé identifiés dans le cadre de leur étude correspondaient tous à l'un de ces trois types, démontrant ainsi une similarité et une simplicité en termes d'approches adoptées, malgré une diversité importante en matière de pays, de contextes légaux, de cultures et d'organisations.

Les partenariats public-privé axés sur la prévention

Ces partenariats public-privé auront pour objectifs la dissuasion, la protection et la détection (dans la mesure où le partenariat vise à acquérir des informations sur des nouvelles cybermenaces pour mieux les comprendre). Nous pouvons d'ores et déjà constater que l'approche de prévention est restreinte, en se limitant aux menaces imminentes et à la diminution des opportunités pour la commission du crime. N'ayant pas la vocation de réagir dans l'immédiat à une attaque, ces partenariats vont plutôt adopter une vision à long terme en matière de coopération. Les membres du partenariat vont chercher à apprendre les uns des autres et mettre en application ces apprentissages au fil de leur collaboration. Ainsi, les bénéfices d'une implication dans ce type de partenariat peuvent ne pas être immédiats, nécessitant l'implication d'acteurs du secteur privé ayant la capacité d'investir dans les activités du partenariat tout en n'espérant pas des retombées immédiates. Ces partenariats public-privé sont généralement initiés par le secteur privé, responsable des intérêts nationaux à plus long terme (ENISA, 2011b).

Les services offerts par un partenariat axé sur la prévention seront de l'ordre des guides de bonnes pratiques, du partage d'informations, du signalement rapide d'une vulnérabilité dans les systèmes, des exercices et simulations, de la sensibilisation, des évaluations techniques et de la définition de standards.

Les partenariats public-privé axés sur l'intervention

Les partenariats axés sur l'intervention auront pour objectifs l'intervention lors d'une attaque et la récupération à la suite de celle-ci. Ces partenariats peuvent donc avoir une vision à court terme, autrement dit de réagir immédiatement lors d'une attaque, ou à long terme, dans l'optique d'établir et améliorer les mécanismes qui permettent une réaction rapide à ce genre d'événements. La valeur de ces partenariats apparaît donc plus claire aux yeux des organisations privées, qui sont plus à même d'initier ce genre de partenariat. Inversement, le secteur public peut également être à l'origine de leur mise en œuvre à la suite d'un événement majeur tel que le 11 septembre 2001. Ces partenariats regroupent généralement des membres ayant de fortes capacités techniques afin de réagir rapidement à une cyberattaque (ENISA, 2011b).

Les services offerts par ces partenariats seront par exemple la gestion de crise et la planification en cas d'urgences et en matière de résilience.

Les partenariats public-privé axés sur l'ensemble des étapes du cycle de cybersécurité

Certains partenariats public-privé seront en mesure de développer et mettre en œuvre un ensemble d'activités permettant de s'adresser à toutes les étapes du cycle de cybersécurité. Ces partenariats peuvent prendre différentes formes. Il peut s'agir, par exemple, d'un partenariat regroupant un très grand nombre d'acteurs aux multiples rôles, compétences et responsabilités, permettant ainsi d'intervenir à toutes les étapes du cycle. Afin de faciliter la gestion des interactions entre un si grand nombre de partenaires, des sous-groupes organisés autour d'un thème ou d'un secteur sont généralement développés. Une autre forme que peut prendre un partenariat axé sur l'ensemble des étapes du cycle de cybersécurité est celle d'une petite organisation regroupant les représentants seniors de différents partenariats axés sur la prévention ou l'intervention (ENISA, 2011b).

Initiatives internationales et stratégies nationales

Cette section a pour objectif de présenter diverses initiatives de partenariats public-privé en cybersécurité, et plus particulièrement celles ayant adopté une approche axée sur la prévention, tel que vu précédemment. Des initiatives internationales seront premièrement présentées, suivies de stratégies nationales de cybersécurité comportant un volet sur les partenariats public-privé.

Les initiatives internationales

Étant donné la nature internationale du cyberespace, il est logique que différents pays tentent d'établir des accords internationaux – qu'ils soient bilatéraux ou multilatéraux – dans le but d'en assurer la régulation et d'éventuellement coordonner des initiatives de cybersécurité. Nous présenterons deux initiatives internationales de partenariats public-privé dans cette section. La première, le Forum of Incident Response and Security Teams (FIRST), occupe une position particulièrement importante à l'échelle mondiale en raison, entre autres, du nombre considérable d'acteurs qu'elle regroupe. Le deuxième exemple, l'European Public-Private Partnership for Resilience (EP3R), une initiative ayant pris fin en 2013, permet de dégager certains constats en matière de partenariat public-privé en cybersécurité à une échelle paneuropéenne.

a) Le Forum of Incident Response and Security Teams, ou FIRST

Dupont (2016) démentit l'hypothèse selon laquelle les institutions policières et judiciaires auraient des difficultés importantes à s'adapter à un environnement numérique en constante mutation; en effet, sa recension de 51 initiatives internationales multilatérales de lutte contre la cybercriminalité démontre que depuis les années 1990, une multitude de « réseaux hybrides mêlant services de police nationaux, organisations in-

ternationales, acteurs non gouvernementaux, associations professionnelles et entreprises » (Dupont, 2016, p. 96) se sont développés afin de lutter contre la cybercriminalité.

À la lecture des données recueillies, Dupont a pu constater le rôle déterminant joué par le secteur privé dans le cadre de ces initiatives internationales. Parmi les 657 acteurs impliqués dans ces initiatives, 47 pour cent (un total de 312) sont des entreprises, et pas moins de 12 pour cent des initiatives analysées ont été mises en œuvre par des entreprises (Dupont, 2016). Parmi celles-ci, nous retrouvons l'initiative Forum of Incident Response and Security Teams (ou FIRST), développée par le secteur privé afin de coordonner la réponse aux incidents informatiques à une échelle internationale.

Il importe d'accorder une attention particulière à cette initiative; tel que l'explique Dupont (2016), FIRST regroupe le plus grand nombre d'acteurs de toutes les initiatives analysées, pour la plupart des entreprises. À l'heure actuelle, FIRST regrouperait plus de 400 membres en provenance de 85 pays (FIRST, 2014). Ses membres sont principalement des équipes d'intervention en cas d'urgence informatique, mieux connues sous leurs appellations anglophones Computer Emergency Response Teams (CERT) ou Computer Security Incident Response Teams (CSIRT). Ces organismes officiels sont chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents informatiques, et peuvent avoir été établis par une diversité d'acteurs : des gouvernements, des entreprises, des universités, des forces de l'ordre, etc. (Global Forum on Cyber Expertise, 2017). Le FIRST agit ainsi à titre de représentant mondial de ces équipes d'intervention. En plus des très nombreuses CSIRT membres de FIRST, des individus et représentant(e)s d'organisations peuvent également se joindre au réseau. Les acteurs impliqués dans FIRST « ne disposent pour la majorité d'entre eux d'aucun autre canal de communication et d'échange avec les initiatives ou acteurs qui composent le réseau global » (Dupont, 2016, p. 116). Ainsi, le FIRST contrôle l'accès à un nombre important d'acteurs intervenant dans le regroupement d'initiatives internationales de lutte contre la cybercriminalité.

Selon la typologie de l'ENISA, le FIRST correspond à un partenariat public-privé axé en grande partie sur la prévention des incidents informatiques : en effet, les objectifs du Forum sont d'encourager la coopération et la coordination dans la prévention d'incidents informatiques et de promouvoir le partage d'informations entre différentes CSIRT à travers le monde. Afin d'atteindre ces objectifs, le FIRST maintient non seulement un réseau international entre les différentes équipes d'intervention, mais offre également des services tels que le développement et partage d'outils, d'informations techniques, de méthodologies et de bonnes pratiques, ainsi que l'organisation de formations et de conférences pour promouvoir ces pratiques en matière de sécurité informatique[57].

b) L'European Public-Private Partnership for Resilience, ou EP3R

En termes de partenariats public-privé européens, le cas de l'European Public-Private Partnership for Resilience, ou EP3R, permet de dégager des enjeux importants pouvant être rencontrés dans un partenariat public-privé d'envergure régionale ou paneuropéenne. En effet, cette première tentative d'établir un partenariat public-privé paneuropéen pour favoriser la sécurité et la résilience dans le domaine des télécommunications fût mise en œuvre en 2009, pour ensuite mettre un terme à ses activités en 2013. Ses objectifs étaient d'offrir une plateforme pour le partage d'informations concernant des politiques et pratiques qui favorisent la sécurité et la résilience des infrastructures critiques d'information, de définir un cadre qui puisse permettre d'améliorer la cohérence et la coordination de politiques en matière de sécurité et résilience en Europe, puis d'identifier et promouvoir des bonnes pratiques (Irion 2013).

Dupré (2014) a effectué des entretiens auprès des participants de l'EP3R afin d'obtenir des informations par rapport à l'initiative, aux enjeux rencontrés, et aux leçons et recommandations pouvant être dégagées. Bien que l'initiative ait été de manière générale appréciée, plusieurs critiques ont néanmoins été formulées à son égard.

Premièrement, plus de la moitié des participants ont signalé que la raison principale qui entravait leur participation au partenariat est le fait que leur organisation n'ait pas été informée de manière adéquate des objectifs et résultats escomptés de l'initiative.

Les participants ne voyaient également pas de retombées claires à leur participation à l'EP3R, ce qui a provoqué le départ de plusieurs membres et une rotation de membres importante. Ainsi, l'instabilité des réseaux personnels gênait le développement d'un lien de confiance entre les membres du partenariat.

Une autre problématique soulevée est le fait que la participation aux activités de l'EP3R, notamment les déplacements requis pour assister à une réunion, était à la charge des participants. Ainsi, la participation dépendait largement des ressources de chaque membre. Plusieurs ont d'ailleurs mentionné que la mise à disposition de fonds pour la participation à l'EP3R aurait eu un impact positif sur le nombre de participants ainsi que leur engagement face au partenariat.

Un autre enjeu identifié par un nombre important de personnes interviewées est le fait que des joueurs importants du secteur privé ne participaient pas à l'initiative, diminuant ainsi son attrait de manière générale, notamment auprès des petites et moyennes entreprises.

Finalement, tous les participants ont déclaré que l'EP3R n'avait pas déterminé de moyens précis pour produire les résultats escomptés. De plus, plusieurs ont noté qu'un manque de connaissances en matière de normes et restrictions juridiques nationales faisait en sorte que les obstacles auxquels les participants

pouvaient être confrontés n'étaient pas considérés, et les recommandations offertes n'étaient donc pas forcément adaptées aux contextes nationaux.

L'EP3R n'est bien évidemment pas le seul partenariat public-privé d'envergure paneuropéenne ayant été créé afin de répondre à des besoins en matière de cybersécurité. La Commission européenne a notamment signé un accord de partenariat public-privé avec l'European Cyber Security Organisation (ECSO)[58] en juillet 2016 dans le cadre de la stratégie européenne de cybersécurité (ECSO, 2018). Ce partenariat public-privé, qui est associé à un effort financier de 450 millions d'euros de la part de la Commission européenne et d'un montant trois fois supérieur en provenance du secteur privé, a pour objectif de faciliter la coopération entre acteurs publics et privés et de construire un marché européen de la cybersécurité qui soit compétitif.

Ces nouveaux partenariats public-privé paneuropéens pourront s'inspirer des expériences de l'EP3R, afin d'anticiper des enjeux pouvant nuire à la participation des différents acteurs et favoriser le succès de leur initiative.

Les stratégies nationales de cybersécurité

La section suivante va présenter un aperçu des stratégies nationales de cybersécurité abordant les partenariats public-privé[59].

Plusieurs pays ont récemment développé des stratégies nationales de cybersécurité qui mettent l'accent sur une forme de partenariat public-privé. Carr (2016) indique que c'est le cas de l'Autriche, de l'Australie, du Canada, de la République tchèque, de l'Estonie, de la Finlande, de la France, de la Hongrie, de l'Inde, du Japon, de la Lituanie, des Pays-Bas, de la Nouvelle-Zélande, de la Slovaquie, de l'Afrique du Sud, du Royaume-Uni et des États-Unis. Tel que vu précédemment dans ce chapitre, de nombreux pays dont les systèmes d'infrastructure critique (par exemple dans les domaines des finances ou du transport) sont privatisés, ont développé des stratégies nationales de cybersécurité qui accordent une importance prépondérante au partenariat public-privé, considéré comme un mécanisme clé pour atténuer les risques (Carr 2016).

Aux États-Unis et au Royaume-Uni, le partenariat public-privé a fréquemment été décrit comme étant la « pierre angulaire » de la stratégie de cybersécurité (Carr, 2016). Dans les deux cas, le secteur privé possède et exploite la majeure partie de l'infrastructure critique. Le gouvernement peut donc difficilement assurer la sécurité de l'infrastructure nationale sans collaborer avec le privé (Etzioni, 2017). Les États-Unis sont d'ailleurs le premier pays à avoir développé des stratégies de cybersécurité qui s'appuient sur les partenariats public-privé, influençant ainsi le développement de stratégies semblables ailleurs. Ces stratégies ont fait leur apparition dès les années 2000 sous la présidence de Bill Clinton. Malgré le fait qu'au cours des années qui suivirent, les partenariats public-privé soient demeurés un pilier de la stratégie nationale, les paramètres et la nature de la relation entre les deux partis n'ont jamais été explicitement définis (Carr, 2016).

En Europe, tel que le stipule l'ENISA, l'un des objectifs communs à toute stratégie nationale de cybersécurité est la collaboration (2017a, 2017b). Cette collaboration est généralement réalisée au moyen d'une des deux structures suivantes : les partenariats public-privé et les centres d'analyse et de partage des informations (ou Information Sharing and Analysis Centers, ISACs selon l'acronyme en anglais). Ces derniers sont décrits de manière plus détaillée dans l'encadré 5.2 ci-dessous.

Encadré 5.2. **Les centres d'analyse et de partage des informations, ou ISACs**

Les centres d'analyse et de partage des informations sont généralement des organisations à but non lucratif qui agissent en tant que ressources centrales pour la collecte d'informations en lien avec des cyber menaces (qui visent généralement les infrastructures critiques) ainsi que le partage bilatéral d'informations entre les secteurs publics et privés (ENISA, 2017a).

Dunn-Cavelty et Suter (2009) notent que les premiers centres d'analyse et de partage des informations ont vu le jour aux États-Unis en 1999, à la suite des recommandations du rapport de la Commission sur la protection des infrastructures critiques établies par le président Clinton en 1996. Le rapport identifiait le partage d'informations entre les différents acteurs impliqués dans le domaine des infrastructures critiques comme étant le besoin le plus urgent afin d'en assurer la protection. Ainsi, il fût recommandé aux différents secteurs de créer des partenariats public-privé qui prendraient la forme de centres d'analyse et de partage des informations, dont l'objectif serait de partager des informations sur la sécurité, les menaces rencontrées, et les meilleures pratiques (Dunn Cavelty & Suter, 2009).

Tels que décrits par le Conseil national des centres d'analyse et de partage des informations américain :

> « Les centres d'analyse et de partage des informations (ISACs) aident les propriétaires et les exploitants d'infrastructures essentielles à protéger leurs installations, leur personnel et leurs clients contre les menaces à la sécurité cyber et physiques et d'autres dangers. Ils recueillent, analysent et diffusent à leurs membres de l'information sur les menaces pouvant donner lieu à des mesures concrètes et fournissent aux membres des outils pour atténuer les risques et améliorer la résilience. […] La plupart des ISACs ont la capacité de signaler les menaces et les incidents 24/7, et peuvent également fixer le niveau de menace pour leurs secteurs. De nombreux ISACs sont reconnus pour réagir et partager de l'information perti-

nente et susceptible de donner lieu à des mesures plus rapidement que les partenaires gouvernementaux. » (National Council of ISACs, 2018)

Il existe de nombreux ISACs à travers le monde et ils œuvrent fréquemment dans des secteurs particuliers (Forum économique mondial, 2017). Par exemple, aux États-Unis, des ISACs ont été créés dans les domaines de l'automobile, de l'aviation, de l'électricité, de la santé, etc. Le partage de connaissances s'effectue également entre les différents secteurs des infrastructures critiques ; les ISACs collaborent et échangent de l'information sur les menaces et les mesures d'atténuation entre eux par l'entremise du Conseil national des ISACs (National Council of ISACs, 2018).

Certaines stratégies européennes précisent des actions spécifiques dans le cadre de partenariats public-privé. C'est le cas, notamment, de la République tchèque et de l'Espagne (Luiijf, Besseling, & Graag, 2013). La stratégie nationale tchèque en cybersécurité (National Security Authority, 2015) propose entre autres la coopération entre secteurs privé et public afin de développer des normes de sécurité uniformes et définir un niveau obligatoire de protection pour tous les acteurs en infrastructures critiques de l'information. La stratégie nationale de l'Espagne propose des mesures semblables, à savoir favoriser le développement de standards en cybersécurité par le biais de partenariats public-privé (Gobierno de España, 2013).

En plus de mesures concrètes en termes de collaboration entre les secteurs privé et public, certaines stratégies définissent précisément les rôles attribués à chaque secteur dans le cadre de ces partenariats public-privé. Par exemple, la stratégie nationale de cybersécurité du Japon indique qu'il est nécessaire pour les entreprises d'affecter un responsable de la sécurité des systèmes d'information (RSSI) qui veille à la sécurité, la disponibilité et l'intégrité des systèmes d'information et de données.

Selon l'ENISA (2017b), la culture d'un pays est l'un des facteurs les plus déterminants dans la mise en œuvre et le fonctionnement d'un partenariat public-privé. Les spécificités culturelles, ainsi que les relations entre les secteurs public et privé d'un pays, auront une influence considérable sur la meilleure approche à adopter pour assurer le succès d'un partenariat.

Par exemple, dans les pays ayant traditionnellement une administration publique très forte, les secteurs privé et public sont éloignés l'un de l'autre et peu amenés à travailler de concert. Dans l'éventualité où un partenariat est établi, des règlements et objectifs précis doivent être convenus, souvent dans un cadre hiérarchique à l'image de la position hiérarchique de l'administration publique (ENISA, 2017b). À l'inverse, les pays dans lesquels les autorités publiques détiennent moins de pouvoir auront une approche plus pragmatique en ce qui concerne les partenariats public-privé; une base juridique ne sera pas forcément requise et des accords de confidentialité peuvent suffire à la création d'un partenariat entre les secteurs public et privé (ENISA, 2017b).

Ce bref survol donne un aperçu des diverses manières dont les partenariats public-privé peuvent être considérés dans les stratégies nationales de cybersécurité. Tel que précisé précédemment, cette thématique sera approfondie dans la contribution de l'ENISA à ce chapitre.

Enjeux

La conclusion de partenariats entre des acteurs issus de la sphère publique et des acteurs privés dans un but de prévenir et lutter contre la cybercriminalité présente différents enjeux. Si certains tiennent de la nature même des acteurs impliqués, d'autres sont inhérents à la structure même des partenariats.

Les enjeux liés aux acteurs : des différences difficiles à concilier

Les partenariats public-privé regroupent des acteurs ayant des identités, mais également des intérêts différents.

a) Des identités institutionnelles différentes

Les acteurs privés et publics se distinguent par des cultures institutionnelles et des valeurs non seulement différentes, mais opposées. En effet, Gal (2002) rappelle que si le secteur public est tourné vers la communauté et se veut solidaire, le secteur privé quant à lui accorde une place centrale à l'individu et à des intérêts qui lui sont propres. Il parait donc difficile de parvenir à instaurer un dialogue entre deux milieux qui peuvent avoir du mal à se comprendre et à parler le même langage (ENISA, 2017).

Outre cette barrière idéologique, des enjeux de temporalité apparaissent également lorsque le privé et le public travaillent ensemble en matière de cybersécurité. En effet, les agents du secteur privé sont poussés à agir rapidement après qu'un incident soit détecté. En effet, craignant que l'affaire ne s'ébruite et de façon à pouvoir rassurer leurs clients, les acteurs privés sont très réactifs en termes de sanctions contre des personnes impliquées, de diffusion des informations relatives à l'incident et de l'amélioration des mesures de protection et de prévention. À l'inverse, les contraintes bureaucratiques inhérentes à l'identité des acteurs gouvernementaux imposent à ces derniers d'agir de manière beaucoup plus lente. Cette différence entre la culture du privé et du public soulève donc des enjeux lors de la réponse à un incident (Germano, 2014).

Aussi, quand face à un incident, le public, contrairement au privé, a un devoir d'information du public qui implique de communiquer sur l'incident et d'en informer les parties intéressées. Le

fonctionnement et la culture du secteur privé dictent, à l'inverse, de ne pas faire part des attaques subies ou des incidents survenus de manière à ne pas entamer la confiance des utilisateurs et la réputation de l'entreprise (Germano, 2014). Cette différence est exacerbée par les notions même d'incident ou de menace, qui ne revêtent pas forcément la même signification pour les acteurs gouvernementaux et les acteurs privés qui ne perçoivent donc pas les défis et enjeux de la cybercriminalité de la même manière (Germano, 2014).

b) Une vision des partenariats public-privé différente : des intérêts et attentes divergents

Tel que le rappelle Carr (2016), « des partenariats public-privé fructueux sont soit caractérisés par des intérêts communs ou, si les intérêts des partenaires ne sont pas bien alignés, régis par des règles ». Or, dans le cadre des partenariats public-privé en cybersécurité, on ne retrouve ni des intérêts communs, ni des règles en quantité suffisante pour structurer ces partenariats. Ainsi, un des problèmes centraux au cœur des partenariats public-privé est l'écart constaté entre les attentes et intérêts qui incitent les deux parties à entrer dans le partenariat.

Des intérêts dictés par des valeurs divergentes

Comme nous venons de le préciser, le secteur privé et le secteur public sont animés par des valeurs différentes. Si ce dernier accorde une place prédominante à la communauté dans son ensemble et a donc à cœur l'intérêt général, le privé quant à lui est animé par des intérêts économiques individuels. Contrairement à ce qu'attendent les acteurs publics, les entreprises prennent des décisions sur un modèle d'affaires qui répond aux marges bénéficiaires et aux intérêts des actionnaires. Ce qui est dans l'intérêt de la société ne revêt donc pas forcément, et bien souvent pas, d'intérêt pour les entreprises. En effet, il est difficile d'évaluer ou même de retirer une quelconque profitabilité des actions prises dans l'intérêt général (Carr, 2016). Le secteur privé s'investit donc en cyber sécurité en fonction d'une analyse des coûts et bénéfices de cet investissement et non dans l'intérêt du public et de la sécurité nationale, comme le font des acteurs publics (Carr, 2016).

L'enjeu de la protection de la vie privée

Un enjeu sur lequel l'intérêt du public et celui du privé ne s'alignent que rarement est celui de la protection de la vie privée et des données personnelles des individus. En effet, les deux secteurs ne poursuivent pas les mêmes buts. Si le public cherche à recueillir certaines données dans un but affiché de protection du public, notamment de prévention du terrorisme, le privé est quant à lui animé par des fins marketing ou commerciales. Or, depuis les révélations d'Edward Snowden sur le système de surveillance de masse organisé par le gouvernement américain et aidé par le secteur privé, les entreprises privées sont de plus en plus réticentes à partager les données de leurs clients afin de ne plus être associées à un tel système, perçu de manière négative par la population et qui serait donc néfaste pour leur image et leur attractivité aux yeux des consommateurs et clients (Germano, 2014). C'est ainsi qu'alors que de plus en plus de compagnies utilisent des méthodes de cryptages permettant de protéger les données de leurs clients et consommateurs, se pose la question de la transmission des clés de décodage aux autorités publiques lorsque celles-ci ont des mandats au nom de la protection de la société. Dans ces cas, le privé semble faire primer son intérêt et ne pas remettre les données demandées aux autorités. Ce fut, par exemple, le cas lorsqu'en 2014 Microsoft refusa de transmettre au FBI certaines informations (Dupont, 2016), mais c'est également toujours le cas avec Apple, dont les dernières techniques de cryptage des données ne peuvent désormais plus du tout être décryptées, même par Apple et même sur présentation d'un mandat (Etzioni, 2017). Si cela est un avancement pour la cybersécurité et la protection des données personnelles à l'égard des gouvernements et des forces de l'ordre, certains notent néanmoins que cela pourrait avoir des conséquences sur le travail des agences de protection de la sécurité nationale (Comey, 2014).

De son côté, le public semble de plus en plus vouloir protéger la diffusion par les entreprises privées des données personnelles de leurs utilisateurs à des fins non consenties par ces derniers. En atteste la gestion par les pouvoirs publics américains et canadiens des révélations de la diffusion des données d'environ 87 millions de comptes recueillies par Facebook à la société de communication stratégique Cambridge Analytica en mars 2018. Mark Zuckerberg, PDG de Facebook, a ainsi comparu devant le Congrès américain au début du mois d'avril 2018 afin de répondre de l'utilisation par la firme de communication de données recueillies par Facebook à des fins politiques (Wong, 2018). De la même manière, Kevin Chan, directeur de la politique publique de Facebook Canada, a dû rendre des comptes devant un comité de députés sur la protection des données personnelles à Ottawa en avril 2018 (Baillargeon, 2018).

Un manque d'intérêt de la part du privé à contracter des partenariats avec le public

Il a été remarqué par plusieurs auteurs que beaucoup d'entreprises du secteur privé tendent à ne pas voir d'intérêt à entrer dans un partenariat avec les acteurs publics (Dupont, 2016; Germano, 2014). En effet, les entreprises contrôlent à la fois leurs opérations et les infrastructures et possèdent des moyens financiers, techniques et humains bien souvent supérieurs à ceux du public. Elles n'ont de plus pas à composer avec les contraintes bureaucratiques, institutionnelles et constitutionnelles des acteurs publics (Dupont, 2016; Germano, 2014). Ainsi, outre les réticences du privé à collaborer avec le public et émanant des différences d'intérêts mentionnées précédemment, le secteur privé se sent suffisamment outillé et capable de faire face aux défis et enjeux de cybercriminalité seul. Dans ce cas, une collaboration ponctuelle basée sur les besoins de l'entreprise et faisant suite à une menace réelle et tangible sera préférée à un partenariat basé sur une approche proactive (Germano, 2014).

c) Une participation citoyenne limitée

Un constat qui se dégage à la lumière des stratégies de cybersécurité est la faible considération accordée au potentiel des

citoyennes et citoyens à contribuer de manière proactive à la prévention et la lutte contre la cybercriminalité. Pourtant, tel que le remarque Luiijf et ses collègues, « la plupart des stratégies nationales de cybersécurité reconnaissent la nécessité d'une approche faisant appel à l'ensemble de la société : citoyens, entreprises, secteur public et gouvernement. » (2013, p. 27) Les stratégies proposent toutefois rarement des actions qui incorporeraient les citoyens comme participants actifs à l'élaboration et la mise en œuvre d'initiatives de cybersécurité et prévention de la criminalité.

Il est intéressant de noter le rôle variable attribué aux citoyennes et citoyens dans le cadre de partenariats public-privé axés sur la prévention de la cybercriminalité. Dans la plupart des cas, le citoyen est considéré comme un acteur passif; certaines informations lui sont partagées par les partenariats public-privé, notamment par le biais d'outils ou de campagnes de sensibilisation qui lui sont destinés afin qu'il sécurise ses propres systèmes. Par exemple, l'initiative luxembourgeoise SECURITYMADEIN.LU offre sur sa plateforme des outils et services ayant pour objectif d'améliorer la cybersécurité des organisations et individus[60]. Dans cette optique, la contribution citoyenne à la lutte contre la cybercriminalité est sous forme d'une responsabilisation individuelle, sans que le partage et la collaboration avec les entités publiques ou privées ne soient bilatéraux.

Certaines initiatives sollicitent tout de même une certaine forme de participation citoyenne lorsqu'il s'agit de recueillir des informations de la part du public, notamment lorsque celui-ci est victime d'un cybercrime. Par exemple, le partenariat public-privé Signal Spam, en France, consiste en une plateforme nationale de signalement des spams[61]. Les internautes sont invités à signaler ce qu'ils considèrent comme étant un spam dans leur messagerie à Signal Spam, qui se charge ensuite de transmettre l'information aux autorités pouvant mettre en œuvre une action adaptée.

Toutefois, la citoyenne ne s'avère pas sollicitée dans une optique de co-construction des solutions pour la prévention et la lutte contre la cybercriminalité. Ces dernières sont évidemment confrontées à l'enjeu particulier qu'elles nécessitent une connaissance approfondie et actuelle des technologies de l'information et des communications pour être en mesure d'enquêter sur ces crimes. Ces connaissances sont non seulement très spécialisées, mais leur accès est également très restreint (Jakobi 2015).

Les enjeux liés à la structure des partenariats public-privé

a) La responsabilité des acteurs : un aspect absent des partenariats

Certains auteurs (Paquet-Clouston, Décary-Hétu & Bilodeau, 2017) ont pu démontrer qu'en matière de cybersécurité, tant le secteur privé, tels que les opérateurs de services ou les entreprises, que le secteur public, tels que les législateurs ou les organismes d'application de la loi, semblent éluder leurs responsabilités. Chacun pour des raisons qui lui sont propres, ces acteurs ont donc tendance à ne pas prendre les mesures adéquates et appropriées pour prévenir et lutter contre la cybercriminalité. Du côté du secteur public, les gouvernements et législateurs semblent ainsi hésiter à introduire des mesures législatives plus sévères et plus nombreuses (Carr, 2016) alors que les actions de répression des agences de l'application de la loi semblent, elles, être davantage isolées et ponctuelles que partie intégrante d'une stratégie de lutte à la cybercriminalité (Paquet-Clouston, Décary-Hétu & Bilodeau, 2017). Les acteurs privés, de leur côté, refusent de prendre en charge ou d'assumer les responsabilités découlant d'une cyberattaque visant leurs clients ou consommateurs, ou visant la sécurité nationale (Carr, 2016). En attestent les récents scandales abordés précédemment et ayant touchés Équifax, agence américaine de crédit dont les clients se sont vus voler leurs données confidentielles (développés dans le Chapitre 2), ou encore Facebook, dont les utilisateurs ont vu leurs informations privées utilisées à des fins politiques par une compagnie tiers. Dans ce dernier cas, les deux acteurs mis en cause, Facebook et Cambridge Analytica, se renvoient la faute, Facebook avançant que la compagnie de communication a utilisé les données à des fins non autorisées par Facebook et Cambridge Analytica affirmant avoir obtenu l'aval du réseau social.

Cette caractéristique individuelle de chaque acteur se retrouve également au niveau collectif. En effet, l'enjeu de l'imputabilité reste mal défini voire absent dans les partenariats public-privés (Carr, 2016). Ainsi donc, ces outils de coopération visant à sécuriser le cyberespace et à empêcher l'occurrence d'incidents ou à lutter contre ceux-ci n'établissent pas de règles claires d'imputabilité (Carr, 2016).

b) Collaboration

Le maintien de la confiance entre les différentes parties

Une des barrières principales à la collaboration entre les acteurs notamment dans le cadre d'un partenariat public-privé est la confiance (Germano, 2014). En effet, des différences de valeurs et d'intérêts mentionnées précédemment peuvent naitre une certaine méfiance ou suspicion envers l'autre et sa capacité à prendre des mesures considérées comme constructives et appropriées. Ainsi, en cas d'incident, le privé et le public ayant des approches de résolution du problème opposées en termes de réactivité et de transparence, comment le privé peut-il s'assurer que le public ne s'ingérera pas dans son fonctionnement (Germano, 2014)? De son côté, comment le public peut-il s'assurer que le privé prendra les mesures adéquates et l'en informera? En atteste l'exemple de la compagnie de crédit Equifax, qui n'a révélé les faits que plus d'un mois après en avoir pris connaissance, et quatre mois après les premiers incidents. De la même manière, la protection de la sécurité nationale peut conduire un gouvernement à adopter des lois et politiques permettant un plus grand contrôle et une plus grande supervision des contenus postés en ligne. Cela pourrait donc contraindre les compagnies de la technologie et de l'information à restreindre ou supprimer certains

contenus. Le privé pourrait donc subir une censure du public au nom de la protection de la société et de la lutte au terrorisme par exemple. De son côté, le public doit avoir confiance dans le fait que les plateformes numériques assureront leur rôle de vigilance en rapportant les contenus illégaux et/ou dangereux.

Outre la difficulté à développer la confiance entre les différents partenaires, un enjeu supplémentaire qui se présente est de maintenir ce niveau de confiance à long terme (ENISA, 2017). La plupart des partenariats public-privé européens recensés dans l'étude de l'ENISA (2017) ont décrit le maintien du lien de confiance avec les partenaires comme une démarche continuelle, qui nécessite à la fois des relations personnelles et un investissement de temps considérable. Au cours de l'évolution d'un partenariat public-privé, le lien de confiance peut facilement être érodé, si par exemple de nouveaux membres se joignent au partenariat, d'anciens membres n'y sont pas suffisamment actifs, ou dans l'éventualité où certains membres tirent profit des services offerts par le partenariat sans pour autant contribuer aux tâches préalablement définies (ENISA, 2017).

Le partage d'informations

Le partage d'informations est considéré vital pour la lutte contre la cybercriminalité (Forum économique mondial, 2017). Cette mesure est fréquemment au cœur des activités des partenariats public-privés. Au Royaume-Uni par exemple, le Cyber Security Information Sharing Partnership (Partenariat de partage d'informations en cyber sécurité, ou CiSP selon l'acronyme en anglais) est une initiative entre le gouvernement et le secteur privé pour échanger des informations en matière de cyber menaces (National Cyber Security Centre, 2018). Aux États-Unis, le National Cybersecurity and Communications Integration Center (Centre national d'intégration de la cybersécurité et des communications, ou NCCIC selon l'acronyme en anglais) sert également de plateforme centrale de partage d'informations où une variété de partenaires impliqués en cybersécurité et protection des communications coordonnent et synchronisent leurs efforts (US-CERT, 2018).

À la fois le secteur public et le secteur privé reconnaissent la nécessité de partager certaines informations afin de mieux prévenir et lutter contre la cybercriminalité. En effet, comme nous l'avons mentionné à plusieurs reprises, aucun acteur seul ne peut y parvenir, et les criminels partageant eux-mêmes des informations afin de s'adapter à l'évolution continuelle de la technologie, il est important que les victimes et agents de prévention et de répression en fassent autant (Forum économique mondial, 2017; Germano, 2014). Ainsi, partager l'information permet de limiter les conséquences néfastes d'une cyberattaque et d'aider les forces de l'ordre, mais également de prévenir les incidents (Forum économique mondial, 2017).

Néanmoins, comme l'indique Carr (2016), l'échange d'informations dans le cadre d'un partenariat public-privé revêt trois enjeux. Premièrement, il est parfois difficile pour une entreprise de faire rapidement la distinction entre un problème technique, une cyberattaque de faible envergure ou une attaque d'une grande ampleur qui puisse avoir des conséquences durables. De plus, pour les raisons évoquées précédemment, il peut paraître plus stratégique pour une entreprise de tenter de comprendre et régler le problème avant que ses compétiteurs ne soient au courant de l'attaque. Partager des informations au sujet de sa vulnérabilité avec les acteurs publics, notamment la police ou la justice, peut aller à l'encontre de ses intérêts commerciaux, et trouver une solution par elle-même peut lui permettre d'acquérir un avantage par rapport à ses compétiteurs. Finalement, une agence privée de sécurité peut être réticente à partager des informations avec le gouvernement, en sachant que celles-ci pourraient être partagées avec ses compétiteurs. Le modèle d'entreprise des agences privées de sécurité est d'obtenir de l'information dans l'optique de la revendre par la suite, et non de la partager. De son côté, la capacité du public à partager certaines informations classifiées peut être limitée aux seuls acteurs du privé ayant une côte de sécurité suffisante (Carr, 2016).

Face à cette problématique, plusieurs réflexions ont été entamées afin de surmonter ces difficultés et de pouvoir organiser l'échange d'informations entre le public et le privé. Le Forum Économique Mondial, organisation internationale rassemblant des multinationales de tous les pays, a ainsi publié en 2017 un guide sur le partage d'informations entre le public et le privé contre la cybercriminalité (Forum Économique Mondial, 2017). Après avoir rappelé l'importance du partage d'informations, mais également les difficultés qu'il présente, le guide s'attèle à répondre à trois questions centrales : quelles informations partager ? Avec qui ? Et comment ? En ce qui concerne le **type de données à partage**r, une attente partagée aussi bien par le secteur privé que par le secteur public est d'obtenir des alertes et informations par rapport à une cybermenace en temps opportun afin de pouvoir réagir promptement. Néanmoins, la collaboration entre le privé et le public est marquée par un manque de clarté sur la nature précise et la profondeur de ces données (Germano, 2014). Le Forum économique mondial (2017) répond à cette problématique en listant cinq types d'informations que les secteurs public et privé devraient s'échanger : des données relatives aux attaques, comme les indicateurs de compromission, le modus operandi des criminels, les facteurs causaux, mais également des informations relatives aux pratiques des acteurs, comme les meilleures pratiques et les leçons apprises ainsi que les mesures de prévention, détection et protection. De plus, le Forum économique mondial (2017) met en lumière les enjeux à prendre en considération afin de partager de manière efficace ces données. Ainsi, les acteurs devraient partager non seulement les données qu'ils sont légalement obligés de divulguer, mais aussi celles pour lesquels ils n'ont aucune obligation légale, tant qu'il ne leur est pas interdit de les partager. En effet, les acteurs, surtout les entreprises, possèdent de nombreuses informations précieuses pour les forces de l'ordre qu'ils ne partagent pas, en l'absence d'obligation légale, et par peur de divulgation auprès de leurs compétiteurs. Il est néanmoins important de rappeler que ces données ne doivent à l'inverse pas être frappées d'une interdiction d'être partagées, sans quoi la protection de la vie privée et des données personnelles des individus ne pourrait être garantie. Il est donc recommandé aux acteurs du privé et du public souhaitant partager certaines

informations de vérifier le cadre normatif en vigueur afin de ne pas divulguer d'informations protégées. En outre, afin d'accélérer l'analyse des renseignements, il est recommandé de partager des données traitées et non brutes, ce qui permet de plus de réduire le risque de partager des informations personnelles ou sensibles. Enfin, le Forum (2017) rappelle que l'échange doit être réciproque, sans quoi aucun des acteurs n'y verrait d'intérêt.

Le deuxième enjeu du partage d'information entre le public et le privé concerne **les méthodes d'échanges**. Une condition à ces échanges est pour les acteurs de bien se connaitre. En effet, il convient que de bonnes relations soient établies, mais également que chaque partie puisse s'assurer que la partie à qui les données sont transmises est fiable et ne se servira pas des données à des fins autres que celles définies par le partenariat, posant par la même l'enjeu de confiance mentionné précédemment (Forum économique mondial, 2017). Il convient également d'impliquer les bonnes personnes, notamment les gestionnaires seniors, et les ressources suffisantes et nécessaires (United States General Accounting Office, 2001). Une transmission via des méthodes sécurisées, telles que le cryptage, est une condition à un partage sécuritaire d'informations potentiellement sensibles (United States General Accounting Office, 2001). Enfin, pour certaines données, notamment les rapports d'incidents, un échange en continu, 24h/24 est préférable, afin de permettre une réponse rapide et efficace (Forum économique mondiale, 2017).

c) Manque de diversité des parties privées impliquées

Comme mentionné précédemment il existe au sein des acteurs privés un manque d'intérêt à s'impliquer dans un partenariat public-privé. Mais il existe un autre enjeu relatif à leur implication, spécifique aux petites et moyennes entreprises (ENISA, 2017). En effet, outre le manque d'intérêt, ces dernières ne se sentent pas concernées ni par les enjeux de cybersécurité ni par les partenariats publics-privés (Germano, 2014). Il a ainsi été remarqué que certaines entreprises, du fait de leur petite taille, ne se sentent pas menacées et ne se perçoivent pas comme des victimes potentielles de cyberattaques. Elles sont donc moins enclines à participer à des mesures de lutte ou de prévention contre la cybercriminalité. Ceci d'autant plus que participer à un partenariat public-privé nécessite du temps et des ressources humaines que les petites et moyennes entreprises n'ont bien souvent pas (ENISA, 2017; Germano, 2014).

Néanmoins, comme le note Germano (2014), un dialogue autour des enjeux et des dangers de la cybercriminalité est amorcé, ce qui pourrait permettre une sensibilisation des entreprises ne se sentant pas concernées et leur implication dans des partenariats. De la même façon, la transformation des normes réglementaires et de responsabilité civile mettrait en lumière les risques encourus par les entreprises ne prenant pas les mesures nécessaires pour prévenir ou répondre à une cyberattaque. Les entreprises réaliseraient donc la nécessité d'être proactives en matière de cybersécurité (Germano, 2017).

Recommandations

Cette section présente quelques recommandations qui se rapportent au développement et à la mise en œuvre de partenariats public-privé en cybersécurité.

Établir une terminologie et classification communes

Tel que vu tout au long de ce rapport, les acteurs impliqués en cybersécurité et cybercriminalité sont confrontés à une absence de terminologies et classifications communes en matière de cybercrimes. Ces lacunes génèrent des enjeux particuliers dans le cadre de partenariats public-privé, alors que les partenaires impliqués peuvent ne pas partager une compréhension commune des menaces. Au-delà du partage d'informations, il importe donc d'être en mesure de partager une terminologie commune en matière de cybercriminalité.

Favoriser le développement d'un lien de confiance entre les partenaires

Le lien de confiance entre les partenaires ne peut être immédiat; il doit être cultivé au fil du temps. Les membres du partenariat doivent s'assurer de faire preuve de transparence, et de communiquer de manière franche et ouverte, aussi bien avec les autres partenaires qu'au sein de leur propre organisation. Ce niveau de confiance peut se traduire par une croyance mutuelle que chaque membre du partenariat pourra retirer des bénéfices de son implication comme dans tout partenariat, en particulier ceux impliquant du partage d'informations, il est essentiel d'établir un cadre précis qui définisse (1) quels sont les rôles des acteurs publics et privés impliqués; (2) quelles sont les relations entre ces acteurs; (3) quels sont les domaines dans lesquels ils coopèrent (ENISA, 2011a).

Mettre en place un cadre pour assurer l'imputabilité des partenaires

Tel que mentionné auparavant dans ce chapitre, les partenariats public-privé (qu'ils soient en cybersécurité ou d'autres domaines) impliquent un enjeu de taille : la responsabilité en lien avec les actions n'incombe pas à un seul partenaire, comme ce peut être le cas dans le cadre d'initiatives purement gouvernementales, mais bien à une diversité d'acteurs issus des secteurs privé et public. Cette responsabilité partagée complexifie l'imputabilité lors d'erreurs commises, qui dans le cyberespace peuvent porter atteinte à une masse critique d'individus.

Des mécanismes doivent donc être élaborés afin que non seulement le secteur privé puisse rendre ses comptes au secteur public, mais que l'inverse se produise également. Des mécanismes doivent être mis en œuvre afin que chaque partenaire puisse démontrer son engagement dans le partenariat (Forrer, Kee, Newcomer, & Boyer, 2010).

Forrer et ses collègues (2010) proposent six dimensions qui peuvent servir de cadre pour évaluer l'imputabilité dans un partenariat public-privé :

- **Les risques** en lien avec les actions du partenariat doivent être clairement identifiés et compris par tous les partenaires. Par la suite, un accord doit être conclu pour déterminer quel partenaire est le plus en mesure d'assumer les responsabilités en lien avec ce risque.
- Une analyse des **coûts et bénéfices** doit être effectuée afin de déterminer quels projets seront les plus appropriés pour le partenariat.
- Une analyse des **impacts sociaux et politiques** du partenariat doit également être réalisée.
- Il importe de s'assurer que **l'expertise** de chaque partenaire, en particulier des acteurs du secteur privé, a été bien identifiée, est mise à profit de manière efficace dans le cadre du partenariat, et fait l'objet d'un suivi adéquat.
- En matière de **collaboration entre les partenaires**, plusieurs éléments doivent être pris en considération. Chaque organisation prenant part au partenariat doit pouvoir compter sur des représentant(e)s faisant preuve de leadership et étant en mesure de s'assurer qu'en cas d'erreurs, les individus responsables répondent de leurs actes. Une communication constante et claire entre les différents partenaires est également essentielle, tout comme une gestion des projets efficaces. Puis, tel que mentionné précédemment, une stratégie devrait être mise en place pour développer et maintenir un lien de confiance entre les partenaires.
- Des **mesures de rendement** doivent être utilisées pour veiller à la mise en œuvre du partenariat et l'obtention des résultats attendus de celui-ci.

Au-delà d'une approche de prévention situationnelle pour prévenir la cybercriminalité

Il ressort de l'ensemble de nos développements, que l'approche de prévention préconisée dans le cadre des partenariats public-privé est presque exclusivement situationnelle ; la prévention des cyberattaques s'effectue par l'entremise d'une sécurisation accrue des systèmes d'information et le partage de connaissances entre acteurs pour faciliter la détection de menaces. L'objectif se veut de réduire les opportunités de commettre des cyberattaques. Or, tel que l'expliquent Kavanagh et ses collègues dans le cas de l'utilisation d'Internet et de technologies de l'information et des communications à des fins terroristes, ces mesures de cybersécurité en ligne ne permettront pas de lutter contre les facteurs hors ligne à la base de ces activités criminelles (2016) et de prévenir ainsi en amont ce type de problématique. Au contraire, elles se concentrent sur l'empêchement d'actions, alors que les conditions pour la commission de crimes sont déjà établies. Ce type d'approche se révèle « préventive-réactive » et ainsi, fondamentalement défensive. Il est par conséquent impératif de développer des initiatives de prévention d'un autre ordre, par exemple de prévention sociale ou proactives, qui puissent contribuer de manière fondamentale à la prévention d'actes cybercriminels.

Conclusion

Ce chapitre avait pour objectif de présenter les grandes tendances actuelles en ce qui concerne notamment les partenariats public-privé en cybersécurité. Ce tour d'horizon aura notamment permis de démontrer que la gestion de relations qui se veulent horizontales telles que dans le cadre de partenariats public-privé implique son lot de défis. En ce qui concerne les partenariats élaborés à des fins de cybersécurité et de prévention de la cybercriminalité, ces défis se voient davantage compliqués par les difficultés intrinsèques à la gouvernance d'une entité aussi vaste et en constante évolution que le cyberespace. Toutefois, il importe de préciser qu'il est difficile d'obtenir des données en provenance du secteur public; la plupart des sources disponibles sont issues du milieu privé ou partiellement financées par celui-ci. Cela engendre deux problèmes : les sujets abordés seront d'intérêt pour le secteur privé, négligeant potentiellement ainsi des enjeux ou aspects qui pourraient être d'utilité pour le public. La seconde problématique est que seule la perspective du privé est obtenue, ce qui engendre peu de remises en cause par rapport à la nécessité d'impliquer le privé en tant qu'acteur central et indispensable en cybersécurité. De plus, les enjeux présentés se rapportent principalement à l'amélioration de modalités d'implication bénéfiques pour le privé. Tel que vu tout au long de ce rapport, il est pertinent d'envisager la possibilité que d'autres modèles de gouvernance, comprenant d'autres acteurs, soient adaptés à la prévention de la cybercriminalité, ainsi qu'à d'autres modèles de prévention.

Contribution

Les PPP : un objectif stratégique d'une stratégie nationale de cybersécurité

Élaboré par l'Agence européenne pour la cybersécurité (ENISA)

Introduction

Alors que la société devient de plus en plus dépendante des technologies de l'information, la protection et la disponibilité des actifs essentiels deviennent un sujet d'intérêt national. Les incidents perturbant les infrastructures et les services informatiques pourraient avoir des effets négatifs majeurs sur le fonctionnement de la société et de l'économie. Aussi, la cybersécurité est de plus en plus considérée comme un enjeu national horizontal et stratégique qui touche les divers niveaux de la société.

Le 6 juillet 2016, la directive sur la sécurité des réseaux et des systèmes d'information (la directive NIS) a été adoptée et est entrée en vigueur en août 2016. La directive NEI impose aux États membres de l'UE d'élaborer et d'adopter une stratégie nationale de cybersécurité (NCSS). Si nécessaire, les États membres peuvent faire appel à l'ENISA pour les aider à rédiger un NCSS. Dans les trois mois suivant l'adoption de leur NCSS, les États membres de l'UE doivent transmettre la stratégie à la Commission européenne.

Les stratégies nationales de cybersécurité sont les principaux documents des États nations pour établir des principes stratégiques, des lignes directrices et des objectifs afin d'atténuer les risques associés à la cybersécurité. De fait, la cybersécurité est une responsabilité partagée et repose donc fortement sur la collaboration.

L'ENISA - l'Agence européenne pour la cybersécurité - travaille dans le domaine des stratégies nationales de cybersécurité (NCSS) depuis 2012. L'objectif de l'ENISA est de soutenir les États membres de l'UE dans leurs efforts pour développer, mettre en œuvre et évaluer leur NCSS en fournissant des outils et des lignes directrices en ligne.

Une législation européenne comme la stratégie de cybersécurité de l'Union européenne : « Un cyberespace ouvert, sûr et sécurisé et une communication conjointe sur la résilience, la dissuasion et la défense : Construire une cybersécurité forte pour l'UE», encourage la nécessité d'une coopération public-privé dans le domaine de la cybersécurité ainsi que l'importance d'instaurer la confiance par le biais de partenariats public-privé.

Establishing Private Public Partnerships

L'un des objectifs stratégiques communs à toutes les stratégies nationales européennes en matière de cybersécurité est la collaboration pour améliorer la cybersécurité à tous les niveaux. Du partage de l'information sur les menaces à la sensibilisation, la collaboration se fait souvent par le biais de partenariats public-privé (PPP).

Dans la majorité des pays, les entreprises privées possèdent des infrastructures essentielles et les services essentiels sont fournis par le secteur privé. Par conséquent, un degré élevé de communication et de coopération peut être un moyen efficace pour les gouvernements de comprendre les besoins et les défis des entreprises privées, mais aussi de s'assurer que les mesures nécessaires sont mises en œuvre pour atteindre un degré de sécurité suffisant.

Le partenariat public-privé peut être un outil efficace de deux façons :

- en mettant en commun l'expertise et les ressources des secteurs privé et public ;
- en établissant une portée, des objectifs et une méthodologie de travail communs pour atteindre des buts communs.

La coopération avec le secteur privé en Bulgarie en est un exemple :

> Partenariat public-privé - L'amélioration de la cybersécurité nécessite une approche combinée, multisectorielle et globale qui met l'accent sur la création d'une cyberorganisation «pangouvernementale» qui inclut la coopération avec les entreprises privées et met l'accent sur l'éducation du citoyen. Les possibilités d'accroître la participation du secteur privé et de faire en sorte que nous tirions parti de leur expertise devraient inclure l'examen conjoint des pratiques exemplaires et des procédures afin de s'assurer qu'aucune partie de l'infrastructure essentielle, qu'elle soit entre les mains du secteur public ou privé, ne devienne un maillon faible et vulnérable.

En 2011, l'ENISA a publié un **guide de bonnes pratiques sur les modèles coopératifs efficaces de PPP**. L'étude révèle les cinq principales composantes associées à la création et au maintien des PPP en répondant aux questions suivantes :

- **Pourquoi,** en se référant à la **portée et à la menace**. L'idée ici est d'identifier le problème réel et d'essayer de le résoudre en couvrant tous les aspects possibles. Il est important que les membres potentiels comprennent clairement la pertinence du PPP pour leur propre organisation. Cela les aidera à justifier leur implication auprès de leur propre direction. C'est également vrai lorsque l'adhésion est obligatoire, elle déterminera le niveau de participation.
- **Qui,** en se référant à la **couverture et le lien**. Avoir des gens passionnés par ce qu'ils font est la clé de cette étape. Un PPP peut impliquer des partenaires au niveau national, paneuropéen ou international et son orientation peut être thématique, sectorielle ou intersectorielle.

- **Comment,** en se référant à la **gouvernance**. L'organisation et la gestion d'un PPP nécessitent une réflexion approfondie. L'organisation d'un PPP, la façon dont les partenaires travaillent ensemble, ses règles et son financement peuvent avoir un impact clé sur le succès d'un partenariat. La gouvernance d'un PPP a été définie comme critique par tous les PPP étudiés.
- **Quoi,** se référant **aux services et aux incitations**. Avoir quelque chose de concret à offrir, écouter les membres et fournir ce qu'ils demandent est crucial pour la réussite d'un PPP.
- **Quand,** se référant **au démarrage et à la durabilité**. Il est très important de comprendre comment les PPP se développent et évoluent. Les organisations du secteur public devraient prendre en considération la stratégie réussie utilisée par de nombreux PPP, en commençant par une approche descendante et en faisant croître le PPP de bas en haut au fil du temps.

Enfin, l'étude recueille des données auprès des parties prenantes des secteurs public et privé et fournit des conseils sur la manière de créer un partenariat et d'aider les parties prenantes à choisir facilement les aspects qui ajouteront de la valeur à leurs efforts dans la mise en place et le fonctionnement des PPP.

En 2017, l'ENISA a mené une étude sur les **modèles coopératifs pour le partenariat public-privé** (PPP) en rassemblant des informations sur les meilleures pratiques et les approches communes. Cette recherche analyse

- le **statut des PPP dans l'UE**,
- identifie les principaux **modèles de collaboration**,
- les **défis actuels** auxquels sont confrontés le secteur privé et le secteur public lors de la mise en place et du développement des PPP, et
- fournit des r**ecommandations pour le développement des PPP** en Europe.

Aujourd'hui, plus de 15 États membres ont établi un partenariat public-privé officiel, une augmentation par rapport à 2012. Dans de nombreux cas, des partenariats sont créés pour mener un projet spécifique, c'est-à-dire un exercice national de cybersécurité ou une campagne de sensibilisation à la cybersécurité (Mois européen de la cybersécurité). Il est très important de noter que depuis le premier Guide de bonnes pratiques, des PPP sectoriels ont été créés dans l'UE à la suite de l'approche des États-Unis. On observe une fois de plus une indication de la maturité et de la sophistication de l'approche de la cybersécurité.

En analysant les PPP en Europe, il est évident que la culture est l'un des déterminants les plus importants concernant la manière dont les partenariats public-privés sont établis, développés et fonctionnent. Il n'existe pas de scénario universel sur la manière de créer un PPP réussi ; ce qui fonctionne parfaitement dans un pays peut être délicat et difficile dans un autre. Cela s'explique principalement par les différences culturelles et par le fait que les relations générales entre le secteur public et le secteur privé diffèrent d'un État membre à l'autre. Dans certains pays, la formalité est la partie la plus importante du PPP, tandis que dans d'autres, le pragmatisme est plus important.

Sur la base de l'étude ENISA - Cooperative Models for Public - Private Partnerships, les types de PPP développés en Europe sont les suivants :

- **PPP institutionnel.** Dans ce type, l'ensemble de l'institution travaille dans le cadre d'un PPP. Habituellement, ce type d'institution offre de nombreux services, tels que la recherche, l'analyse, l'élaboration de bonnes pratiques et de lignes directrices, le service d'assistance, les audits de sécurité et certains services plus ciblés. Ce PPP est lié à la protection des infrastructures essentielles. En effet, l'institution est chargée de la protection de ces dernières par un acte juridique (la loi sur la gestion des situations d'urgence/de crise par exemple). Une solution appropriée est la coopération dans le cadre du PPP avec les secteurs critiques. Les moyens communs de coopération sont les groupes de travail, les groupes d'intervention rapide et les communautés à long terme. L'objectif est de sécuriser les infrastructures critiques en général, ainsi les cybermenaces sont considérées comme des éléments importants dans le paysage de la menace.
- **PPP axé sur les objectifs**. Les PPP de ce type sont créés dans le but de créer une culture de la cybersécurité dans les États membres. Il existe généralement une plate-forme ou un conseil qui réunit les secteurs privés et publics pour échanger des connaissances et des bonnes pratiques. L'objectif pour les membres est de se concentrer autour d'un sujet ou d'un but spécifique.
- **Externalisation des services PPP.** Les PPP de ce type sont des initiatives créées par le gouvernement et le secteur privé. Leur tâche principale est de sensibiliser les parties prenantes à la cybersécurité et à la cybersécurité. Ces PPP peuvent en fait être considérés comme une tierce partie pour les services d'externalisation qui répondent aux besoins de l'industrie et soutiennent le gouvernement dans le processus d'élaboration des politiques (par exemple, la mise en œuvre des NEI, l'élaboration de stratégies nationales de cybersécurité).
- **PPP hybride.** Ce type de PPP comprend les CSIRT fonctionnant dans le cadre d'un PPP. Dans ce cas, les gouvernements décident de confier à une entité expérimentée - ayant déjà une expérience avérée dans l'exploitation du CSIRT - la prestation de services du CSIRT à l'administration publique ou à l'ensemble du pays.

Enfin, quelques recommandations basées sur les principaux défis sont analysées dans l'étude 2017 de l'ENISA pour aider les PPP à être plus efficaces et à évoluer au sein de l'UE.

Construire la confiance dans les PPP

L'établissement et le maintien de la confiance entre les entités publiques-privées, privées-privées et publiques-publiques a été reconnu comme l'un des plus grands défis des PPP ; la plupart des PPP définissent la confiance comme un processus continu qui implique des relations personnelles et prend beaucoup de temps.

Il existe plusieurs mécanismes qui soutiennent le renforcement de la confiance et sont utilisés par les PPP, tels que les réunions régulières, les réunions en face à face, les événements sociaux, les conférences thématiques, les exercices conjoints.

Les réunions en face à face, les réunions régulières et les événements sociaux sont considérés comme les outils les plus efficaces pour bâtir la confiance, car ils contribuent à bâtir des partenariats à long terme. L'interaction qualitative personnelle entre les membres du PPP est considérée comme un point clé pour la réussite du PPP.

Dans le processus de construction de la confiance, le besoin d'un «manager» serait considéré comme un catalyseur car il/elle serait quelqu'un qui croit en la cause de, qui est dévoué à la présence et au maintien de celle-ci et par cette attitude inspire d'autres à s'impliquer et à collaborer.

Les PPP avec un haut niveau de confiance sont évidemment plus efficaces - ils reconnaissent les besoins des secteurs public et privé et sont capables d'y répondre par la coopération.

La motivation du secteur privé à participer est une priorité lors de la mise en place d'un PPP

Ce qui est clairement visible dans chaque modèle de PPP analysé est le fait que pour créer un PPP réussi et efficace, des ressources sont nécessaires. Ce genre de collaboration a besoin d'une force motrice pour les stimuler, afin qu'elle soit vraiment vitale. Il ne suffit pas de fournir des incitations et de l'argent. Les PPP ne se développeront pas s'il n'y a pas assez de personnes pour y travailler. Un PPP a vraiment besoin de quelqu'un qui interagit avec chaque membre du partenariat ; il dirige l'ordre du jour, organise la réunion et conserve une perspective stratégique. Les PPP ont besoin d'un groupe entier de personnes qui préparent les plans d'action et travaillent en étroite collaboration avec l'administration publique et l'industrie. Les PPP les plus sophistiqués sont généralement des ONG ou des institutions créées uniquement pour établir et renforcer la coopération et la collaboration entre les secteurs public et privé.

Promotion du concept de PPP auprès des petites et moyennes entreprises (PME)

Il est courant que les grandes entreprises soient le plus souvent impliquées dans les PPP. Les PME n'ont pas les ressources nécessaires pour s'impliquer et la plupart du temps, elles ne se rendent pas compte que la participation à un PPP pourrait être bénéfique pour elles. Il serait également utile, d'un point de vue sociétal, d'impliquer d'autres types de parties prenantes comme les PME et les jeunes pousses dans le PPP afin d'acquérir de l'expérience auprès d'acteurs plus importants dans ce domaine.

Les institutions publiques à la tête du PPP ou du plan d'action national pour les PPP

La cybersécurité étant hautement interdisciplinaire, il existe généralement de nombreux organismes publics impliqués dans les PPP - Ministère de l'Intérieur, Ministère de la Défense, Ministère de l'Économie ou du Développement pour n'en citer que quelques-uns. Il est très important que l'administration publique communique clairement et honnêtement ses besoins et ses limites au secteur privé.

Le point de contact n'est peut-être que l'aspect le plus visible, la pointe de l'iceberg. Mais ce qui est beaucoup plus important, c'est le fait que les entités gouvernementales impliquées dans un PPP devraient savoir à l'avance - c'est-à-dire avant d'inviter des partenaires du secteur privé à y adhérer - ce qu'ils veulent réaliser, ce que leur contribution va entraîner et ce que le secteur privé devrait apporter. En d'autres termes, il faut mettre au point la stratégie avant d'adhérer au PPP.

Il est très frustrant pour les représentants du secteur privé d'assister à des désaccords entre les principales institutions publiques. Le secteur privé s'attend à ce que le gouvernement agisse. Si le secteur public pouvait convenir d'un point de contact unique pour les PPP, cela pourrait être extrêmement bénéfique pour l'ensemble du PPP.

Le PPP concerne la coopération privé-privé, public-public et privé-public et privé-public. Se concentrer uniquement sur les relations entre le secteur public et le secteur privé pourrait être une vision à très court terme pour la politique de PPP. Le bon niveau de dialogue et de compréhension entre les organismes publics est souvent la clé du succès d'un PPP.

Il en va de même pour le secteur privé. Le PPP réussi intègre non seulement l'administration privée et l'industrie, mais aussi différentes entités de l'industrie (par exemple, des sociétés d'énergie, des banques, des télécommunications).

Pour cette raison, les PPP dans l'ensemble de l'UE devraient également se concentrer sur la coopération et la collaboration entre le secteur privé et le secteur privé et le secteur public et le secteur public.

Conclusion

Il est évident que les partenariats nécessitent un cadre clair précisant les rôles des secteurs public et privé, leurs relations et les domaines de coopération. Si les organisations doivent faire face à des exigences réglementaires et/ou non ré-

glementaires cohérentes, simples et efficaces, la coordination public-privé doit être optimisée.

L'ENISA soutient les États membres de l'UE sur la manière de développer les PPP en fournissant des recommandations, de bonnes pratiques, des lignes directrices et en réunissant les parties prenantes pour collaborer, échanger des points de vue et des informations. **La cybersécurité est une responsabilité partagée** et l'ENISA, avec la communauté, va de l'avant et travaille à rendre la collaboration et le partage de l'information et des connaissances plus forts et plus fiables. Les efforts multiformes de l'ENISA dans le domaine de la cybersécurité soutiennent et renforcent une Europe plus sûre et plus sûre sur le plan cybernétique.

Notes

56 http://www.europeanfinancialcoalition.eu/

57 https://www.first.org/

58 Établie en juin 2016, l'ECSO est une association sans but lucratif (ASBL) dont l'objectif est de soutenir toute initiative visant à développer et promouvoir la cybersécurité en Europe. Elle rassemble plus d'une cinquantaine d'organisations publiques et privées et représente la contrepartie contractuelle dirigée par le secteur privé à la Commission européenne pour la mise en œuvre du partenariat public-privé (https://ecs-org.eu/about).

59 La question des partenariats public-privé dans les stratégies nationales de cybersécurité sera approfondie par l'ENISA dans sa contribution à ce chapitre.

60 https://securitymadein.lu/tools/

61 https://www.signal-spam.fr/

Références

ANSSI. (2016). Adoption de la directive network and information security (NIS) : l'ANSSI, pilote de la transposition en France. Repéré à https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

Avina, J. (2011). Public-private partnerships in the fight against crime: An emerging frontier in corporate social responsibility. Journal of Financial Crime, 18(3), (p.282-291), https:// doi.org/10.1108/13590791111147505

Baillargeon S. (2018). À Ottawa, des députés outragés ont affronté des dirigeants de Facebook. Le Devoir. Repéré à https://www.ledevoir.com/culture/medias/525624/facebook-a-livre-un-peu-ouvert-au-parlement-d-ottawa

Bechkoum, K., Thomas, P., Campbell, L., & Brown, M. (2017). Towards Stronger Cyber Security Public Private Partnerships in Developing Countries. Gloucestershire, Angleterre: University of Gloucestersmahire.

Busch, N. E., & Givens, A. D. (2012). Public-private partnerships in homeland security: Opportunities and challenges. Homeland Security Affairs, 8(18). Repéré à https://www.hsaj.org/articles/233

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. International Affairs, 92(1), 43-62.

Comey, J. (2014). Going dark: Are technology, privacy, and public safety on a collision course? (Speech). Washington, DC: Brookings Institution. Repéré à http://www.fbi.gov

CIPC, World Bank Sustainable Development Department for Latin America and the Caribbean, Chambre de commerce de Bogotá, & Instituto Sou da Paz. (2011). Public-Private Partnerships and Community Safety: Guide to Action.

Dunn Cavelty, M., & Brunner, E. M. (2007). Introduction: information, power, and security—an outline of debates and implications. In M. Dunn Cavelty, V. Mauer, & S. F. Krishna-Hensel (Éd.), Power and security in the information age: investigating the role of the state in cyberspace (p. 8-9). Burlington, Vermont: Ashgate Publishing.

Dunn Cavelty, M., & Suter, M. (2009). Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. International Journal of Critical Infrastructure Protection, 2(4), 179-187.

Dupont, B. (2016). La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale. Cultures & Conflits, 102.

Dupré, L. (2014). EP3R 2010-2013: Four Years of Pan-European Public Private Cooperation. Héraklion, Grèce: L'Agence européenne chargée de la sécurité des réseaux et de l'information.

ECSO. (2018). About the cPPP. Repéré à https://ecs-org.eu/cppp

ECSO. (2018). About ECSO. Repéré à https://ecs-org.eu/about

ENISA. (2011a). Cooperative Models for Effective Public Private Partnerships: Desktop Research Report. Héraklion, Grèce: L'Agence européenne chargée de la sécurité des réseaux et de l'information.

ENISA. (2011b). Cooperative Models for Effective Public Private Partnerships: Good Practice Guide. Héraklion, Grèce: L'Agence européenne chargée de la sécurité des réseaux et de l'information.

ENISA. (2017a). Cooperative Models for Information Sharing and Analysis Centers (ISACs). Héraklion, Grèce: L'Agence européenne chargée de la sécurité des réseaux et de l'information. Repéré à https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

ENISA. (2017b). Cooperative Models for Public Private Partnership (PPP). Héraklion, Grèce: L'Agence européenne chargée de la sécurité des réseaux et de l'information. Repéré à https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

Etzioni, A. (2017). The fusion of the private and public sectors. Contemporary Politics, 23(1), 53-62.

FIRST. (2014). FIRST Members around the world. Repéré à https://www.first.org/members/map

Forrer, J., Kee, J. E., Newcomer, K. E., & Boyer, E. (2010). Public–Private Partnerships and the Public Accountability Question. Public Administration Review, 70(3), 475-484. https://doi.org/10.1111/j.1540-6210.2010.02161.x

Forum économique mondial. (2017). Guidance on Public-Private Information Sharing against Cybercrime (No. 040117 00026464). Genève, Suisse : Forum économique mondial

Gal,S (2002). A semiotics of the public/private distinction. Difference: A Journal of Feminist Cultural Studies, 13(1), 77-95

Gardiner, L. (2009). The foundation for corporate citizenship and sustainable businesses. Présenté à VII Annual Local Networks Forum, Istanbul.

Germano, J. H. (2014). Cybersecurity Partnerships: A New Era of Public-Private Collaboration. New York, NY: The Center on Law and Security, New York University School of Law.

Global Forum on Cyber Expertise. (2017). Global Good Practices - National Computer Security Incident Response Teams (CSIRTS).

Gobierno de España. (2013). National Cyber Security Strategy.

Irion K. (2013) The Governance of Network and Information Security in the European Union: The European Public-Private

Partnership for Resilience (EP3R). In: Krüger J., Nickolay B., Gaycken S. (eds) The Secure Information Society. Springer, London

Jakobi, A. P. (2015). Non-state actors and global crime governance: Explaining the variance of public-private interaction. The British Journal of Politics & International, 18(1), 72-89.

Kaijankoski, E. A. (2015). Cybersecurity Information Sharing Between Public-Private Sector Agencies. Naval Postgraduate School, Monterey, Californie.

Kavanagh, C., & Porret, M. (2016). Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust. ICT4Peace Foundation; United Nations Counter-Terrorism Committee Executive Directorate.

Le Conseil canadien pour les partenariats public-privé. (2016). Définitions et modèles de partenariats public-privé. Repéré à http://www.pppcouncil.ca/web/Knowledge_Centre/What_are_P3s_/Definitions_Models/web/P3_Knowledge_Centre/About_P3s/Definitions_Models.aspx?hkey=79b9874d-4498-46b1-929f-37ce461ab4bc

Li, B., & Akintoye, A. (2003). An overview of public-private partnerships. In Public-Private Partnerships: Managing Risks and Opportunities. Oxford, Royaume-Uni: Blackwell Science Ltd.

Luiijf, E. Besseling, K & Graag, P. (2013). Nineteen national cybersecurity strategies. International Journal of Critical Infrastructures, 9(1/2), 3-31.

Manley, M. (2015). Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership. Journal of Strategic Security, 8(5), 85-98. http://dx.doi.org/10.5038/1944-0472.8.3S.1478

National Council of ISACs. (2018). About ISACs. Repéré à https://www.nationalisacs.org/about-isacs

National Cyber Security Centre. (2018). Cyber Security Information Sharing Partnership (CiSP). Repéré à https://www.ncsc.gov.uk/cisp

National Security Authority. (2015). National cyber security strategy of the Czech Repubic for the period from 2015 to 2020. Repéré à https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

ONUDC. (2011). Principes directeurs applicables à la prévention du crime. Manuel d'application pratique. Repéré à l'adresse : https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/Handbook_on_the_Crime_Prevention_Guidelines_French.pdf

Paquet-Clouston, M. Bilodeau, B. & Décary-Hétu. (2017). Can We Trust Social Media Data ? Social Network Manipulation by an IoT Botnet. Proceedings of the 8th International Conference on Social Media & Society. Toronto, Canada

Sécurité publique Canada. (2017, juillet 4). Infrastructures essentielles. Repéré à https://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-fr.aspx

SECURITYMADEIN.LU. (2018). Tools and services from the Luxembourg cybersecurity ecosystem. Repéré à l'adresse https://securitymadein.lu/tools/

Tropina, T. (2015). Public-Private Collaboration: Cybercrime, Cybersecurity and National Security. In Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. Springer International Publishing. Repéré à www.springer.com/gp/book/9783319164465

United States General Accounting Office. (2001). Information Sharing: Practices That Can Benefit Critical Infrastructure Protection, GAO-02-24. Washington, D.C.

US-CERT. (2018). National Cybersecurity and Communications Integration Center. Repéré à https://www.us-cert.gov/nccic

Weihe, G. (2005). Public-Private Partnerships: Addressing a Nebulous Concept. Présenté à 10th International Research Symposium on Public Management, Glasgow Caledonian University, Écosse.

Wong, J.C. (2018). Congress grills Facebook CEO over data misuse – as it happened. The Guardian. Repéré à https://www.theguardian.com/technology/live/2018/apr/10/mark-zuckerberg-testimony-live-congress-facebook-cambridge-analytica

Centre international pour la prévention de la criminalité

465, rue Saint-Jean, bureau 803
Montréal (Québec) H2Y 2R6
Canada

+1 514 288-6731

cipc@cipc-icpc.org
www.cipc-icpc.org