Centre
international
pour la
prévention
de la criminalité

International
Centre
for the
Prevention
of Crime

Centro
Internacional
para la
Prevención
de la Criminalidad

6th International Report

CRIME PREVENTION AND COMMUNITY SAFETY: Preventing Cybercrime


PASSWORD

6TH INTERNATIONAL REPORT ON CRIME PREVENTION AND COMMUNITY SAFETY: Preventing Cybercrime

ISBN:
Print: 978-2-924939-01-7
PDF: 978-2-924939-02-4
USB key: 978-2-924939-03-1

Published by:
International Centre for the Prevention of Crime
465 Saint-Jean Street, Suite 803, Montréal, Québec, Canada, H2Y 2R6
Telephone: 1 514 288-6731
Email: cipc@cipc-icpc.org

The report is available in English, French, and Spanish on ICPC's website:
www.cipc-icpc.org

Disclaimer:
The editorial content of the 6th International Report on Crime Prevention and Community Safety represents the views and findings of the authors alone and not necessarily those of sponsors, or supporters, or those consulted in its preparation.

The International Centre for the Prevention of Crime (ICPC), located in Montreal, Canada is the leading crime prevention institution at the international level. It has been promoting international standards of crime prevention and criminal justice with the goal of advancing community safety and improved quality of life for more than 20 years. ICPC works with member governments, international institutions, local authorities and organizations in the Americas, Europe, Africa, and Oceania, by offering a knowledge base on crime prevention; policies, practices and tools to reduce risk factors associated with crime, violence and insecurity.

This publication was funded mainly by Public Safety Canada.

Editorial and Production Team: the 6th International Report on Crime Prevention and Community Safety was produced under the supervision of Ann Champoux, ICPC Director General.

Editor in chief: Pablo Madriaza Ph. D

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

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

Production Manager: Anne Onana

Translation: Tony Kwan

The Report also beneficiated from the collaboration of ICPC staff members: Kassa Bourne.

AKNOWLEDGEMENTS

The preparation of the International Report is a major undertaking, and is made possible by the interest and commitment of many people. We would like to thank very sincerely all of ICPC's Staff for their contribution and our Board of Directors 2017-2018 for their support:

- Ms. Chantal Bernier, President
- Professor Peter Homel, Administrator, Griffith Criminology Institute, Griffith University, Australia
- Mr Paul Girard, Treasurer
- Dr Vincenzo Castelli, Administrator, Onlus Nova Consorzio per l'innovazione sociale
- Dr Adam Tomison, Administrator, Australian Institute of Criminology
- Ms Anie Samson, Administrator, Montreal
- Ms Kalpana Viswanath, Administrator, Member of the Steering Committee - Global Network of Safer Cities of UN Habitat and Board Member - International Centre for the Prevention of Crime (ICPC)
- Dr Tina Silbernagl, Administrator, Programme Manager of the GIZ Inclusive Violence and Crime Prevention for Safe Public Spaces (VCP) programme
- Mr Claude A. Sarrazin, Administrator, SIRCO

We also owe our sincere thanks to our members, and to the members of our Scientific Committee who gave us their advice on the selection of topics for the Report, and provided us with valuable information and support. Unfortunately, the timescale for this Report did not allow for an in-person editorial meeting, but we hope that our Board, Members and Scientific Committee will not feel that their views have been misinterpreted. Any errors are ours alone. The members of the Scientific Committee are:

- Mr Kauko Aromaa, Director, European Institute for Crime Prevention and Control (HEUNI), Finland
- Dr Elena Azaola, Centro de Investigaciones y Estudios Superiores en Antropología Social, Mexico
- Dr Benoit Dupont, University of Montreal, Canada
- Professor Peter Homel, Australian Institute of Criminology (AIC) and Asia Pacific Centre for the Prevention of Crime (APCPC) Australia
- Dr Tim Hope, University of Salford, UK
- Dr Azzedine Rakkah, Centre d'Études et de Recherches Internationales (CERI), France
- Dr Elrena van der Spuy, University of Cape Town, South Africa
- Dr Anne Wyvekens, Centre National de la Recherche Scientifique, France

We have received tremendous support from our contributors and their work greatly enriches the report: 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 and Nabi Youla Doumbia.

We received very valuable advice and support from other experts including Dr. Jacqueline Karn from Economic and Social Research Council, UK; Bernardo Perez, UN-Habitat's Consultant; Daniel Ventre and Anne Wyvekens from the CNRS, France; Ehren Edwards and Patrick Hénault from Public Safety Canada; Matti Joutsen, Anni Lietonen, Inka Liljia andNatalia Ollus from HEUNI, Finland; Elena Azaola from Centro de Investigaciones y Estudios Superiores en Antropología Social, Mexico; Katharina Peschke, Johannes de Haan, Nail Walsh and Anika Holterhof from UNODC, Austria.

There are many other policy makers, practitioners and researchers we cannot name individually but whose work and advice has inspired us, and to whom we would like to extend our sincere thanks.

A MESSAGE FROM THE PRESIDENT OF ICPC

Despite numerous variations within countries, we have noticed that «traditional» crime rates have been on the decline since 2003. However, if we consider the evolution of cybercrime over the past years, it is clear that it has not ceased to increase.

The 6th International Report on Crime Prevention and Community Safety is mainly focused on the prevention of cybercrime. The rise in cybercrime attacks, the incidence of this new form of crime on a daily basis and the rising costs associated with cybercrime in several countries show the need to develop new preventive methods and tools.

This Report is intended to provide insights, strategies and initiatives on the subject by providing field workers, governmental and non-governmental institutions an evidence-based data source detailing the state of cybercrime worldwide as well as relevant prevention efforts.

The 6th International Report is the result of sustained teamwork and could not have been published without the contribution of the ICPC's staff and members, but also of academic and institutional partners who have, once, again helped with advice, support and content. I would also like to acknowledge the Government of Canada, whose central contribution made it possible for us all to benefit from the information in this Report.

I hope you will find the data and analyses in this Report to support your own efforts in the prevention of cybercrime.

Chantal Bernier
President, ICPC

A MESSAGE FROM THE DIRECTOR GENERAL OF ICPC

As the new Director General of the International Centre for the Prevention of Crime (ICPC), I had the great honor of coordinating the development and publication of the 6th International Report on Crime Prevention and Community Safety. The 6th edition mainly focuses on the prevention of cybercrime.

With 24 years of expertise in the prevention of crime and security, the ICPC's mission is to promote crime prevention, support and assist communities, municipalities, regions and countries on a global scale.

In a world increasingly focused on sharing expertise and evidence-based crime prevention policies, and with the emergence of the cyberspace in recent years, it is all the more important to consider new emerging forms of crime and to think of preventive tools and methods to counter cybercrime, a phenomenon that is increasingly becoming a central issue at the global level. How does one prevent cybercrime and is it possible to establish a set of preventive norms and models for it?

As part of our mandate, the ICPC wanted to answer these questions through this International Report focusing on the prevention of cybercrime. Each chapter of the 6th edition addresses a dimension of this prevention. As in previous editions, Chapter 1 presents the latest trends in overall crime prevention. Chapter 2 directly addresses cybercrime and lays the foundation for the following chapters. Chapter 3 provides an overview on cybercrime as well as cybercriminal and cybervictim profiles. Chapter 4 discusses the prevention of cybercrime, as well as gaps and initiatives developed in the current context. Finally, chapter 5 presents public and private partnerships in the prevention of cybercrime.

I am very proud of this Report, which is the result of teamwork and collaboration. I would like to thank the entire ICPC staff as well as our contributors for this product of exceptional quality. I hope it will provide you with information and tools necessary to prevent cybercrime, and implement evidence-based strategies and initiatives in the field.

Ann Champoux
Director General, ICPC

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

A

ASEAN: Association of Southeast Asian Nations

APSA: African Peace and Security Architecture

AU: African Union

B

BEC: Business Email Compromise

BSA: Business Software Alliance

C

CCJPC: Commission on Crime Prevention and Criminal Justice

CCPPP: Canadian Council for Public-Private Partnerships

CCSPJP: Citizen Council for Public Safety and Criminal Justice

CCSS: CARICOM Crime and Security Strategy

CERT: Brazilian National Computer Emergency Response Team

CIIP: Critical Information Infrastructure Protection

CSIRT: Computer Security Incident Response Team

D

DARE : Drug Abuse Resistance Education

E

ECOSOC: United Nations Economic and Social Council

ECSO: European Cyber Security Organisation

ENISA: European Network and Information Security Agency

EP3R: European Public-Private Partnership for Resilience

ESCWA: United Nations Economic and Social Commission for West Asia

EU: European Union

EU IRU: Europol Internet Referral Unit

EUCPN: European Crime Prevention Network

F

FBI: Federal Bureau of Investigation

G

GDPR: General Data Protection Regulation

H

HIV: Human Immunodeficiency Virus

HR: Homicide Rate

I

IC3: Internet Crime Complaint Center

ICMEC: International Centre for Missing and Exploited Children

ICPC: International Centre for the Prevention of Crime

IDB: Inter-American Development Bank

IETI: Critical Information Technology Infrastructure

ILO: International Labour Organization

ISAC: Information Sharing and Analysis Center

ISSM: Information Systems Security Manager

ITU: International Telecommunication Union

L

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

LIST OF ACRONYMS AND ABBREVIATIONS

N

NIS : Network and Information Security

O

OAS: Organization of American States

OECD: Organisation for Economic Co-operation and Development

OLAF: European Anti-Fraud Office

P

PADO: Programa de Alta Dedicación Operativa

PROMEVIL: Promotion of new city jobs

PSD: Peace and Security Department

PSP: National Public Safety Partnership

R

RTM : Risk Terrain Modeling

S

SQF: Stop, Question, and Frisks

U

UN: United Nations

UN Women: United Nations Entity for Gender Equality and the Empowerment of Women

UNGASS: United Nations General Assembly Special Session

UNICEF: United Nations Children's Fund

UNODC: United Nations Office on Drugs and Crime

V

VRN : Violence Reduction Network

W

WHO : World Health Organization

LIST OF CONTRIBUTORS

Alex Kigerl

Ph. D, Assistant Research and Professor of Criminal Justice and Criminology, Washington State University
USA

Anna Sarri

National Cyber Security Strategies Team
European Network and Information Security Agency
Greece

Belisario Contreras

Cybersecurity Program Manager
Organization of American States
USA

Benoit Dupont

Professor, University of Montreal
Scientific Director of the Smart Cybersecurity Network (SERENE-RISC)
Canada Research Chair for Security, Identity, and Technology
Canada

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

Criminal Analysis Department of Carabineros de Chile and Mathematical Modelling Centre of the University of Chile (CEAMOS)
Chile

Cécile Doutriaux

Lawyer
Cyberdefense Chair Member of the Saint-Cyr Schools
France

Dimitra Liveri

National Cyber Security Strategies Team
European Network and Information Security Agency
Greece

Eleni Darra

National Cyber Security Strategies Team
European Network and Information Security Agency
Greece

ENISA

The European Union Agency for Network and Information Security
Greece

Jeff Hearn

Professor Emeritus
Hanken School of Economics
Finland

Jérôme Barlatier

Squadron Commander
Central Criminal Intelligence Unit (SCRC)
France

Judith Germano

Senior Fellow, NYU Center for Cybersecurity (CCS)
NYU Center on Law & Security (CLS)
Adjunct Professor of Law, NYU School of Law
USA

Karuppannan Jaishankar

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

Kerry-Ann Barrett

Cybersecurity Policy Specialist
Organization of American States
USA

Matthew Hall

Ulster University
Associate Academic and Researcher
UK

Nabi Youla Doumbia

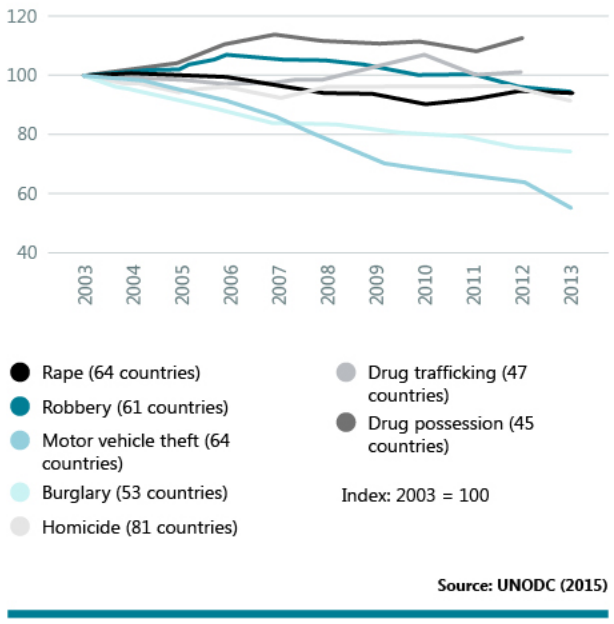
Ph.D in Criminology, University of Montreal
Research Coordinator for the project: "Homicides en Afrique"
Canada

INTRODUCTION AND SYNTHESIS OF CURRENT TRENDS AND KNOWLEDGE

If there is one fact that clearly emerges from the work done to prepare the preceding two ICPC International Reports (ICPC, 2014, 2016) it is that, notwithstanding the enormous variations between regions and countries, crime rates for traditional offences have been falling steadily since 2003, with the notable exception of drug-related crimes.

In contrast, cyberspace is constantly growing in importance. This observation led us to pose the following question: is there a relationship between the decline in traditional types of crime and the growing significance of cyberspace? One possible hypothesis is that the global decrease in crime does not necessarily portend the disappearance of traditional types of crime, but rather their transformation as they migrate towards cyberspace. This, however, is a difficult hypothesis to prove due to the lack of relevant data. As we shall see in Chapter 2, current data largely reflects the economic interests of private businesses. In effect, the categories used for defining "crimes" or "victims" are broad, highly disputed and depend exclusively on information provided by the clients of private businesses. As such, the resulting datasets are not representative of global realities.

Figure 1. **Global trends of selected crimes, 2003-2013**



Source: UNODC (2015)

Although this may seem to be a difficult hypothesis to prove, it is impossible to deny cyberspace's importance in contemporary daily life, particularly in relation to crime. In effect, cybercrime has gone beyond the status of a mere emerging issue to become a major problem in most countries worldwide. Cybercrime prevention has therefore become an issue that demands immediate response. That bring said, is it possible to prevent cybercrime? Do effective prevention models or frameworks exist? As with conventional forms of crime or other phenomena, such as radicalization leading to violence, prevention has been something of an afterthought in policy responses to cybercrime. Research has focused more on cybersecurity and situational prevention rather than on prevention in a broader sense. Moreover, cybersecurity chiefly addresses the security issues affecting private businesses and the digital infrastructure rather than those affecting individuals. In effect, notwithstanding the evident difficulties of situating cybercrime in a traditional geographic space and the tendency to focus on cross-border factors, most individual victims reside in specific geographic locations. The main challenge, then, is to first identify the mechanisms required to understand cyber-victimization processes, and then implement the most effective prevention strategies based on the interface between delocalized crime and its local victims. Of course, the question of individual victims has been addressed in research studies and specific prevention measures do exist. However, as the focus has essentially been on victims' behaviour rather than on the actions of offenders or, at a deeper level, the relevant criminogenic factors, such prevention approaches remain incomplete and largely underdeveloped.

Tous These considerations have led us to produce an International Report focusing exclusively on the topic of cybercrime prevention, with the express purpose of identifying the shortfalls in terms of information and prevention approaches. In contrast with preceding International Reports in which different issues were addressed around specific topics, this edition was conceived of as an integrated whole in which each chapter tackles a particular dimension of cybercrime prevention. As with past editions, Chapter 1 provides an update on the general trends in crime prevention. Consequently, the topic of cybercrime is actually introduced in the Report's core chapter, Chapter 2. Essentially, Chapter 2 serves to contextualize the problem of cybercrime as well as the principal topics addressed in the following chapters. The topic of Chapter 3 is cyber-criminology, i.e., the study of cybercrime, cybercriminals and victims of cybercrime. In Chapter 4, we examine prevention per se by presenting in-depth discussions of the prevention measures implemented to date. In addition, this chapter discusses the problem of information gaps. Finally, Chapter 5 examines a fundamental dimension of global governance in cybercrime prevention: public-private partnerships.

International Report on Crime Prevention and Community Safety

The International Report is the flagship publication of the International Centre for the Prevention of Crime (ICPC). Every two years, the ICPC does a comprehensive review of the new trends in crime prevention to spur discussion and debate on prevention practices and public policy. In addition to its analysis of global trends in crime prevention, the International Report has also examined specific topics in-depth since its 4th edition. As previously mentioned, the principal topic of this edition is cybercrime prevention.

As with the preceding reports, this edition examines prevention from several angles. The report begins with an in-depth examination of relevant empirical research. That said, from the perspective of prevention, other instruments exist that also have significant influence on practical efforts to reduce victimization and build safer communities. These other instruments, which include international norms and standards, national strategies and local practices, also warrant attention. In effect, this report draws on the work of UN and regional organizations, proven and/or promising practices, policy debates and discussions, and academic research. In keeping with the ICPC's mission, the object of this report is to foster open dialogue between research and practice, that is to say between researchers, decision-makers and practitioners..

This report's intended target audience is comprised of three key sectors: decision-makers and elected officials mandated to build safer and more inclusive societies at global, state and local levels; practitioners or professionals whose activities have a major influence on building safer and healthier communities, such as the law enforcement and justice system, social workers or healthcare professionals, teachers, civil society or NGOs; and the research community, including universities and institutes which contribute to producing and delivering knowledge and information designed to assess the effectiveness, costs and benefits of current and past prevention policies and practices.

The information presented in this report is drawn from a wide range of sources, including reports produced by UN agencies, international or regional institutions such as the World Bank, the European Commission, the African Union, ASEAN or the Organization of American States, national or local governments, reports produced by NGOs, as well as sources originating from research institutions or academia. As always, the ICPC's vast international network, composed of governments and member organizations active in the field of crime prevention and community safety, remains a privileged source of information.

The ICPC published its 5th International Report in 2016 analyzing the role of cities in matters of public safety and crime (see Box No. 1 for a summary of the topics addressed in preceding editions). The 5th edition of the Report also underscored the importance of the United Nations Conference on Housing and Sustainable Urban Development, Habitat III, held in Quito in October 2016. The 5th International Report stressed the fact that urban dynamics and certain characteristics of cities often have an influence on crime and violence just as, conversely, certain urban factors can be conducive to crime prevention and development beneficial to individuals and communities.

Box 1. **International Reports on Crime Prevention and Community Safety: 2008 - 2016**

Preceding International Reports have examined trends in crime, crime prevention, community safety and insecurity, as well as addressed specific subjects and topics.

Among the topics addressed in past reports:

2008: women's safety, youth safety, school safety, safety in public spaces

2010: migration, organized crime, drugs and alcohol

2012: human trafficking and exploitation, informal settlements, post-conflict and post-disaster areas, drug production in developed countries

2014: migration and the displacement of persons within and across borders

2016: cities and the New Urban Agenda

Trends in crime prevention and community safety:

2008: international crime prevention norms and standards, international crime prevention networks, national and local strategies; knowledge-based prevention; the role of institutional actors, particularly the police and justice system actors; new services in support of security in everyday life (private security, mediation and conflict resolution); enhancing the role of local governments and community stakeholders

2010: principal trends in crime prevention; good governance (decentralization, legitimacy issues, regulation of private security, broadening the role of civil society); social and educational approaches; training, professional development and capacity building; assessing crime prevention effectiveness

2012: global survey on security strategies in cities and neighbourhoods

2014: indigenous migration, prevention of human trafficking, intimate partner violence

2016: principal trends in crime and its prevention; urban safety; territory and public safety policies from a Latin American perspective; public transportation and crime prevention; drug consumption in urban contexts; and radicalization leading towards violence in cities.

Topics addressed

Chapter 1. Trends in crime and its prevention

The object of Chapter 1 is to summarize the main statistical trends in crime and present an overview of crime prevention efforts around the world. Chapter 1 is divided into three parts. Part I focuses on the international trends in crime. In particular, we took a closer look at seven different topics: homicides, homicides of women, violence against children and youth, urban violence, drug-related crime, incarceration rates and the feeling of insecurity. Part II focuses on recent crime prevention efforts of international and regional organizations, particularly UN-affiliated organizations. Finally, Part III offers a survey of the latest empirical studies related to the topic at hand. To that end, a literature review was done on the scientific literature containing analyses of empirical data published between 2015 and 2017. The object of this review was to summarize the most recent crime prevention information. That, in turn, enabled us to provide a realistic picture of the prevailing interests and concerns in the global research community. Three main topics were analyzed in this report: research on the community and urban policing approach; the role of the police in prevention, particularly as regards its use of crime analysis; and the relationship between youth and delinquency. This chapter's most important findings are as follows:

- Although Latin America remains the region with the highest homicide rates in the world, this violence is concentrated in certain countries of the region. Moreover, violence is, in turn, concentrated in certain cities of those countries and in certain sectors of said cities. El Salvador and Honduras have the world's highest national homicide rates. However, Brazil and Mexico are home to the majority of the world's most violent cities. Based on national averages, 25% of the world's homicide victims in 2015 were women. Violence against children and youth is practically a universal phenomenon, existing in both rich and poor countries.
- Analysis of the initiatives of international organizations clearly indicates the importance of significant cooperation and coordination between the countries and regions of the world, particularly in connection with a handful of justice-related issues such as organized crime, terrorism, cybercrime, human trafficking, drug-related crimes, and so on. Unfortunately, most cooperation initiatives put more emphasis on criminal justice than on prevention.
- Our review of the literature found information concerning the importance given to community and civic policing initiatives, particularly in African and Asian countries. Typically, such initiatives focus on neighbourhood watch and control, thereby replicating a traditional model of policing. Also apparent was the growing global importance of crime analysis for the purpose of crime prevention, particularly in police departments in South America. Finally, recent studies have shown that actions based on punitive prevention and rehabilitation, increased sentencing and aggressive policing approaches are not effective in preventing crime.

Chapter 2. Crime in a digital world

In Chapter 2, we problematize our approach to cybercrime phenomena. To that end, we begin with an examination of cyberspace (i.e., the specific environment where cybercrime occurs) by specifically focusing on governance issues and factors of inequality. In the chapter's second section, we consider the difficulties intrinsic to quantifying cybercrime, difficulties which are structural, methodological and conceptual in nature. Finally, in the third section we propose a somewhat impressionistic global overview of cybercrime, based on our review of the available data and information.

A number of interesting observations emerged from this chapter:

- Cyberspace forms a very particular environment with its own specific conditions and dynamics, many of which are crucial to understanding cybercrime phenomena. In particular, cyberspace's sui generis governance model decentralizes the responsibilities of ensuring security and protection, and combating and preventing crime. As such, these responsibilities are no longer the exclusive jurisdiction of public sector authorities. This situation has resulted in a "governance gap," which facilitates the operation of cybercriminal activities and affects the security of all internet users.
- Moreover, cyberspace constitutes a milieu that is distinct from the real world. Although real world factors and conditions influence virtual world factors and conditions, they are not identical to them. Thus, while "macro" issues bearing on inequalities identified in the real world (economic, social, developmental, gender-related, etc.) influence the construction of virtual inequalities (digital access, skills and usage issues), the latter nonetheless are embedded in a distinct system of inequality.
- The two preceding points are crucial to our understanding of the cybercrime and cyber victimization phenomena. In effect, one does not observe direct correlations between cyberspace dynamics (whether such affect criminals and/or victims) and the inequalities observed in the real world;

correlations are instead indirect, transformed and complicated through the prism of cyberspace. Researchers must, therefore, confront a major challenge: rethinking their theories on crime in the context of cyberspace.

- The study of cybercriminal activities is challenging due to their extremely heterogeneous nature, which is subject to rapid and constant evolution. Nevertheless, several key aspects are readily apparent and of particular interest to the field of prevention. First of all, the current state of knowledge concerning the factors conducive to cybercriminal activities (and to cyber-victimization) remains quite underdeveloped. It would appear, based on the small number of studies on the subject that correlations exist between the classic factors of the real world (e.g., those described in the ecosystemic approach to risk factors) and cybercrime. However, these correlations seem indirect and dependent on very specific processes and articulations, which are transformed by the transition from the real world to cyberspace, an environment characterized by distinct conditions.
- Finally, there are major gaps in the available data that are of highly varying quality. Nevertheless, certain preliminary conclusions may be drawn from this data regarding the differentiated spatial distribution of various cybercrime phenomena, the emergence of geographic poles of cybercrime characterized by specific activities, and particular modes of governance.

Chapter 3. Cybercrimes, cybercriminals and cybervictims

Chapter 3 proposes an overview of current criminological research on cybercrime. What is meant by the term cybercrime? What is known about the different types of cybercrime? Who are the perpetrators and who are the victims? These are the questions on criminologists' research agendas. Additionally, as scholars endeavour to answer these questions, they are simultaneously seeking to determine whether criminology's traditional theories on delinquency and victimization are useful in the new environment that is cyberspace or whether new approaches are needed to better apprehend this subject. Consequently, our first step will be to examine the different definitional perspectives in the scientific literature, as well as the principal theories applied for understanding the various types of cybercrime. Next, we examine the advances made in criminology in relation to three phenomena in particular: hacking, cyberfraud and cyberviolence.

Several findings emerged from this overview:

- The definition of cybercrime is a subject of debate in the research community. Cybercrimes are sometimes considered "old wine in new bottles," sometimes "new wine in new bottles" and sometimes "old wine – without the bottles." As a result, different researchers use different definitions in accordance with their respective research interests. This results in highly disparate datasets, which render the making of comparisons a methodologically challenging exercise.
- The paucity of data on individual victims is due to the fact that the latter do not report crimes to the competent authorities, either because they lack the relevant knowledge or because they have little confidence that action will be taken by the justice system. As for institutional victims, they generally fail to report cybercrimes crimes due to the fear of damage to their reputations.
- The absolute impossibility of developing characteristic profiles, generally applicable to cybercriminals or, for that matter, to cybercrime victims. There are as many profiles as there are cybercrimes.
- Theories from traditional criminology do generate some results, but much work is still needed to better understand cybercrime. Moreover, researchers are working on developing new theories specific to cyberspace.

Chapter 4. Cybercrime prevention approaches

Today, cyberspace is the subject of theoretical and practical debates in relation to crime prevention. A number of governments use the terms cybersecurity and cybercrime interchangeably and focus their efforts on protecting critical information infrastructure at the expense of much needed preliminary reflection on crime prevention in cyberspace. The object of this chapter is to take a fresh look at the principal developments in traditional approaches to crime prevention – i.e., the developmental, environmental and partnership approaches – in this new context. To that end, it begins by clearly differentiating between cybersecurity and cybercrime, both conceptually and operationally. Finally, in this chapter we analyze the application of these traditional approaches, based on the different measures taken to prevent some of the most frequently cited crimes in international conventions, namely cyberbullying, online sexual exploitation of minors, and cyberfraud. A number of interesting aspects emerged in this chapter:

- The prevalence of international and multilevel cooperation: in light of the multiple risk factors and the fact that cybercrime is unfettered by borders, efforts to prevent it imply international and multilevel cooperation in areas such as harmonizing legal frameworks, information sharing and disseminating promising practices.
- An integrated approach: combating these crimes requires an integrated approach, involving actors, such as the criminal justice system, youth protection services, the IT sector, the educational sector, health care and law enforcement, all working together from the vantage point of developmental and environmental prevention.
- Knowledge development: proper development of crime prevention initiatives requires large quantities of information, particularly regarding specific risk factors. However, knowledge in relation to the changes of traditional risk factors arising from internet use remains quite limited.

Chapter 5. Public-private partnerships in cybercrime prevention

The fifth and final chapter tackles the question of public-private partnerships in cybersecurity, particularly in relation to cybercrime prevention. The chapter begins by defining the concept of the public-private partnership before examining its emergence into crime prevention.

The second part of the chapter provides an overview of public-private partnerships in cybercrime prevention, followed by a description of the stakeholders in these types of partnerships and of their partnership implementation and development approaches, including the specific components thereof. Third, comes a brief survey of international public-private partnerships and national strategies focusing on cybercrime prevention. Fourth, comes a discussion on the issues encountered in such partnerships. This chapter concludes with a few recommendations.

A number of findings emerged from this chapter:

- As we have underscored elsewhere in this report, cyberspace implies a particular governance model, one requiring the involvement of a variety of actors assuming responsibilities traditionally attributed to the public sector, such as security management. In effect, the private sector is gradually coming to be recognized as an indispensable actor in cybersecurity, given its ownership of infrastructure, which is not only subject to cyberattacks, but is also instrumental in both facilitating and preventing them. This notion of the private sector's indispensable role is largely taken as a given in the literature, despite the potentially problematic central role it plays in knowledge production on security issues.
- The majority of prevention measures implemented as part of public-private partnerships concern situational prevention, mainly with the goal of protecting critical infrastructure. Although knowledge of the factors explaining cybercrime and cyber-victimization remains very limited, the expert resources in public-private partnerships nevertheless tout their potential for contributing significantly to the social prevention of cybercrime. However, mobilizing the private sector in prevention initiatives that do not generate immediate impacts remains a major challenge, as attests the experience in crime prevention more generally.
- Finally, in certain respects, the issues encountered in the framework of public-private partnerships in cybercrime prevention are the same as in any partnership between the public and private sectors. Divergences in terms of institutional identities, interests and expectations, as well as perceptions of conflicting values, are not unique to cybercrime prevention. However, such issues are perhaps more salient in cyberspace where the private sector plays a preponderant role.

References

ICPC. (2014). 4th International Report on Crime Prevention and Community Safety. Montreal: International Centre for the Prevention of Crime. Retrieved from http://www.crime-prevention-intl.org/en/publications/report/report/article/4e-rapport-international-sur-la-prevention-de-la-criminalite-et-la-securite-quotidienne.html

CPC. (2016). 5th International Report on Crime Prevention and Community Safety: Cities and the New urban Agenda. Montreal : International Centre for the Prevention of Crime. Retrieved from http://www.crime-prevention-intl.org/en/publications/report/report/article/5e-rapport-international-sur-la-prevention-de-la-criminalite-et-la-securite-quotidienne-les-vi.html

UNODC. (2015). State of crime and criminal justice worldwide. Report of the Secretary-General (A/CONF.222/4). UN Congress on Crime Prevention & Criminal Justice. Doha: UNODC.


CROSS
CRIME
SCENE

CHAPTER 1

TRENDS IN CRIME AND ITS PREVENTION

The object of Chapter 1 is to summarize the main statistical trends in crime and present an overview of crime prevention efforts around the world. Chapter 1 is divided into three parts. Part I focuses on the international trends in crime. In particular, we took a closer look at seven different topics: homicides, homicides of women, violence against children and youth, urban violence, drug-related crime, incarceration rates and the feeling of insecurity. Part II focuses on recent crime prevention efforts of international and regional organizations. Finally, Part III offers a survey of the latest empirical studies related to the topic at hand. To that end, a literature review was done on the scientific literature containing analyses of empirical data published between 2015 and 2017. The object of this review was to summarize the most recent crime prevention information. That, in turn, enabled us to provide a realistic picture of the prevailing interests and concerns in the global research community. Three main topics were analyzed in this report: research on the community and urban policing approach; the role of the police in prevention, particularly as regards its use of crime analysis; and the relationship between youth and delinquency.

Introduction

As with previous editions of the ICPC's International Report, the objective of Chapter 1 is to provide an overview of the main trends in crime and its prevention.

The organization of this chapter is somewhat different, in comparison to past editions. To that end, revisions were made to the general indicators addressed in the last five editions of the Report, through which we identified the seven principal topics addressed in the first part of this chapter. In addition, we conducted a review of the scientific literature containing empirical data, published between 2015 and 2017. The object of this review was to describe the most recent information on crime prevention and in so doing, provide a realistic global picture of the priorities and concerns guiding research in this field.

This chapter is divided into three parts. Part I provides an overview of the main global trends in crime. Part II discusses the latest developments in crime prevention at the international, regional and national levels, particularly at the level of international and national organizations. Finally, in Part III, we examine three topics which emerged from the literature review, focusing in particular on the effectiveness of the measures implemented.

Part I – Trends in crime

Notwithstanding efforts made to harmonize how different crimes are categorized, based on the International Classification of Crime for Statistical Purposes (UNODC, 2015a), crime statistics remain a major issue with implications for public policy on crime prevention. For example, in a recent ECOSOC report, Africa and Oceania were not included in its analysis of trends in intentional homicides due to the fragmentary or irregular nature of data from those regions (ECOSOC, 2017). Consequently, the data presented herein must be considered in this context.

Homicides

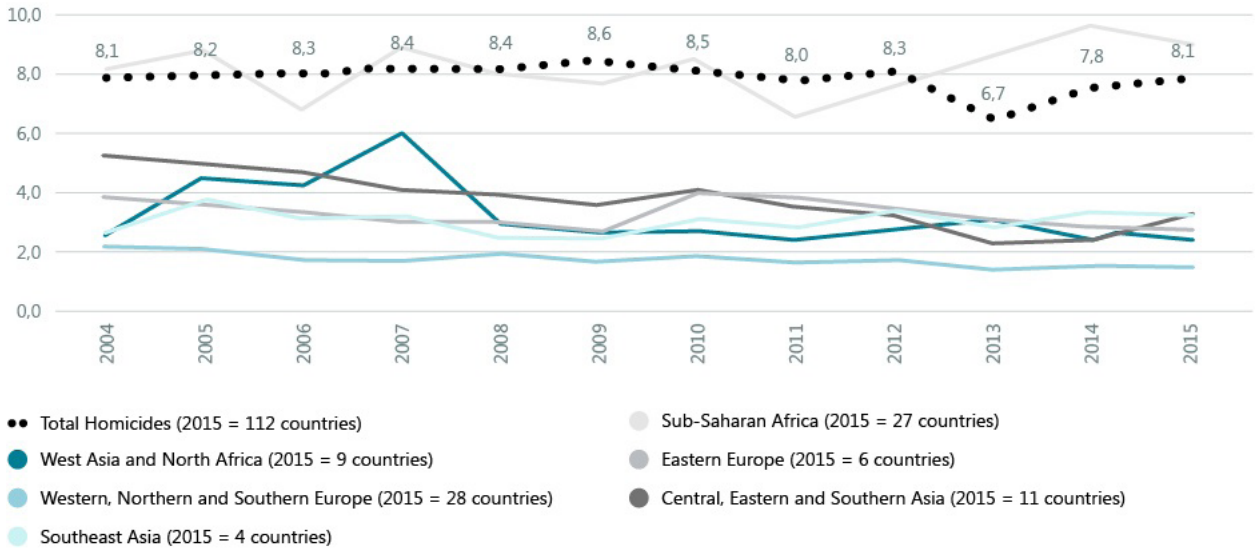
Between 2004 and 2015, the homicide rate (HR) remained relatively stable, at around 8.0 per 100,000 inhabitants (8‰). This statistic, however, does not show the significant variation in regional homicide rates. In effect, crime is not characterized by a homogeneous spatial distribution, but tends to be highly concentrated in specific territories. This spatial heterogeneity can be seen on all scales, from the macro level (some countries have higher crime rates than others) to the local and micro-local level (the majority of criminal activities are concentrated in some cities and, within these cities, certain specific territories).

Box 1.1. **The 10 countries with the highest homicide rates in the world (2015)**

El Salvador	108.6
Honduras	63.8
Venezuela	57.1
Jamaica	43.2
South Africa	34.3
Trinidad and Tobago	30.9
Brazil	26.7
Colombia	26.5
Guyana	19.4
Mexico	16.3

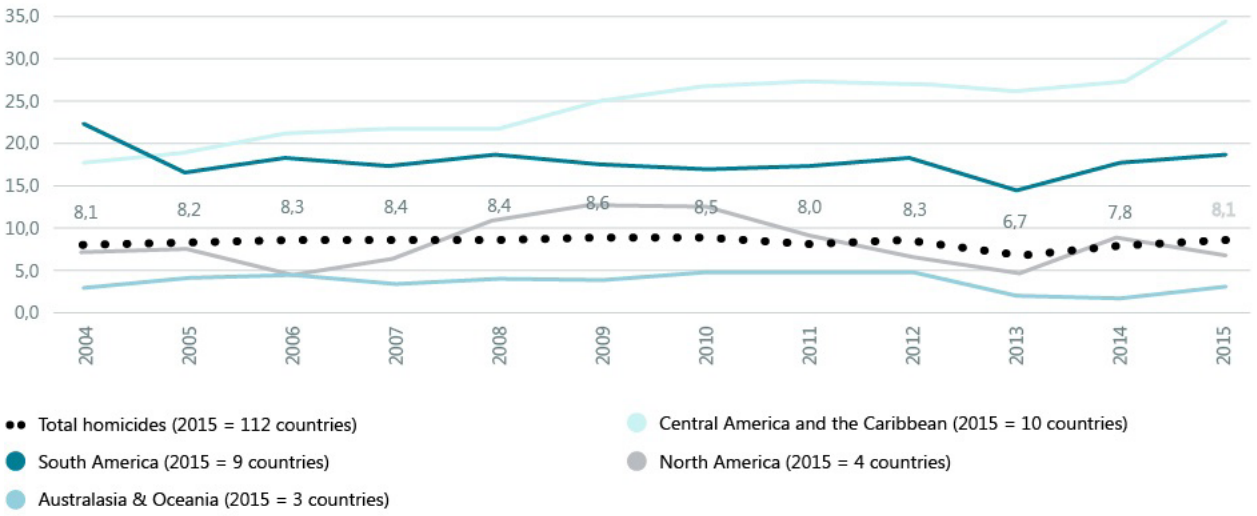
Source: UNODC

Figure 1.1. **Homicide rates per 100,000 population, by region (part 1)**



Source: UNODC

Figure 1.2. **Homicide rates per 100,000 population, by region (part 2)**



Source: UNODC

Figures 1.1 and 1.2 indicate the homicide rates in different regions. Latin America remains the region with the highest HR in the world. This is due in large part to the continuous increase in homicides in Central America and the Caribbean since 2004, including a 24% increase between 2014 and 2015. El Salvador (108.6%ooo) and Honduras (63.8%ooo) are the countries with highest homicide rates in the world. According to data from UNODC Statistics, violence associated with street gangs and organized crime largely accounts for the homicides in both countries. In 2011, 65.4% of the homicides in the Bahamas, 50% in Jamaica and 37.1% in Costa Rica were due to the activities of organized crime and street gangs. In 2012, the corresponding statistic was 16.8% in El Salvador and 52.1% in Panama.

In South America the HR is lower, but quite high nonetheless. Between 2006 and 2012, this region experienced a certain stability with an HR of approximately 18%ooo. Beginning in 2013, its HR began to rise again, reaching 19.1%ooo in 2015, principally due to the high national rates in Venezuela (57.2%ooo), Brazil (26.7%ooo) and Colombia (26.3%ooo). Colombia is an interesting case: although its HR remains very high, it has experienced a gradual decline in homicides since 2004. The opposite occurred in Venezuela as the HR increased from 36.9%ooo in 2004 to 57.2%ooo in 2015. North America experienced a considerable degree of variation between 2004 and 2015, but its HR has been gradually declining since 2009. During this period, the highest HR observed in the region was 12.3%ooo.

UNODC Statistics lack complete data on sub-Saharan Africa, except for the years 2005, 2010 and 2015. The data from those three years is sufficient to indicate an upward trend in the HR since 2011. In 2015, the region's HR was 9.2%ooo, which is above the global average. In the African context, South Africa stands out, as its national HR (34.3%ooo) is fifth highest in the world – and has been trending upwards since 2010. According to the Institute for Security Studies, after a decline between 2004 and 2012, homicides in South Africa increased 22% between 2012 and 2017.[1] The Democratic Republic of the Congo (13.4%ooo) and the Central African Republic (13.1%ooo) also have high homicide rates. In contrast, Cusson et al (2017) observe, in a recently published book, a significant decline in homicide rates in West Africa between 2008 and 2012, with the exceptions of Nigeria and Niger. For example, the HR in Côte d'Ivoire fell by 75%. Likewise, Guinea Conakry and Guinea-Bissau each experienced a decline of 60%. Stable economic growth, democratization and growing middle classes may, according to these authors, be among this trend's explanatory factors, particularly as these developments are connected with an increase in private security services and improved police practices (Cusson et al., 2017).

In Southeast Asia, there has been a relatively slight increase in the HR, particularly since the 2008 economic crisis. In effect, the region's HR increased from 2.5%ooo to 3.3%ooo in 2015. This increase is, however, largely attributable to the Philippines, where the HR increased from 7.5%ooo in 2004 to 9.8%ooo in 2015, an upward trend that is likely to continue in the coming years in the context of violent repression of drug consumers and traffickers, notably marked by the phenomenon of extrajudicial executions (Kreuzer, 2016).

Homicide rates have been declining in the world's other regions. Moreover, the HRs for these regions have been lower than the global average since 2004. The HR is very low in western, northern and southern Europe (1.4%ooo in 2015) and characterized by a slight but constant decline since 2004. Australia's HR dropped 34% between 2004 and 2015 when it reached 0.98%ooo. However, it must be noted that there was an increase in the Middle East and North Africa between 2004 and 2007, after which the HR stabilized at around 3%ooo.

BOX 1.2. **Firearms and mass killings**

In many countries, especially the USA, the relationship between access to firearms and homicide has become the subject of increasing debate mainly due to mass killings that regularly shock public opinion. According to the database maintained on the "Mother Jones" website, between the beginning of 2015 and the month of March, 2018, there were twenty-seven mass shootings in the United States[2] which resulted in 258 persons killed and 728 wounded. In most of these cases, semi-automatic rifles were used. Gun culture and the permissive laws governing the purchase of firearms in the United States are often blamed, with the country having the highest ratio of firearms per capita compared to any country in the world: 89 firearms for every 100 inhabitants (Small Arms Survey, 2007). A recent study estimated that 22% of Americans own firearms, with an ownership average of 4.8 arms per person, which means there are 265 million firearms in the country (Azrael, Hepburn, Hemenway, & Miller, 2017). According to the same study, in 2015, 36,252 deaths were caused by firearms and over 80,000 persons were wounded by firearms; 60.7% of these deaths were suicides and 37.1% were homicides. According to UNODC Statistics in 2012, 60% of the homicides in the United States were caused by firearms versus 32% globally, in 2011.

The relationship between crime and firearms has been widely debated in the United States. Between 1994 and 2004, under the Federal Assault Weapons Ban it was illegal to purchase semi-automatic weapons in the country. An assessment of this ban's impact on violent crime did not indicate a significant effect, due notably to the fact that this type of firearm is not usually used in the commission of violent crimes (Koper, Woods, & Roth, 2004). However, the homicide rate in Mexico increased significantly once this ban was lifted, particularly in border cities (Chicoine, 2017), which could indicate a correlation, most likely made possible by significant arms trafficking between the two countries.

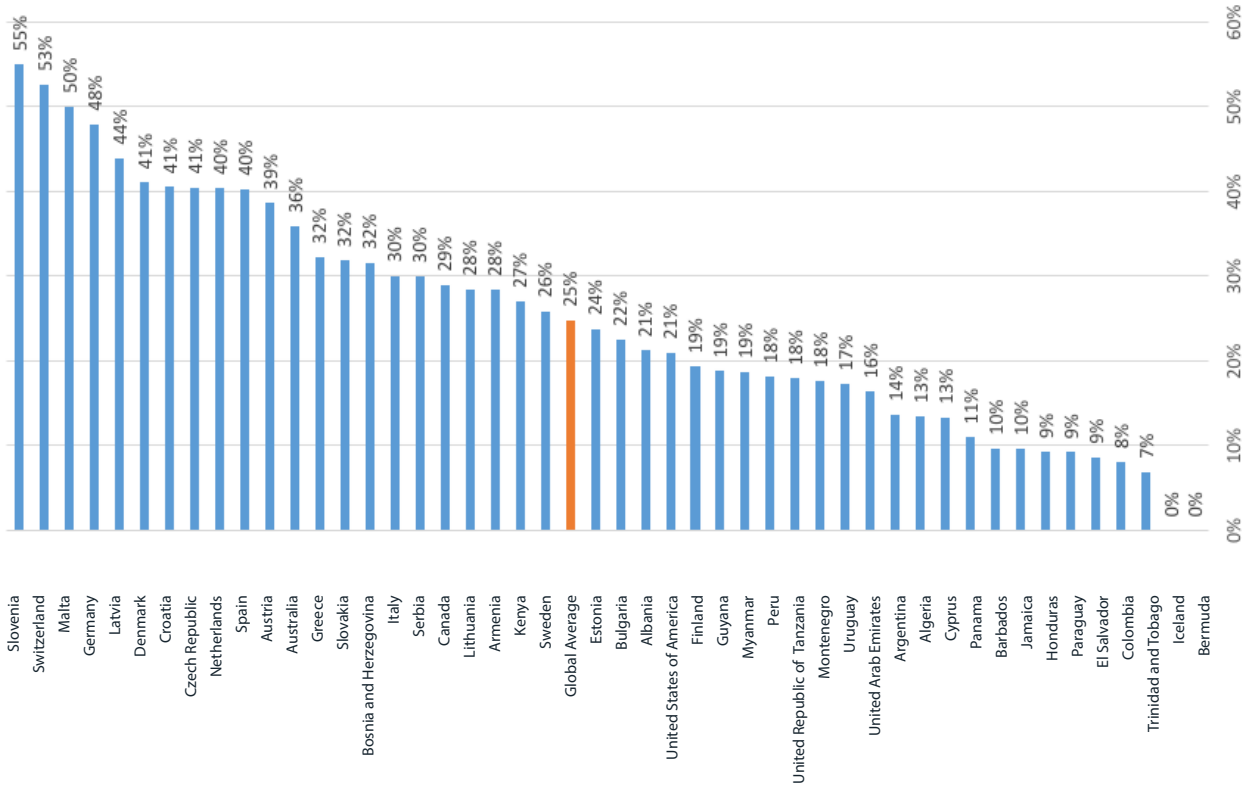
A high ratio of firearms is not systematically correlated to a higher homicide rate (Small arms survey, 2007). However, Levan (2013) suggests that there is no causal relationship between bearing firearms and crime, but rather that bearing firearms could constitutes a facilitator of violence. This is particularly the case with spousal violence, where the presence of a firearm in the home triples the risk of homicide (Levan, 2013).

Female victims of homicide

In 2015, women accounted for 25% of homicide victims worldwide. According to UNODC Statistics, this figure remained relatively stable between 2006 and 2014 (between 28% and 29%).

As has been pointed out on numerous occasions, male victims are over-represented in both ordinary crimes and homicides (ICPC, 2016). However, as Figure 1.3 shows, the countries with the highest HRs are also the ones where the percentage of female homicide victims is lowest.[3] In other words, men are the main victims in countries where violence is the most prevalent.

Figure 1.3. **Proportion of female intentional homicide victims relative to total victims of both sexes (ratio female/male) in 2015**



Source: UNODC

Violence against children and youth

According to a report published in 2017 by "Know violence in Childhood," a global initiative based in New Dehli, India, three out of four children in the world (1.7 billion) were the victims of some form of violence in 2015, including 100,000 homicides[4] (Shiva Kumar & Stern, 2017).

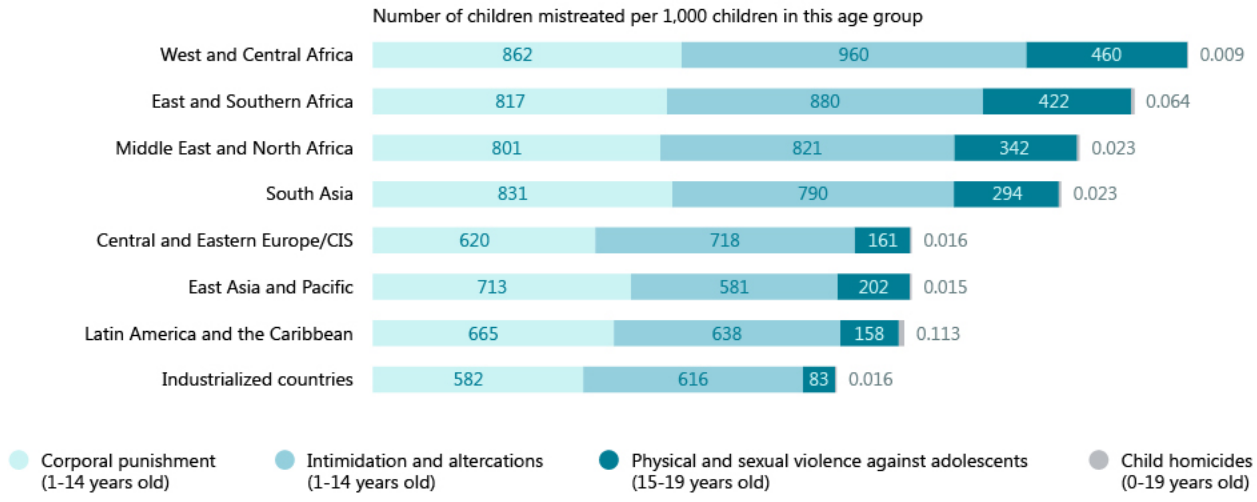
According to this report, violence against children is practically universal, affecting the North to the same degree as the South. This is true of corporal punishment and bullying, which six to nine out of every ten children in the world experience (see Figure 1.4). However, although this problem is universal, regional differences do exist. For example, the highest rates of physical and sexual violence are found in Africa, the Middle East and South Asia. On the other hand, the highest child HRs (0-19 years) are recorded in Latin America (HR: 11.3%ooo), as well as West and Central Africa (HR: 9.9%ooo).

Table 1.1. **Countries with the highest child homicides rates**

Country	
El Salvador	27
Guatemala	22
Venezuela	20
Lesotho	18
Brazil	17
Swaziland	16
Panama	15
Democratic Republic of the Congo	14
Nigeria	14
Colombia	13
Honduras	13
Jamaica	13
Rwanda	13

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

Graphique 1.4. **Prevalence of violence against children per region (2015)**



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

Cities and violence

The Citizen's Council for Public Safety and Criminal Justice (CCSPJP), based in Mexico, publishes an annual ranking of the cities with the highest HRs in the world (Table 1.2). In the CCSPJP's 2017 index, Latin America is highly over-represented with 42 cities out of 50 on the list. The average homicide rate for these 50 urban centres was 59.17‰ and the vast majority of these cities are in Brazil (17) and Mexico (12). As for the eight non-Latin American cities, four are in the United States, three in South Africa and one in Jamaica. It is important to highlight the fact that the US is the only so-called "developed" country on the list, which serves to illustrate the reality of violence in certain urban centres in the country, violence which is only getting worse. St. Louis for example saw its HR increase from 49.93‰ in 2015 to 65.83‰ in 2017. Likewise, Baltimore's HR rose from 33.9‰ in 2015 to 55.5‰ in 2017. Other cities in the United States experienced similar increases. Chicago for example experienced an 80% increase between 2015 and 2016. On the other hand, major cities such as New York and Los Angeles have experienced a steady and gradual decrease in their HRs (Fagan & Richman, 2017). According to these authors, this variation is explained by local factors, notably the public's lack of confidence in municipal governments and the police, increases in tensions between small street gangs and, especially, recurring epidemics of illegal drugs. The most recent case being that of the opioids epidemic (Box 1.3.).

Table 1.2. **Cities with the highest homicide rates in the world (per 100,000 population)**

Ranking	City	Country	Homicide rate per 100,000 population
1	Los Cabos	Mexico	111.33
2	Caracas	Venezuela	111.19
3	Acapulco	Mexico	106.6
4	Natal	Brazil	102.56
5	Tijuana	Mexico	100.77
6	La Paz	Mexico	84.79
7	Fortaleza	Brazil	83.48
8	Victoria	Mexico	83.32
9	Guayana	Venezuela	80.28
10	Belém	Brazil	71.38
11	Vitória da Conquista	Brazil	70.26
12	Culiacán	Mexico	70.1
13	St. Louis	United States	65.83
14	Maceió	Brazil	63.94
15	Cape Town	South Africa	62.25
16	Kingston	Jamaica	59.71
17	San Salvador	El Salvador	59.06
18	Aracaju	Brazil	58.88
19	Feira de Santana	Brazil	58.81
20	Juárez	Mexico	56.16
21	Baltimore	United States	55.48
22	Recife	Brazill	54.96
23	Maturín	Venezuela	54.43
24	Guatemala	Guatemala	53.49
25	Salvador	Brazil	51.58

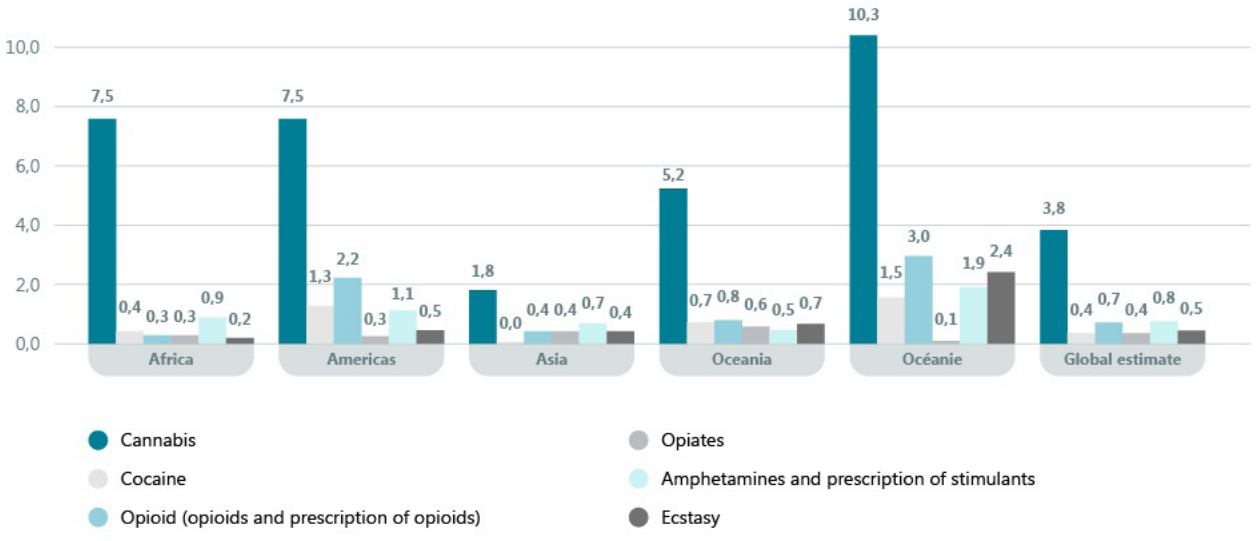
Source: CCSPJP (2018)

Drug market diversification and the legalization of cannabis

According to the World Drug Report (UNODC, 2017b), 5% of the global adult population apparently used drugs at least once in 2015, with cannabis being the most popular choice (Figure 1.5). Approximately 29.5 million suffer from disorders connected with this consumption. Opioids remain the most dangerous drugs, followed by amphetamines, which are the cause of numerous premature deaths from overdoses or infectious diseases transmitted via inappropriate injection practices (UNODC, 2017b). Opioids are also the drugs most associated with the commission of criminal offences (ICPC, 2015).

The drug market is continuing to diversify, notably due to the persistence of traditional drugs even as new psychoactive substances emerge (UNODC, 2017b). As DuPont has shown (2018), this diversification may also reflect the decentralization of synthetic drugs production.

Figure 1.5. **Prevalence of drug consumption per region in 2015 (%)**



Source: UNODC

Box 1.3. **The opioids crisis in the United States**

A problem in many countries, the harm caused by opioids is particularly evident in the United States of America. The misuse of pharmaceutical opioids, coupled with an increase in heroin and fentanyl use, has resulted in a combined and interrelated epidemic in the United States, as well as in an increase in morbidity and mortality related to opioids.

The United States accounts for approximately one quarter of the estimated number of drug-related deaths worldwide, including overdose deaths. Mostly driven by opioids, overdose deaths in the United States more than tripled during the period 1999-2015, from 16,849 to 52,404 annually, and increased by 11.4% in 2017 alone, to reach the highest level ever recorded. Indeed, far more people die from the misuse of opioids in the United States each year than from road traffic accidents or violence.

The emergence of derivatives of prescription medicines, classified as new psychoactive substances (NPS), particularly fentanyl analogues, has been associated with rising numbers of overdoses, including fatal overdoses, among opioid users. In recent years, several emergent synthetic opioids have been associated with increasing numbers of serious adverse events and deaths. The pills and powders containing synthetic opioids sold on the illicit market pose a threat to public health, a problem that is compounded by the variation in both the quantity and potency of their active components.

Sourc : UNODC (2017b, p. 10)

Moreover, cocaine production increased 30% between 2013 and 2015, while that of opium increased 33% from 2015 to 2016 (UNODC, 2017b). In the former case, this is largely due to rising production in Colombia. As for opium, higher production is a reflection of the improved yields in poppy fields in Afghanistan. Despite improvements in the identification of trafficking networks, the trend towards a diversification of trafficking routes has continued (UNODC, 2017b).

The major development, however, has been the legalization of cannabis in Uruguay, as well as in eight states in the United States, plus the District of Columbia (UNODC, 2017b). Likewise, Canada recently announced that the recreational use of cannabis would be legalized on October 17, 2018. South Africa, following a legal ruling in 2017, has de facto legalized cannabis consumption; this decision was confirmed by the Constitutional Court in September 2018. Several countries, particularly in Europe, the Americas and Oceania have recently legalized the medicinal use of cannabis. Although, globally, there is still no consensus on this matter, a transition from the war on drugs towards a public health approach based on decriminalization is evidently under way (ICPC, 2015). In fact, in certain cases (i.e., cannabis) this transition may lead to legalization

Incarceration rates as an indicator of trends in crime rates

Regarding incarceration rates, three different periods are evident. From 2004 to 2007, the incarceration rate fluctuated. Between 2007 and 2012, one observed a gradual rise in the incarceration rate coinciding with the onset of the 2008 recession. Beginning in 2012, the incarceration rate began a gradual decline.

There are major regional differences in incarceration rates. North America has the highest regional incarceration rate in the world (449.9 persons imprisoned per 100,000 inhabitants), due

to the large prison population in the United States. The highest incarceration rate observed in North America during the study period was in 2015. The United States has the world's highest national incarceration rate (675.6%ooo), far ahead of Trinidad and Tobago (547.54%ooo) and El Salvador (532.84%ooo).

Central America and the Caribbean have the second highest regional incarceration rate, despite a gradual decline observed since 2011. In contrast, South America, which has an incarceration rate about equal to the global average, experienced a nearly linear rise between 2005 (152.2%ooo) and 2015 when it reached the highest rate recorded during the study period (235.6%ooo). In Eastern Europe, the trend was in the opposite direction. In effect, since 2004 (263), the region has been recording a fall in the incarceration rate, which has accelerated since 2011. In a recent ECOSOC report (2017), this decline was attributed to the deterrent effect of the region's homicide conviction rate, which is higher than in other regions.

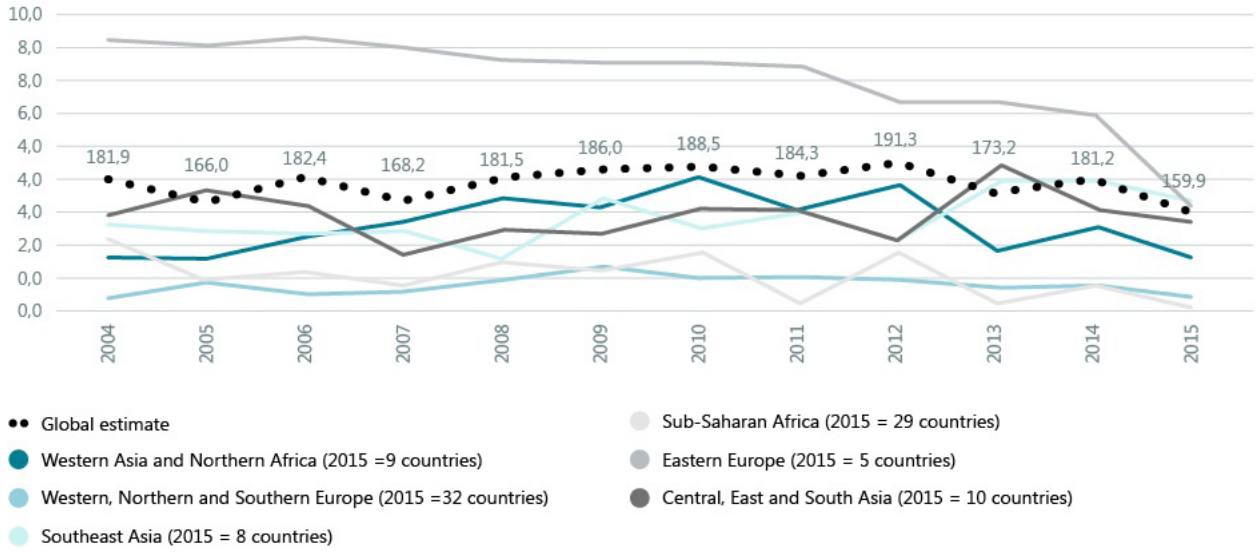
This same report, however, calls into question the criminal justice system's influence on crime: "More people in prison does not necessarily result in lower homicide rates, and declining imprisonment does not automatically produce a crime wave" (ECOSOC, 2017, p. 9). In effect, a number of studies have raised questions regarding the criminal justice system's dissuasive impact on crime (Cullen, Jonson, & Nagin, 2011; Harding, Morenoff, Nguyen, & Bushway, 2017; Loeffler, 2013; Roeder, Eisen, Bowling, Stiglitz, & Chettiar, 2015). Roeder et al (2015), for instance, explain that incarceration rates in the United States had a very a limited effect starting in the 1990s and practically none after the year 2000. Cullen et al (2011) explain that there exists very little evidence confirming the effectiveness of imprisonment in lowering recidivism rates and that, in fact, the evidence points the other way: imprisonment has a criminogenic effect.

Table 1.3. **Global incarceration rates (2004-2015)**

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Incarceration rate per 100,000 population	181.9	166.0	182.4	168.2	181.5	186.0	188.5	184.3	191.3	173.2	181.2	159.9
% of persons incarcerated who were sentenced	73.5	72.3	68.0	70.5	67.3	68.1	68.6	72.6	65.1	69.7	71.0	80.0
% of foreign persons incarcerated	0.04	0.04	0.04	0.05	0.04	0.05	0.04	0.04	0.04	0.04	0.04	0.07
% of youth incarcerated	0.30	0.69	0.76	0.73	0.69	0.76	0.95	1.09	1.00	0.99	0.98	0.92
% of adult women incarcerated	3.74	4.32	4.76	4.85	4.72	4.39	4.59	4.60	5.59	4.53	5.94	6.74

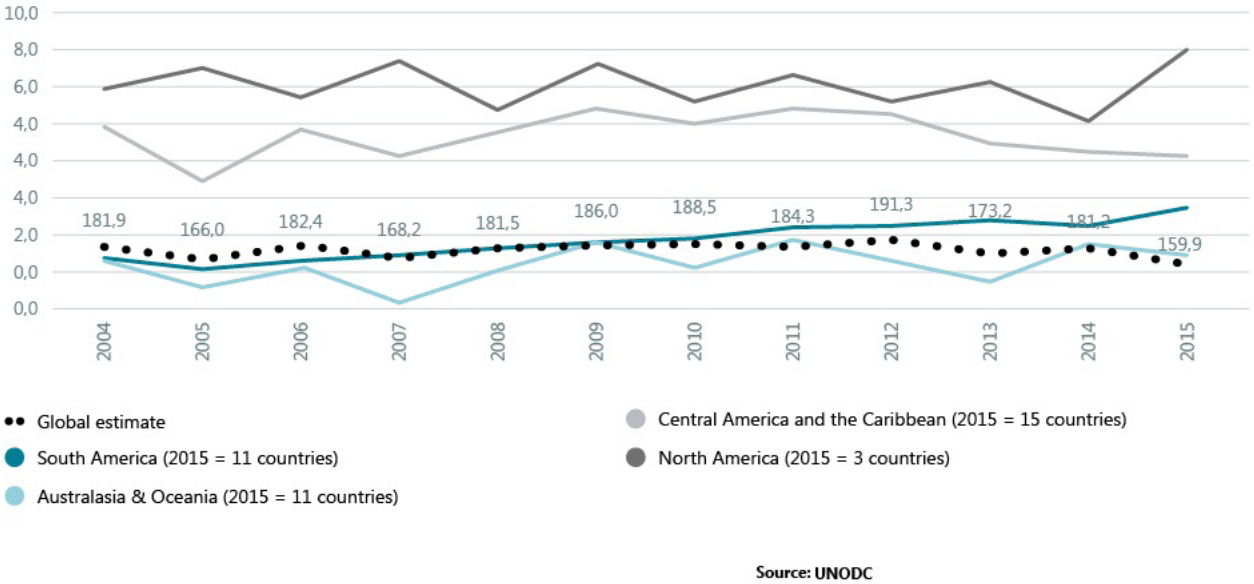
Source: UNODC

Figure 1.6. **Incarceration rates per 100,000 population per region (Part 1)**



Source: UNODC

Figure 1.7. **Incarceration rates per 100,000 population per region (Part 2)**



Source: UNODC

The feeling of insecurity

The 1960s saw the birth of research on the feeling of insecurity, due, notably, to growing concerns about citizens' attitudes and perceptions regarding public policy (Gouseti, 2017). Naturally, one of the principal issues was to analyze the link between actual crimes and the feeling of insecurity (Lewis & Salem, 2016). However, the research community has not succeeded in identifying a direct relationship between these two phenomena at the individual level (Zhao, Lawton, & Longmire, 2015). According to most researchers, the feeling of insecurity is a complex phenomenon, influenced by several variables, including crime (ICPC, 2016b; Jackson & Gouseti, 2014). For others, research on crime and research on the feeling of insecurity represent related but separate fields of study (Johnson, 2016). The feeling of insecurity consists of three components: the affective response; the behavioural component, which concerns the actions one takes to avoid victimization (e.g., installing an alarm system, avoiding public transportation, etc.); and the cognitive component, i.e., how one assesses the risks of victimization and the resulting consequences (Gouseti, 2017).

Box 1.4. **Individual factors influencing the feeling of insecurity**

- Personal experiences, e.g., past incidents of victimization (direct or indirect).
- Gender: men have a greater fear of large groups while women fear lone assailants and sexual assaults.
- Age: seniors tend to feel less safe although they are comparatively less frequently victimized. .
- One's ability to defend oneself.
- One's state of health.
- Educational level: people with more education are less inclined to feel insecure.
- Social vulnerability: one's employment status is a factor, as is membership in a minority.
- Social status: persons with educational, professional and financial resources see crime as a minor issue.

Source: ICPC (2016b)

At the present time, no international survey exists that would enable international comparisons on the feeling of insecurity, based on a uniform methodology. "Barometer" type surveys probably come closest to this model. However, the various barometers (e.g., the Eurobarometer) are each carried out in accordance with different needs. This does not facilitate interregional comparisons. For example, neither the Arab Barometer nor the Asian Barometer regularly ask specific questions on the feeling of insecurity. In the latter case, only the second wave of the barometer (i.e., 9 countries in 2005-2008) included a question in relation to this issue. In the event, 86.1% of the respondents felt safe or very safe (Asian Barometer, 2008).

The latest Eurobarometer concerning public perceptions of security provides insight on this issue in Europe (European Commission, 2017). Nine out of ten Europeans say they feel safe in their city or neighbourhood. On the other hand, the percentage of persons who perceive the European Union as a safe region fell by 11% between 2011 and 2017, due, notably, to the terrorist attacks executed since 2015. In effect, most survey respondents consider terrorism, organized crime and cybercrime to be the region's principal security issues.

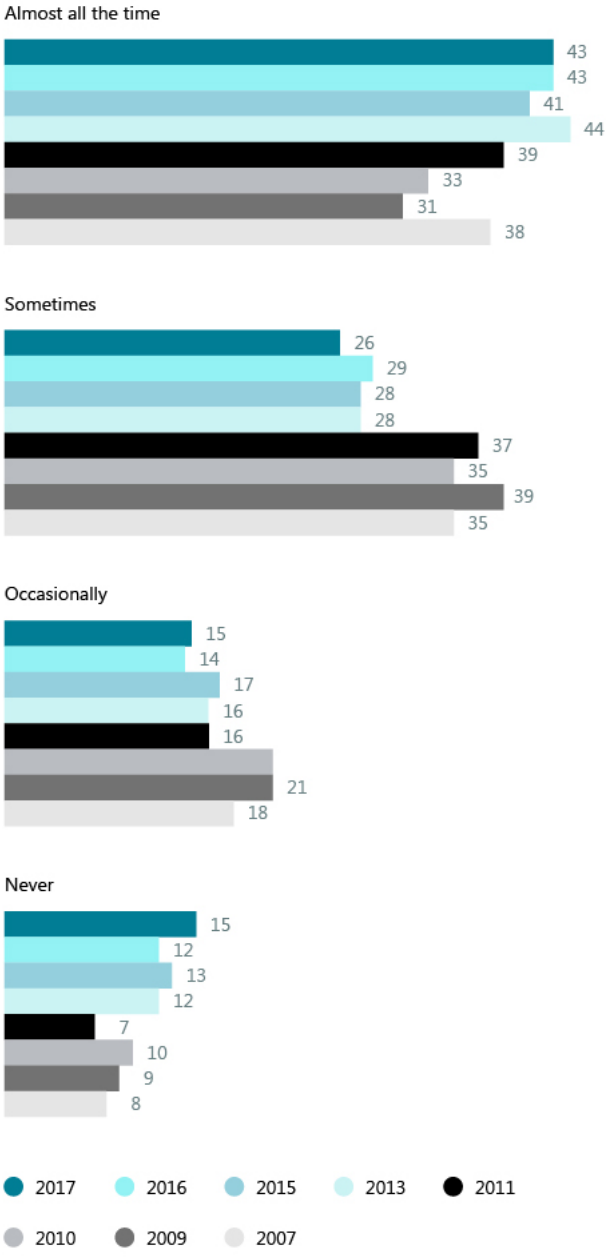
In Latin America, a completely different situation prevails (*Corporación Latinobarómetro*, 2017). In 2017, nearly half of survey respondents acknowledged fear of being victimized by crime, a percentage, moreover, that has risen in an almost linear fashion since 2009. The percentage of the region's respondents who never felt this fear during 2017 was 15%. Although this percentage seems logical, in light of the region's high homicide rates, it's important to bear in mind the country-to-country variations. In Chili and Uruguay, countries with very low crime rates, the percentage of persons who affirm that they never feared being victimized by crime were 16% and 20% respectively. And yet, the corresponding percentage was higher in Honduras (23%) and Guatemala (24%), two countries with very high homicide rates. These figures serve to demonstrate the profound disconnect that exists between the feeling of insecurity and crime.

In the case of Africa, the last AfroBarometer (2017) indicates that 68.9% of respondents have never feared being victimized by crime in their own homes. However, wide variations exist between different countries. This percentage was the lowest in Madagascar (40.3%), followed by South Africa (46.6%). And yet, the homicide rate in Madagascar is very low (0.62%ooo in 2010, according to UNODC Statistics) compared to South Africa, which has the fifth highest homicide rate in the world (Box 1.1).

Figure 1.8. **To what extent do you agree or disagree with each of the following statements on public safety? (Europe)**

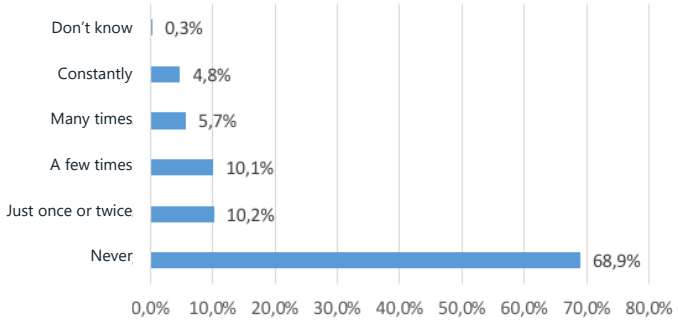
Source: European Commission (2017)

Figure 1.9. **How often do you worry about being the victim of a violent crime?**



Source: Corporación Latinobarómetro (2017)

Figure 1.10. **Fear of crime in one's own home (Africa, 36 countries)**

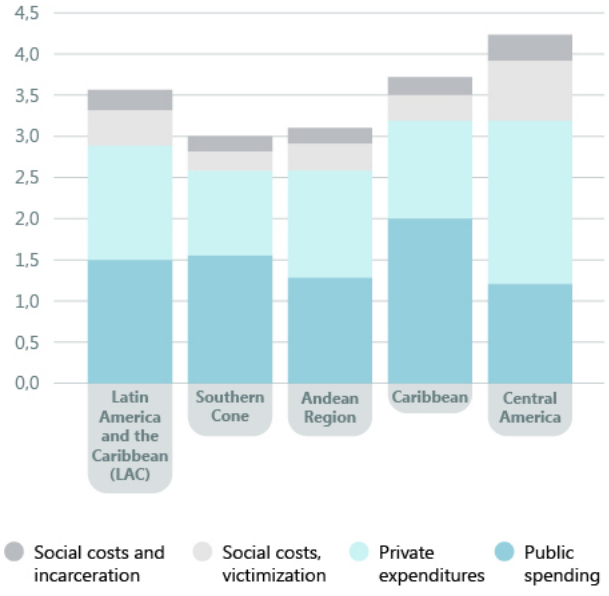


Source: AfroBarometer

BOX 1.5. **Estimated costs of crime and violence in Latin America**

A recent Inter-American Development Bank study updated the estimated costs of crime in the region (Banco interamericano de desarrollo, 2017). Estimates were based on three types of costs: social costs, private sector costs and costs to the State.

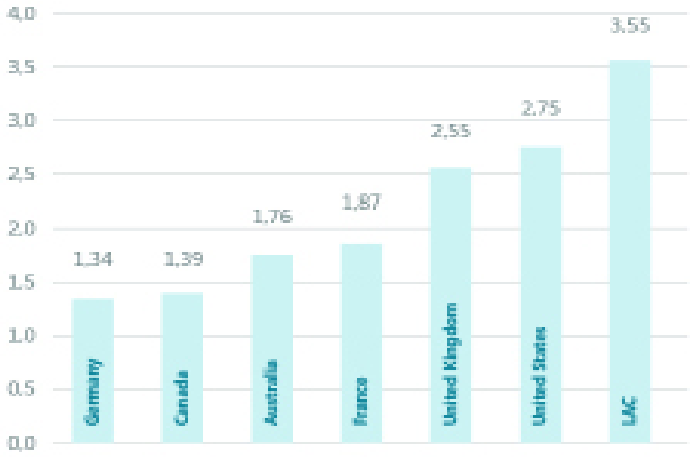
Figure 1.11. **Estimated costs of crime in Latin America (% of GDP)**



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

According to estimates, the region recorded an average annual loss of between 114,500 million and 170,400 million dollars US, as a result of crime, i.e., 3.5% of the regional GDP. The subregion with the highest percentage is Central America, followed by the Caribbean. The two countries with the highest costs in the region are also the ones with the highest rates of violence and crime in the world, namely Honduras (6.5% of GDP) and El Salvador (5.9% of GDP). Countries with a very low homicide rate, such as Chili or Uruguay, also record lower crime-associated costs. Conversely, Mexico, which has a high crime rate, is also the country where the cost of crime is the lowest in the region, in terms of the percentage of GDP.

Graphique 1.12. **International comparison of estimated costs of crime (% of GDP)**



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

The study also made a comparison between six Western countries and Latin America (see Figure 1.12). In every case and in every sub-component, the cost of crime in Latin America is higher than in these six Western countries. However, regarding the cost of imprisonment, costs in Australia and the UK are comparable to the region's while those in the United States are higher, which is not surprising given the latter country's high incarceration rates. Fourteen of Latin America's seventeen countries have higher costs than Western countries. Chili and Peru, for example, have costs similar to those in the United States, despite lower incarceration rates.

Part II - International and regional developments in crime prevention

Part II, we will describe the latest developments and initiatives in crime prevention undertaken by international and regional organizations.

Initiatives at the international level

a) The Doha Declaration

As mentioned in the 5th International Report, the 13th United Nations Congress on Crime Prevention and Criminal Justice was held in Doha, in 2015 (ICPC, 2016a). This event resulted in the adoption of the **Doha Declaration on Integrating Crime Prevention and Criminal Justice** (UNODC, 2015b). As its name indicates, this declaration addresses a fundamental issue in relation to security, namely the frequent lack of coordination between the criminal justice system and crime prevention strategies, which are seen as related but distinct areas of policy and action. Following this declaration, the UNODC launched a **Global Program** to support four key aspects of this integration: strengthening judicial integrity and preventing corruption in the justice sector (solid, reliable and transparent institutions); promoting the rehabilitation and social reintegration of prisoners to give them a new chance in life (fair, humane and effective criminal justice systems); preventing juvenile delinquency through sports programs and basic skills training (juvenile delinquency prevention); and supporting the integration of crime prevention and the rule of law at all levels of education (education for justice).

b) Violence prevention at the WHO

The WHO has launched a **Global Campaign for Violence Prevention** (GCVP) with the objective of implementing the recommendations published in its 2002 World report on violence and health. To that end, the GCVP aims to raise awareness about the problem of violence and emphasize the crucial role that public health can play in addressing its causes and consequences while at the same time encouraging prevention (2017).

Also in 2017, the WHO launched its **Global Plan of Action** to strengthen the role of the health system in addressing interpersonal violence, in particular against women and girls, and against children (WHO, 2017). This plan of action follows up on resolution WHA67.15 of the 67th World Health Assembly. It is specifically addressed at women, girls and children due to the particular characteristics of the violence to which they are subject, based notably on gender inequalities and discrimination (WHO, 2017). It proposes a series of practical actions which member States can undertake to strengthen their health systems in order to fight against this type of violence.

Box 1.6. **Objectives of the Global plan of action to strengthen the role of the health system within a national multisectoral response to address interpersonal violence**

The objectives are:

1. To address the health and other negative conse-

quences of interpersonal violence, in particular against women and girls, and against children, by providing quality comprehensive health services and programming, and by facilitating access to multisectoral services.
2. To prevent interpersonal violence, in particular against women and girls, and against children.

Strategic directions:

In order to achieve the objectives, four strategic directions are proposed that address both the health system mandate of the plan and the public health approach to addressing interpersonal violence.

1. Strengthen health system leadership and governance.
2. Strengthen health service delivery and health workers'/providers' capacity to respond.
3. Strengthen programming to prevent interpersonal violence, notably via the actions the health system can directly implement, including identifying people at risk and carrying out health promotion activities, as well as those violence prevention actions to which it can contribute through multisectoral actions.
4. Improve information and evidence.

Source: WHO (2017)

c) Agenda 2030 for Children: the End Violence Solutions Summit

On February 14-15, 2018, a high level conference was held in Stockholm, Sweden, on violence against children: **Agenda 2030 for Children** - the End Violence Solutions Summit (Global Initiative to End All Corporal Punishment of Children, 2018). This agenda is in keeping with the 17 Sustainable Development Goals, which the world's leaders have undertaken to achieve by 2030, in particular Goal No. 16.2: "end abuse, exploitation, trafficking and all forms of violence against and torture of children," in the entire world. In July 2016, an initial global partnership was launched to this end at the initiative of governments, UNICEF, the WHO and various other stakeholders. This group includes 15 pioneering countries. In addition, Japan, Brazil and the United Arab Emirates announced their intention to join during the Stockholm Summit. To date, Sweden is the only country taking part in this initiative that is considered an economically developed country.

d) High level meetings

26th Session of the Commission on Crime Prevention and Criminal Justice (May 2017)

The 26th Session of the Commission was an opportunity to further examine and discuss eleven draft resolutions bearing on a variety of issues including, notably, the fight against human trafficking and migrant smuggling, the links between terrorism and transnational organized crime, prison systems and imprisonment, and mainstreaming gender perspectives in the fight against transnational organized crime, as well as in cybercrime prevention (UNODC, undated).

7th Conference of the States Parties to the United Nations Convention against Corruption (November 2017)

On 6-10 November 2017, the 7th Conference of the States Parties to the United Nations Convention against Corruption was held in Vienna with over 1,700 delegates in attendance, from approximately 180 countries. Eight resolutions were adopted at the Conference, including resolutions on strengthening international cooperation and prevention systems, based on comprehensive multidisciplinary approaches (Conference of the States Parties to the Convention of the United Nations against Corruption, 2017).

61st Session of the Commission on Narcotic Drugs (March 2018)

The Commission on Narcotic Drugs is the governing body of the United Nations Office on Drugs and Crime (UNODC). Its mandate is to guide and assist States in the implementation of its recommendations, notably by monitoring the measures taken and by disseminating recommended practices (Commission on Narcotic Drugs, undated). The main objective pursued at this Session was to build consensus among States, international organizations and civil society organizations concerning resolutions under consideration on: combating the synthetic opioids crisis; protecting children; strengthening drug prevention in schools; measures to prevent mother-to-child HIV transmission; and preparations for the planned ministerial meeting at the Commission session in 2019. In the event, the Session resulted in the adoption of 11 resolutions, as well as amendments in the lists of scheduled substances.

High level meeting to assess the United Nations Global Plan of Action to Combat the Trafficking of Persons (September 2017)

On 27-28 September, a high level plenary meeting of the UN General Assembly was held in New York to not only assess the progress made in the implementation of the Global Plan of Action to Combat Trafficking in Persons (2010), but also the deficiencies and difficulties, which may have emerged (UN, undated). In addition, this meeting saw the adoption of a "Policy Statement on the Implementation of the United Nations Global Plan of Action to Combat Trafficking in Persons," which included, notably, a commitment to end modern-day slavery.

Concerning prevention, the Member States underscored the importance of continuing the efforts to effectively combat human trafficking, notably by addressing its underlying causes and factors, such as poverty, unemployment, migration, etc.

Regional, national and local initiatives

a) Africa

LIn 2016, the African Peace and Security Architecture (APSA), which is responsible for conflict prevention, conflict management and peace-building in the African Union (AU), released its **APSA roadmap 2016 – 2020** (APSA, 2016). This document provides a shared understanding of the results to be achieved by all APSA stakeholders, notably by highlighting the need to increase collaboration and coordination. It focuses on five strategic priority areas: 1) conflict prevention; 2) crisis and conflict management; 3) post-conflict reconstruction and peace-building; 4) strategic security issues; and 5) coordination and partnerships. Priority No. 4 includes crime-related issues, such as illegal flows of small arms and light weapons, counter-terrorism, illicit financial flows, transnational organized crime and cybercrime.

The African Union Commission (AUC) has implemented an action plan with the objective of **Silencing the Guns by 2020**. This initiative is seen by the international community as a major step forward for Africa, particularly regarding countries still afflicted by conflict (ISS, 2018). According to the Institute for Security Studies (ISS), this action plan is confronted with three challenges: funding, disarmament of fragile communities, and maintaining justice and the rule of law throughout the process. In the same vein, the African Union's Peace and Security Department (PSD) launched its **Gender, Peace and Security Programme (2015-2020)** with the aim of developing effective strategies for mainstreaming gender in peace and security, notably in relation to issues such as women's effective participation in peace and security, protection in times of conflict and public recognition in the post-conflict phase (African Union - Peace and Security Department, 2016). This program will develop partnerships to ensure effective joint coordination and policy development in this area by the AUC, the UN and the regional economic communities. Moreover, this plan will capitalize on knowledge development and research to guide and inform the development of long-term strategies and mechanisms to address these priorities.

In 2016, the UNODC launched its R**egional Programme 2016-2021** for East Africa: Promoting the Rule of Law and Human Security in East Africa (UNODC, 2016). This plan aims to continue strengthening the rule of law and enhancing human security in the region through five pillars or sub-programs: countering transnational organized crime and trafficking, countering corruption, terrorism prevention, crime prevention and criminal justice, and prevention of drug use, and treatment and care of drug use disorders. Expected outcomes, to be achieved by the end of 2021, have been identified for each sub-program. In the case of the crime prevention and criminal justice sub-program, three expected outcomes (which emphasize criminal justice more than prevention) have been identified: member States conduct effective, efficient and sustainable reforms of justice and law enforcement institutions, thereby increasing access to justice, member States have an improved quality, efficiency and fairness of the criminal justice process, including catering to the needs of vulnerable groups, and member States put in place comprehensive crime prevention, rehabilitation and reintegration programmes.

b) North America

In 2014, the **Violence Reduction Network** (VRN) was launched in the United States (Lopez, 2017). The aim of this initiative is to facilitate inter-agency cooperation between local law enforcement agencies and their federal partners in order to identify problems and implement strategies to produce significant results for the entire community. In effect, local agencies are provided with resources through training and technical assistance programs, as well as tools designed to improve information sharing. According to a recent assessment, the VRN is currently achieving its objectives and is successfully responding to the needs of police departments while at the same time significantly improving communication between local and federal law enforcement agencies. In light of the VRN's positive results, the federal government launched the **National Public Safety Partnership** (PSP) in June 2017, under the auspices of the Department of Justice. The PSP broadened the VRN's scope by enhancing support in the investigation, prosecution, and deterrence of violent crime, especially crime related to gun violence, gangs, and drug trafficking. The PSP facilitates communication between the federal government and cities in order to strengthen local violence reduction strategies, in accordance with evidence-based approaches that are, moreover, tailored to local needs.

In 2017, in response to growing concerns in Canada regarding street gangs, the federal government announced new funding for **gun and gang violence** prevention programs (Public Safety Canada, 2017b). This initiative seeks to unite

> "federal, provincial and territorial efforts to support [...] prevention [...] efforts, build and leverage unique federal expertise and resources to advance intelligence related to the illegal trafficking of firearms, and invest in border security to interdict illicit goods including guns and drugs" (Public Safety Canada, 2017b, para. 2)

The **National Action Plan to Combat Human Trafficking** recently concluded in 2016, but not before a number of successes were achieved in 2015 and 2016 (Public Safety Canada, 2017a), particularly in relation to prevention. In effect, several public awareness and training campaigns were carried out including, notably, a national awareness campaign on the domestic sex trafficking of Indigenous people, which targeted rural, urban and Northern communities. Another important prevention effort was the public awareness campaign on human trafficking, aimed at youth and those in their social environments (parents, teachers and service providers), which sought to alert them to the methods used by traffickers, as well as raise their awareness of the effects of victimization.

Box 1.7. **Public Safety Canada's Crime Prevention Inventory**

Canada's Ministry of Public Safety recently established a Crime Prevention Inventory (CPI), which, for the first time, enables nationwide centralized access to evidence-based crime prevention programs from across the country. The CPI includes 190 programs, from every province and territory. All have been implemented and all have been assessed. As such, the CPI is a resource that will provide researchers, decision-makers and crime prevention practitioners with access to reliable information. Moreover, Public Safety Canada's new Crime Prevention Inventory allows users to search for programs using filters such as the program's topic, characteristics of target populations, location, program outcomes, etc.

Source: Public Safety Canada (2018)

c) Latin America and the Caribbean

The OAS has established the **Inter-American Network for the Prevention of Violence and Crime**, as a follow-up to Resolution 2866, which the OAS General Assembly adopted in 2014 (OEA, undated). This mechanism was created to facilitate dialogue and the sharing of knowledge and best practices, among decision-makers, researchers, experts, government officials, the private sector and the general public, on violence and crime prevention issues throughout the Americas.

In 2015, the OAS General Assembly adopted the **Inter-American Convention on Protecting the Human Rights of Older Persons**. Article 9 of this convention directly addresses violence against older persons and its prevention. It encourages member governments to adopt legislative and administrative measures to: prevent violence against older persons; sensitize and train government officials and society as a whole regarding this issue; promote and strengthen support services for victims; and facilitate the reporting of such offences (Asamblea General, OEA, 2015). In 2016, the OAS General Assembly adopted a resolution entitled **Advancing Hemispheric Security: A Multidimensional Approach** to provide a framework for the Assembly's activities in the area of security, notably in relation to crime and violence prevention, countering human trafficking and small arms and light weapons smuggling, organized crime and police cooperation (Asamblea General, OEA, 2016). In adopting the Inter-American Program for the Promotion and Protection of the Human Rights of Migrants, Including Migrant Workers and their Families, the OAS General Assembly underscored the importance of strengthening the prevention of violence and crime against migrant populations. In 2017, the OAS General Assembly adopted a new resolution on **Advancing Hemispheric Security: A Multidimensional Approach**, which, in the same vein as the resolution of 2016 provides a framework for the Assembly's work on security related issues (Asamblea General, OEA, 2017). In this iteration, it placed particular emphasis on crimes that affect the environment, as well as on the security implications of climate change.

d) Southeast Asia

One of the region's key issues is the need to improve intra-regional cooperation, particularly regarding organized crime. In 2017, the **Association of Southeast Asian Nations (ASEAN)** held a high level regional conference to discuss and build consensus on recommendations for the effective implementation of the "Treaty on Mutual Legal Assistance in Criminal Matters" (UNODC, 2017a). A number of key difficulties were identified at the conference, including member countries' lack of familiarity with the legal systems of other countries in the region, the absence of a common language and poor communication both within countries as well as between them.

The sexual exploitation of minors is probably one of the main issues in Southeast Asia, along with the related issue of sexual tourism (UNODC, 2014). In 2014, the UNODC's regional office released a series of reports with the object of enhancing the relevant policy and legislative responses of the countries concerned, in particular Cambodia, Laos, Myanmar and Vietnam. More specifically, the UNODC made a number of recommendations, chief among them the need to improve law enforcement agencies and policing responses, strengthening the legal framework and developing intra-regional cooperation.

An issue of particular note in Southeast Asia is the growing concern around **wildlife and timber trafficking**. In response, the member nations of ASEAN met recently in Bangkok to launch the **ASEAN Wildlife Enforcement Network** to enhance intra-regional coordination in this area (UNODC, 2018).

There is also great concern in the Southeast Asia regarding drug-related issues. This concern arises from the localization in the region of much of the world's production of synthetic drugs and opium. A number of countries have begun to take measures to combat this problem. For example, Myanmar has recently announced a **New National Drug Control Strategy** (The Republic of the Union of Myanmar, 2018). This strategy was developed in response to the Special Session of the United Nations General Assembly on the World Drug Problem (UNGASS), held in 2016. Thus, in the spirit of UNGASS, it seeks to bring about a significant change in public policy in favour of an evidence-based public health approach, while at the same time advocating concrete strategies to address the negative effects of drug production, trafficking and use.

e) Europe

The European Commission has developed a new **European Agenda on Security** for 2015-2020 (European Commission, 2015), based on five principles: a) ensuring full compliance with fundamental rights; b) more transparency, accountability and democratic control, to give citizens confidence; c) ensuring bet-

ter application and implementation of existing EU legal instruments; d) adopting a more unified inter-agency and cross-sectoral approach; and e) harmonizing the internal and external dimensions of security. On the basis of these five principles, there exists, moreover, a willingness to strengthen partnerships and coordinate efforts in relation to security issues. In effect, in operational terms, this new agenda underscores the importance of better information sharing within the European Union and better coordination of operations in the field. In addition, it also accords more importance to training, program funding, and research and innovation in the area of security. Within this framework, the new agenda has prioritized three policy areas during its five-year term: **terrorism, organized crime and cybercrime**. Much of the European Commission's efforts addressing terrorism and radicalization prevention is more concerned with criminal justice and prosecution than prevention. For example, in 2016, it promoted the creation of the European Counter Terrorism Centre (ECTC) within Europol, which is charged with working in collaboration with Eurojust, another EU agency. It also created the Internet Referral Unit (IRU), within the same law enforcement agency, for the purposes of combating extremist propaganda – a role also played by the European Forum for Urban Safety (EFUS). In terms of prevention, the new agenda promotes education, youth engagement, and interconfessional and intercultural dialogue, as well as employment and social inclusion. Regarding organized crime, one of the objectives is "to disrupt organised criminal networks involved in smuggling of migrants by stepping up cross-border investigations with the support of EU agencies" (European Commission, 2015, p. 19). Three types of organized crime will receive priority attention: light arms and small weapons smuggling, human trafficking and the sexual exploitation of minors. Moreover, one of the key issues to be addressed is the funding of such networks, which, as it happens, is often associated with corruption, fraud and smuggling. Thus, an objective of the Agenda's anti-money laundering efforts is to facilitate the detection and monitoring of money transfers. Finally, regarding cybercrime, the new agenda stresses the importance of 1) fully implementing existing European legislation and 2) efforts to cooperate with the private sector.

The European Anti-Fraud Office (OLAF) recently released its 2016-2020 strategic plan (European Commission, 2016). OLAF's mandate is to 1) conduct independent investigations on fraud and corruption, 2) strengthen citizens' confidence in the EU's institutions and 3) develop its policies in the fight against fraud. There is greater focus on prevention under the third point. More specifically, OLAF's objectives are to develop policy and anti-fraud legislation, reduce the illicit trade in tobacco products and support Member States in the fight against fraud, corruption and other illegal activities.

Part III - Recent trends in empirical studies on crime prevention

Based on a review of the literature, effected between 2015 and 2017, we were able to identify empirical studies specifically concerned with the subject of crime prevention[5]. This systematic review enabled us to present a current overview of the subject, from a scientific perspective. We categorized these empirical studies based on key word searches and the geographical region. The topics addressed in these studies are summarized in Table 1.4 below:

Table 1.4. **Topics addressed in the recent scientific literature (2015-2017)[6]**

Community policing	17
Policing	15
Youth	14
Violence	10
Situational prevention	9
Others	7
Schools	6
Public policy	5
The feeling of insecurity	4
Criminal justice	4
Mental health	4
Territoriality/urban issues	4
Gender	3
Neighbourhood watch	3
Minority communities	2
Coordination issues	2
Tertiary prevention	2
Families	2
Organized crime	2
Drugs	1
Arms	1
Domestic violence	1
Social problems	1
Intervention	1
Security	1

Our review enabled us to collect a wealth of data. However, this chapter's space restrictions forced us to confine our analysis to what appear to be the four most important topics in current empirical research: community and urban policing approaches, the role of the police in prevention, crime analysis as a prevention tool for the police and the relationship between youth and crime. In certain cases, pertinent scientific papers from 2018 were also discussed.

Box 1.8. **The deficiencies of the "top down" approach in crime prevention: the case of the Palestinian territories**

Based on an experience in the Palestinian territories, Homel and Masson (2016) explain the deficiencies present in the "top down" approaches, characteristic of international donors, as compared to the benefits of "bottom up" approaches. Top down approaches are elaborated from the vantage point of donors and decision-makers, without taking into consideration the opinions of local actors. In contrast, "bottom up" models are premised on the idea that local strategies must be designed on the ground in partnership with local actors. According to Homel and Masson, in "top down" approaches deficiencies arise, notably, from the absence of local ownership, difficulties in managing governance issues, the effects of the coopting of political and security agency elites, and neglecting the citizenry's opinions and needs. In contrast, the bottom up approach used in the Palestinian territories proved effective in resolving local security problems in an urban context characterized by social conflict. This process began with public consultations, which led to the forming of a local security committee whose members participated in the elaboration of a partnership agreement and local action plan.

The community-based prevention approaches: from community policing to neighbourhood watch groups

Much of the current research on the relationship between crime prevention and the community is associated with the community policing approach (Gill, Weisburd, Bennett, Telep, & Vitter, 2011). This approach often connotes a police department that is physically closer to the community and more sensitive to its needs, due to its deep knowledge of the local context. This approach aims to increase the population's trust in the police and enhance the latter's legitimacy. Moreover, this model encourages civic engagement in law enforcement (Smith & Scott, 2013). Such engagement may include consultations and citizens participating in local committees or direct participation. Occasionally, citizens may even replace the police in certain of the latter's normal activities rather than simply collaborate with law enforcement. A notable example: monitoring activities carried out by citizens under the "neighbourhood watch" model. In fact, most of the documents indexed for this survey emphasized this dimension of local community engagement. It's interesting to note the large number of papers which analyze this issue in other regions outside of North America.

In Malaysia, for example, a community policing approach exists, dating back to 2007, which is premised on establishing local partnerships with the police and community actors (Hassan & Abdullah, 2017). Ishak (2016) analyzed public perceptions of the effectiveness of this approach and found that 72.1% of the persons surveyed consider the police effective in their crime control actions. He also compared this community policing approach with neighbourhood watch models, which were perceived to be much less effective. Hassan and Abdullah (2017) sought to identify the sociodemographic factors influencing Malaysians' participation in community policing support committees, as well as the consequences of such participation. The members of such committees tend to be men, married, from the private sector and local property owners. Individuals who participate in these committees have greater self-confidence, are more aware of what's happening in the neighbourhood, feel more useful to the community and feel more appreciated as members of it. Another study in Malaysia made a qualitative assessment of alarm systems as a means of crime prevention (Lyndon, Selvadurai, Sum, & Abidin, 2017). According to this study's findings, the utilization of alarm systems was correlated to a reduction in crime, mainly because it enabled the creation of a network for ensuring public safety at the local level, which, in turn, fostered good relations between neighbours.

In Pakistan, one particular study sought to determine how certain characteristics in two neighbourhoods influence violence levels, in a context where the actions of the police are considered ineffective (Aqil, 2016). Among the factors identified as important were the weakening of the social fabric, the role of social organizations and the absence of public meeting places.

In Nigeria, Ijimakinwa et al (2016) compared the capabilities of "neighbourhood watch groups" in terms of detecting crime-related issues vs. the capabilities of the police. This type of group emerged as an alternative in a context where the police were perceived as ineffective, corrupt and brutal (Ijimakinwa et al., 2016; Ojebuyi, Onyechi, Oladapo, Oyedele, & Fadipe, 2016). Ijimakinwa et al (2016) conclude that community engagement in this type of monitoring activity can increase public satisfaction regarding the police, as well as foster information sharing on crime and security issues. Ojebuyi et al (2016) did a more in-depth analysis of the effectiveness of these groups' activities. In Nigeria, there exists a wide variety of monitoring type groups, including neighbourhood watch groups, religious and ethnic militias, private security agencies, etc. To a significant extent the public's feeling of security is associated with the activities of these groups. According to Ojebuyi et al, this is due to a strategy of communitization of security, in which this type of organization in ubiquitous in public spaces and has endeavoured to

communitize private problems and the role of the State, notably, by providing the police with funding (for fuel, vehicles, construction of police stations, etc.). In any case, it has facilitated the reporting of crimes and police intelligence work.

In Colombia, Bonilla (2016) analyzed perceptions regarding civic participation in building security and the effectiveness of community policing, in a context of policing reforms in Latin America. Said reforms, moreover, are associated with the region's democratization process, which includes a more active role for citizens (ICPC, 2016a). Bonilla's findings indicate that community policing enjoys a more positive assessment (77%) than the police in general (33%) and is considered more effective in resolving crime-related issues at the local level. This positive assessment is explained, notably, by perceptions of the community police's proximity and rapid response. On the other hand, only 26% consider the local security committees effective in terms of prevention. Ribeiro et al (2016) conducted a study in Brazil on the perception police officers have of community policing. In this case, "community policing" refers to police action in partnership with the community. This study demonstrates that the police in Brazil employ the term community policing to cover a broad range of practices, not all of which are consistent with the basic concept underlying this approach. On the contrary, the Brazilian police employ innovative concepts such as neighbourhood watch groups, etc., in conjunction with traditional policing practices based on control and repression.

This set of papers highlights the trend towards an approach based on the communitization of security. In Western countries and Latin America, this trend is associated with efforts to ensure coordination and partnership with the police. However, in developing countries in other regions, it tends to connote policing by groups issued from the community itself, groups which actually assume certain responsibilities of the police. In the latter case, prevention is not addressed as such, as this type of group focuses instead on monitoring and control rather than on the underlying causes of crime. However, in so doing, it reproduces the traditional policing model.

BOX 1.9. **Testing the "broken windows" theory**

In their famous paper, Wilson and Kelling (1982) explain the basic principles of the "broken windows" theory. According to them, social disorder (loitering, alcohol consumption, etc.) and physical disorder (empty lots, abandoned buildings, etc.) make people fearful, which leads them to move out of their neighbourhood. That in turn weakens structures of informal control and further increases disorder, which draws more potential criminals into the area and increases crime. However, this relationship between disorder and crime, which is the cornerstone of the zero tolerance model in New York, is the subject of considerable debate in the literature (A. A. Braga & Welsh, 2016).

A recent meta-analysis sought to assess the effectiveness of policing strategies which focus on disorder to reduce crime (Anthony A. Braga, Welsh, & Schnell, 2015). This meta-analysis suggests that such strategies are correlated with a statistically significant, albeit modest, overall effect on crime reduction. However, this overall effect needs to be considered in detail. Community interventions and problem resolution programs designed to modify conditions of social and physical disorder in certain places have proven highly effective in reducing crime. On the other hand, aggressive policing strategies which target individual disorders, such as preventive control for example, do not generate a significant reduction in crime.

In another study, David Weisburd et al (2016) analyze the effectiveness of the S QF policing strategy, which consists of stopping, questioning and frisking persons suspected of criminal offences. SQF is part of the toolbox used in the "zero tolerance" model. This approach has been strongly criticized for racial profiling. In effect, police officers have tended to stop youth and minorities, particularly from so-called "sensitive" neighbourhoods (D. Weisburd, Wooditch, et al., 2016). The results of this study indicate that the SQF strategy has a slight deterrent effect on crime, particularly when employed in areas associated with "hotspots." However, according to Weisburd et al, although this strategy may be effective to a certain extent, this does not necessarily imply that it is also efficient. In effect, after a total of 700,000 SQFs, crime decreased by barely 2%. Moreover, this decrease was correlated with misdemeanours – "low intensity" crime, as it were. Furthermore, as they point out, empirical criteria cannot be the only criteria to consider in a democratic society, when what is at stake is the legitimacy of policing activities and, indeed, that of the police department itself.

The approach has been criticized for targeting the young, minorities, and specific neighborhoods of NYC These findings suggest that police departments should adopt a model based on community coproduction rather than privilege a zero tolerance policing model, which focuses on a sub-set of social disorders and entails measures such as arresting and preventively controlling drunks, adolescents, homeless persons, etc.

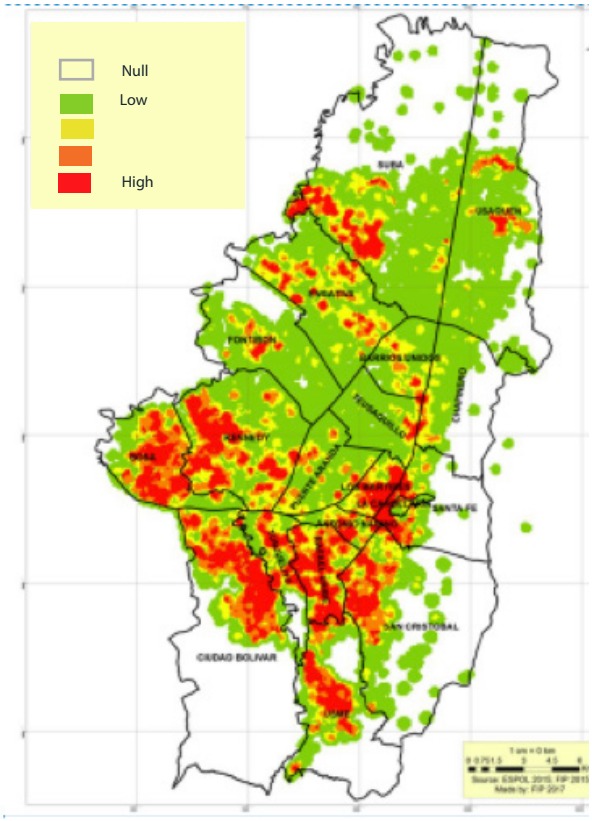
Crime analysis as a prevention tool for the police

Crime analysis based on geographic information systems constitutes one of the more recent revolutions in terms of prevention tools, particularly in policing. Not only does this type of analysis enable precise analyses of the spatial distribution of crime, but it also facilitates successful crime prediction (Anthony A. Braga et al., 2017). The contribution made by Chilei's Carabineros,

discussed later in this chapter, offers a South American perspective on this type of analysis. Research indicates that crime is concentrated in hotspots rather than evenly distributed in a given city or country (Anthony A. Braga et al., 2017; D. Weisburd, Braga, Groff, & Wooditch, 2017). A recent study, for example, demonstrates that, over the last sixteen years, there has been a certain stability in terms of the spatial concentration of eight types of crime in certain segments of streets and intersections in the city of Vancouver (Andresen, Curman, & Linning, 2017). This law of crime concentration has modified policing by encouraging the adoption of a model which emphasizes preventative and intelligent patrolling, as opposed to the traditional model of maintaining a constant police presence and occupation. This change has effectively led to reduced crime in areas identified as hotspots (A.A. Braga, Papachristos, & Hureau, 2012; Sherman & Weisburd, 1995; D. Weisburd, Braga, et al., 2017). Although this hotspots-based approach to policing has been effective in reducing crime (including in areas adjacent to hotspots), there are, however, very few studies assessing the effect of this policing model on large urban areas. David Weisburd et al (2017) have demonstrated that the implementation of hotspots policing has a beneficial effect on large urban areas as well, as attests, for example, the 10% reduction in theft. In another study, Sarit Weisburd (2016) turned the question on its head by asking whether the frequent dispatching of police officers outside of their normal districts, in response to 911 calls, impacts crime rates in said normal districts. She estimates that a 10% decrease in the presence of the police may increase crime by 4.6%. A study in the Netherlands focused on the importance of the time of day in relation to crime (Montoya, Junger, & Ongena, 2016). In effect, burglaries during the day occur for different reasons than nighttime burglaries. During the day, control of access and territoriality[7] are the explanatory factors; at night, however, target selection is just as important as control of access.

In South America, this type of analysis is rapidly gaining in importance. A study in the city of Bogotá, Colombia, for example, shows the applicability of kernel density estimation modeling for defining crime hotspots (Barreras, Dıaz, Riascos, & Ribero, 2016). Another study in the city of Montevideo, Uruguay, demonstrates the effectiveness of videosurveillance cameras under police control for crime prevention in the sectors where they are installed, a result which runs counter to those of meta-analyses on this subject (Welsh & Farrington, 2007). However, this same analysis also demonstrates that effective videosurveillance resulted in a displacement of crime rather than its reduction.

Illustration 1.1. **Risk of presence of illicit drug dealing activity in Bogotá**



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

Box 1.10. "**Hotspot policing" as a prevention tool of the police in Montevideo, Uruguay**

One of the most recent examples of a police department's successful application of crime analysis for crime prevention purposes is the **High Operational Engagement Program** (Programa de Alta Dedicación Operativa—PADO) of the police in Montevideo, Uruguay (BID & Ministerio del Interior de la República Oriental del Uruguay, 2018). This program reformed the police patrolling system, which, in turn, implied major organizational changes entailing professionalization of policing practices, advanced training and the utilization of new technologies. The program's use of the PredPol software to facilitate crime prediction led the police to reorganize its patrolling, formerly based on randomly dispatching units to different sectors, in favour of intelligent patrolling concentrated in crime hotspots. According to an assessment of the program, its implementation resulted in a 22% reduction in violent robberies.

Many of these studies focus on crime density in a specific area. However, crime is the result of multiple spatial factors. Risk terrain modeling (RTM) is a methodology for weighing different crime risk factors to facilitate the identification of high risk areas (Caplan, Kennedy, & Miller, 2011). This type of analysis is important in countries with low crime rates. In Japan, for example, Ohyama and Amemiya (2018) show that, in comparison with other tools, RTM is twice as effective for forecasting crime. This tool has also been used in countries with high crime rates. In Colombia for example, RTM analysis has enabled an assessment of

the effects of socioeconomic segregation on the risks of falling victim to violent crime in Bogotá by identifying pertinent environmental factors (Giménez-Santana, Caplan, & Drawve, 2018). Escudero and Ramirez (2018) used the same approach to analyze the market for illicit drugs in the same city. They stressed the importance of RTM as a tool for monitoring and evaluating the drug market, and, thereby, for elaborating appropriate prevention strategies.

Another category of studies focused on other ways of utilizing crime analysis. In South Korea, for example, one study demonstrated the utility of information from electronic devices (i.e., the internet of things) for predicting the risk to pedestrians of being victimized by crime, particularly with regard to street level sexual harassment (Suh & Song, 2016). In Japan, Nakamura and Murae (2017) assessed the utilization of public safety maps elaborated by local actors. These maps are designed to identify sites where a crime is likely to occur as well as sites where crime rarely happens, which makes them very useful tools for local public safety assessments. This study demonstrated that public safety maps can improve our understanding of which characteristics are typically found in dangerous places and which in safe ones. Intergenerational consultation and communication were the key factors in contributing to the effectiveness of such safety maps.

Youth, violence and crime

Box 1.11. **National youth violence prevention strategies: an international comparative study**

In 2017, the ICPC conducted an international comparative study of national youth violence prevention strategies in six countries (Canada, Colombia, France, Norway, South African and the United States) with the objective of determining how coordination is ensured during the implementation of prevention policies. This study made the following findings:

- These strategies were influenced by the decline in broad preventative approaches, based on social or primary prevention, in favour of approaches with very specifically targeted prevention activities. Furthermore, none of the countries studied had put in place an integrated youth violence prevention strategy.
- The local level is crucial to the coordination process, both in the operational implementation of prevention actions and in the development thereof. However, real difficulties exist in the effective and coherent coordination of actions at the local level, as well as in coordination between the local and national levels.
- Regarding the issue of participation, this study underscored the lack of systematization with respect to participatory processes which include a broad range of actors.

Source: ICPC (2017)

Street gangs are probably one of the greatest challenges faced by youth crime prevention policies. As such, this was one of most frequently studied issues in the documents indexed and consulted for this study. One study proposed to analyze the impact on the homicide rate of the 2012 truce with the "maras" in El Salvador (Katz, Hedberg, & Amaya, 2016). According to this study's findings, a significant decrease in homicides in El Salvador did occur following the declaration of the truce. In another study, Huey et al (2016) carried out a meta-analysis of interventions with street gangs in North America. According to this meta-analysis, only 37% of interventions addressed the issue from the vantage point of prevention. In particular, Huey et al examined the effects of these interventions on antisocial behaviour and gang membership. The results proved mixed. These interventions had no significant effect on antisocial behaviour. As for gang membership, a weak but statistically significant[8] effect was observed. Sharkey et al (2017) conducted a qualitative research study, based on interviews with youth in a probation program, out of which emerged a few recommendations for facilitating youth gang desistance. These recommendations highlighted the need for comprehensive and coordinated work with all members of the community (families, friends, law enforcement, teachers, etc.). They also emphasized that this type of intervention must not necessarily target gang members only, but should instead address the specific needs of youth in general.

Box 1.12. **The "GREAT" street gangs intervention program: an evolving program**

Widely recognized for its effectiveness, the Gang Resistance Education and Training (GREAT) program is probably one of the world's best known street gang intervention programs. However, beyond its effectiveness, one of GREAT's most interesting aspects is how it has evolved and improved over the course of several assessment processes. In effect, an assessment not only serves to determine whether a measure is effective or not (in a narrow binary sense), but can also serve to promote a process of continuous improvement. The GREAT program was initially criticized due to its origins in a failed program (DARE). It was also negatively assessed because it failed to produce the expected results on gang membership, despite achieving success in relation to other variables (Campie et al., 2017; Esbensen, Osgood, Peterson, Taylor, & Carson, 2013). A second assessment indicated similar results. This led to a reformulation of the program to incorporate, in greater detail, the risk factors associated with gang membership (Campie et al., 2017). The resulting third assessment was positive (Esbensen et al., 2013). In es-

sence, following its reformulation, the program was shown to have an impact on gang membership and on participants' relations with delinquent peers.

Another series of studies focused more particularly on youth violence. One such study sought to assess whether the "Safe and Successful Youth Initiative" in the Commonwealth of Massachusetts has had an impact on violence in its target communities (Campie et al., 2017). This program works with youth aged 17 to 25 with a demonstrated risk of violence, i.e., youth who have either already offended or belong to a street gang. The program focuses on enhancing participants' life skills, social and community relations and situational environment. Unlike other approaches in the United States, this program is not associated with an aggressive policing strategy. The ten cities that adopted this program experienced a drop of 2.8 violent crimes per month, per 100,000 inhabitants, in comparison with thirty other cities in the state, as well as a decrease of between 5 and 5.7 victims of violence per month, per 100,000 inhabitants, among victims aged 14 to 24. Another positive result of participation in the program was that it reduced the risk of incarceration.

Table 1.5. **Factors taken into account in the study by Jennings et al. (2016)**

Protective factors	Risk factors
Individual factors	
Absence of impulsiveness Academic success No physical mistreatment No sexual abuse	Pro-criminal attitudes Neglect
Family-related factors	
Positive parent-child relations	Poverty Unemployed household head
Peer relations-related factors	
Positive relations with peers	Delinquent peers
School and neighbourhood-related factors	
Positive school environment	Exposure to violence
Biological factors	
Early developmental delay	Low birth weight Prenatal complications Perinatal complications
Cultural factors	
No cultural stresses	Cultural assimilation

Source: Jennings et al. (2016)

Jennings et al (2016) studied risk and protective factors bearing on the likelihood of recourse to violence among a population of young Puerto Ricans aged 5 to 13 in the United States. Based on a longitudinal study with three waves of data collection, they found that the cumulative effect of risk factors increased the chances of recourse to violence among children aged 5 to 9 by between 18% and 43% and by between 37% and 63% among children aged 10 to 13. Conversely, the cumulative effect of protective factors played a fundamental role in lessening the chances of recourse to violence: for children 5-9, by between 19% and 45%; and for children 10-13, by between 21% and 33%. In their conclusions, Jennings et al stressed the importance of early prevention for preventing the recourse to violence, particularly in Latino communities in the United States. In the same vein, Souveraine et al (2016) analyzed the factors associated with at-risk youth becoming life-course persistent offenders in South Africa. The two main factors were identified: mistreatment and violence at home and in the school environment, and the presence of family members or friends with criminal records. The severity of the offences committed is also associated with these same factors, as are other factors such as victimization and school performance and motivation. Finally, an offender's age when committing his first offence was found to be associated with mistreatment and violence at home, as well as violence in the immediate neighbourhood.

A meta-analysis updated the current state of knowledge regarding the effectiveness of persistent delinquency prevention programs with at-risk youth (de Vries, Hoeve, Assink, Stams, & Asscher, 2015). This study showed that the overall effect of such programs is positive but minor. In terms of the major approaches, the ones which have proved most effective are behavioral-oriented programs, including behaviour modeling or behaviour contracting and parenting skills training. This meta-analysis also demonstrated that multicomponent programs, and programs conducted outside of the family context, are more effective than individual or group programs.

Another study stressed the difficulties encountered in implementing an evidence-based juvenile delinquency prevention program in Chili (Pantoja, 2015). The program in question offered multisystemic therapy for families, with support from the Under-Secretariat for Crime Prevention. The author pointed out that, despite the program's innovative character, several obstacles prevented its successful implementation, in particular an unfavourable

context and an absence of leadership favourable to innovation. In South Africa, a qualitative study assessed the challenges encountered during the implementation of the "Ke Moja" program, an initiative designed to prevent drug use in the country's schools (Khosa, Dube, & Nkomo, 2017). The authors of this study observed that although the program was considered a success, it faced major challenges, including a lack of ownership on the part of local actors, owing to a top-down approach (see Box 1.8), and low motivationl, due to the low salaries paid to the program's monitors.

Box 1.13. **A meta-review of the effectiveness of prevention and rehabilitation programs**

Weisburd, Farrington and Gill (2016, 2017) conducted a meta-review of the effectiveness of crime prevention and offender reinsertion programs, based on 155 systematic reviews. They identified seven broad policy areas where the effectiveness of such programming has been tested: :

1. **Prevention and social development.** This category is comprised of community intervention programs aimed at preventing antisocial behaviour, which target children and adolescents up to the age of 18 in order to change individual, family or school environment risk factors.

   This type of program generally produces positive outcomes in terms of reducing delinquency and aggressive behaviour. In particular, the more intensive and long term programs have proven highly effective, as have those targeting at-risk children.

2. **Community intervention.** These programs encompass a number of different strategies from civic engagement to interventions with at-risk youth, to correctional services and offender reinsertion into the community. Many different programs have demonstrated their effectiveness.

   Primary prevention programs (mentoring for example) have proven effective. Secondary prevention programs, however, have produced less consistent results. Programs that work on rebuilding and/or establishing social bonds with at-risk youth have demonstrated a high degree of effectiveness, as have community correctional programs which focus on risk factors or on restoring the offender's ties with the community. In contrast, general deterrence programs or punitive programs based on repression produced the most negative – indeed counter-productive – outcomes.

3. **Situational prevention.** These programs focus on reducing vulnerabilities in the built environment or on measures to modify the behaviour of criminals and victims to reduce the risk of criminal activity.

   Measures such as improved street lighting, CCTV cameras, re-victimization prevention strategies, neighbourhood watch programs and counter-terrorism measures have produced desirable effects in terms of crime prevention.

4. **Law enforcement.** This approach includes training programs and interventions related to policing activities, which are designed to influence crime.

"Hotspots" policing, conflict resolution programs, directed police patrolling to reduce gun violence, targeted deterrence approaches and the forensic use of DNA all produce positive crime reduction results. Community policing programs increase the public's satisfaction with the police and improve perceptions concerning the latter's legitimacy.

In contrast, neither second response programs nor drug abuse resistance education (DARE) programs have proven very effective.

5. **Sentencing and deterrence.** This category includes programs designed to assess the effects of sentencing and deterrence on crime prevention.

   The severity of sentencing has not influenced crime nor, for that matter, have general deterrence programs. Mandatory drug treatment programs for women, juvenile drug courts and capital punishment have produced uncertain outcomes. On the other hand, non-custodial sentences and judicial interventions in prison environments have contributed to reducing criminal behaviour. Among the more promising initiatives are mental health courts and other mental health programs.

6. **Correctional interventions.** This category encompasses a range of programs provided in correctional settings, including training, vocational and religious programs, drug treatment programs, psychosocial programs, programs for sex offenders and mental health programs.

   Group cognitive-behavioural therapy programs for offenders in general, as well as ones targeting sex offenders, hormonal treatment programs for sex offenders and therapeutic communities in custodial settings for substance-abusing offenders have all proven highly effective. Programs offering basic education for adults or postsecondary education have also proven to be solidly evidence-based. As have general vocational training programs for offenders. In contrast, insight-oriented therapies for sex offenders have not been effective.

7. **Drug Treatment.** The largest and most enduring positive effects have been observed with naltrexone treatment and therapeutic communities. Both types of treatment have proven effective in reducing consumption and recidivism. Both, moreover, are based on medication as well as social intervention. The only purely medication-based program that has shown promise is buprenorphine substitution therapy. Other types of drug substitution programs – and other reintegration and monitoring programs – have not produced sufficiently conclusive results.

Conclusion

Part I, which dealt with the current trends in crime, highlighted the enormous variations between regions and within regions. Thus, although Latin America remains the region with the highest homicide rate in the world, violence is concentrated in certain countries of that region and, in turn, in certain cities of those countries. Similarly, a country such as the United States, for example, which has experienced a constant general decline in crime since the 1990s, is home to cities with homicide rates higher than most cities in Latin America. This strongly supports the view that the study and prevention of crime, in particular traditional crime, must mainly be based on local conditions. In that sense, rather than regional analyses, what is required is an analysis of the characteristics shared by cities with high crime rates, which in turn implies the need for a deeper comparative knowledge in terms of cities. After all, cities are becoming increasingly important in global terms. As such, urban government is becoming a specific level of governance as important as international and national governance.

Be that as it may, analyses of initiatives by international organizations typically stress the importance of cooperation and coordination between countries and between regions, particularly in relation to a handful of crime related challenges, such as organized crime, terrorism, cybercrime, human trafficking, drug-related issues, corruption, etc. In essence, precisely the types of issues raised by the globalization of criminal activities, which has made borders irrelevant. Organized crime is the best example. Criminal organizations have distribution networks and branches in different countries, and take advantage, for example, of migratory flows to facilitate human trafficking, drug trafficking, etc. No country is able to comprehensively confront this kind of issue while acting in isolation. Hence, the pressing need to coordinate strategies in terms of criminal justice and prevention, as well as to facilitate better information sharing and foster a real willingness to cooperate with other countries. Unfortunately, it is our observation that most cooperation initiatives put greater emphasis on criminal justice than on prevention.

Is it possible to envisage an approach to crime prevention that is simultaneously international and local? At first sight, this seems contradictory, not least because different organizations are involved at each level. However, as we saw in the case of cybercrime, although criminals may conduct their activities beyond a given nation's borders, the victims are mostly local. Hence the necessity of considering the international and local dimensions in an integrated fashion. Instead of studying these dimensions separately, it is increasingly urgent to see crime today from a glocal perspective. Glocalization is a new coinage which refers to the "simultaneous occurrence of both universalizing and particularizing tendencies in contemporary social, political, and economic systems" (Blatter, undated, paragr. 1). Hobbs (1998) was one of the first to apply this concept to crime or, to be more specific, to organized crime, in his discussion of how organized

crime is simultaneously structured and influenced by its international scope and its actions at the local level. This approach, moreover, is also applicable to traditional local crimes. The challenge, then, in a context of glocal crimes, is to analyze the interfaces between the international and local levels, with the objective of developing and implementing comprehensive prevention strategies. Once again, the coordination between these two dimensions – the local and the international – constitutes one of the great issues in crime prevention today.

Contribution

Crime Prediction Model

Developed by Carabineros de Chile with the Centre for Security Analysis and Modeling (CEAMOS) of the University of Chile

> With an average success rate of 35%, this model is widely used in the South American country's police stations where it plays an important role in modeling preventive police patrolling in the country's main cities.

Crime is one of Chile's three most sensitive security problems. Consequently, for some time now, the national police force – los Carabineros de Chile – has adopted a series of measures to provide citizens with better and more effective crime prevention.

One of these measures has been the decisive integration of crime analysis and its associated methodologies as one of the Carabineros' main tools for processing police information and making strategic, operational and tactical decisions.

Among the Carabineros' numerous initiatives to that end was the creation of crime analysis technological platforms, as well as the delivery of clear and timely information to police officers engaged in preventive police patrolling.

In effect, these platforms use digital systems to analyze information on criminal networks, develop offender profiles and carry out crime mapping/georeferencing, etc.

Towards a crime prediction model

One of the ways law enforcement agencies prevent crime is by distributing peace officers to specific locations. Obviously, there is a greater chance of successful prevention when officers are dispatched to areas where offenders would likely have committed crimes were it not for the deterrent effect of preventive police patrolling.

In effect, one of the main challenges of law enforcement agencies is the ability to distribute their personnel to the right locations.

To this end, researchers specializing in crime prevention issues worldwide have designed various models over the years, which, although applied with varying degrees of success, have nonetheless contributed to developing an important body of knowledge on the subject.

It was in this context that the Carabineros of Chile and the University of Chile's Center for Security Analysis and Modeling (CEAMOS) formed an academic and professional cooperation partnership to develop a useful scientific tool for planning police prevention activities as a function of crime "hot spots," i.e., areas with the highest probabilities of being the site of specific types of offences.

This partnership led to the development of a crime prediction model, which is currently in use in 37 of the Carabineros' operational units (police stations) in Santiago, Chili's capital, as well as in 22 other police stations located in the country's other major urban centres.

Integration of three modelss

The model consists of an algorithm based on the following three complex probabilistic models. This model enables the identification of crime risk zones in different areas, which, in effect, endows it with predictive value.

- The Multikernel Predictor Model estimates crime risk by means of spatio-temporal functions called kernels, which are used to identify the periods with the strongest study signals. To that end, the algorithm processes two sets of data on criminal activity: historical trends (a priori data) and latest trends (a posteriori data).
- The Prospective Model is derived from the ProMap software developed by Kate Bowers, Shane Johnson and Ken Pease at the University College of London. ProMap generates a risk surface as a function of time.
- Based on the Dempster-Shafer theory and the theory of belief functions, the Dempster-Shafer Evidence Model calculates probabilities to generate a crime risk surface.

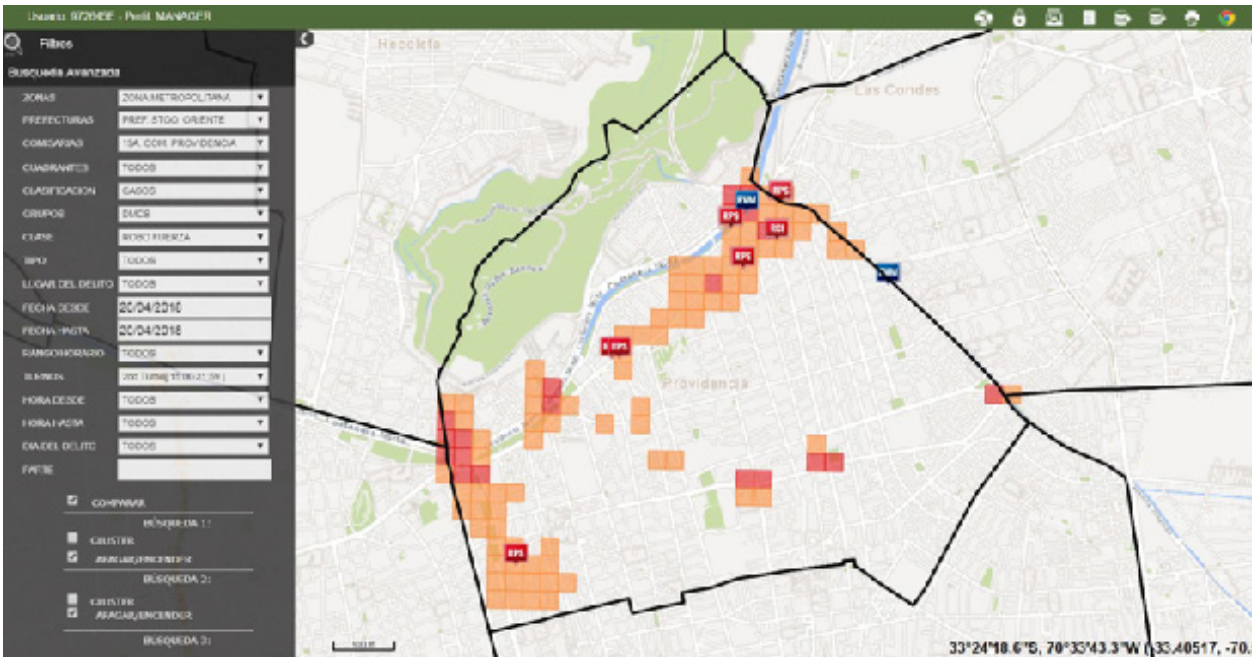
Applications

The development of this new model resulted in the creation of a complex software capable of identifying the zones where there is a high risk of crime early enough for each police station to adequately plan preventive patrolling. In effect, it enables those in charge of planning operations and distributing human and logistical resources to make the appropriate decisions in a timely manner.

These areas of risk are calculated for crimes in the categories of "burglary" and "robbery with violence." The results, which are laid out in a grid composed of squares measuring 150 by 150 meters, apply to the next 5 shifts following the running of the application (which is done every morning).

Moreover, this software has been integrated as a module of the SAIT 2.0 territorial information analysis system (i.e., the Carabineros georeferencing and territorial information analysis platform) for use in the preventive services planning process and for prioritizing patrols in the sectors with the highest risk of certain specific crimes.

Illustration 2. **Screenshot of the SAIT 2.0 territorial information analysis system**



In addition, this crime prediction system is also integrated into the SIMCCAR platform, the Carabineros' mobile monitoring and control system, which enables officers on the ground to access the online databases of security, personal identification and justice agencies by means of a personal digital assistant; this information is highly useful to peace officers engaged in preventive patrolling and identity checks.

The device's menu includes an option (Applications/Map) that shows the predictions on a map according to staffing, geographical location (jurisdiction) and the user's functions and responsibilities. The user can also see his own location on the map and verify whether it coincides or not with the grid's highest-risk areas.

Finally, the simultaneous use of the SAIT 2.0 modules, "Predictor Delictual" (Crime Predictor) and "Monitoreo Simccar" (Simccar Monitoring), enables monitoring of the device's geographical location in the territory and thus the execution of preventive police patrolling and identity checks in the highest crime risk sectors.

To date, the application of this model has generated an average success rate of 35% to 40%.

Illustration 3. **Mobile monitoring SIMCCAR platform**

Contribution

Emerging security actors and the downward trend in homicide rates in West Africa : The case of Burkina Faso, Côte d'Ivoire, Niger and Senegal

Nabi Youla Doumbia
Ph. D in Criminology, University of Montreal
Research Coordinator for the project "Homicides en Afrique", Canada

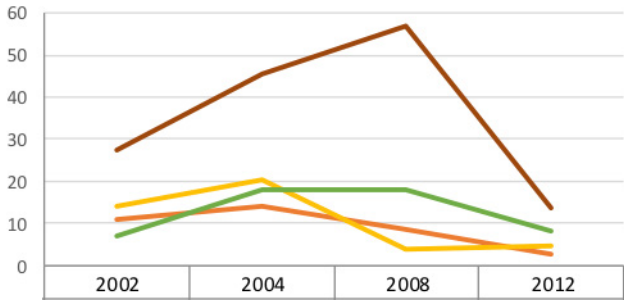
Homicides do not constitute a monolithic category. The term encompasses a multitude of sub-categories based on different motives. In French-speaking West Africa, over a dozen such sub-categories are recognized. The main types in this region are analogous to the main types elsewhere in the world, namely: domestic homicide (infanticide, spousal homicide, etc.); homicides during quarrels and physical altercations, often between friends engaged in petty squabbles; and homicide perpetrated in the course of other crimes, typically armed robbery and rape. These three types of homicide account for over 80% of all cases (Cusson, Doumbia and Yebouet, 2017). The study of homicide constitutes a strategic approach to analyzing the problem of societal violence. In effect, studying homicide amounts to examining a veritable taxonomy of social problems and types of incidents which may culminate in the extreme and tragic outcome of homicide. It follows that preventing homicide entails averting or interrupting the occurrence of incidents and/or social problems such as armed robbery, conjugal violence and brawls. Moreover, homicide data is superior to the data on other types of crime (Van Dijk , 2008). The World Health Organization (WHO) Mortality Database contains statistics on homicide worldwide provided by the United Nations Office on Drugs and Crime (UNODC). This data constitutes a useful resource for international homicide rate comparisons. An analysis of the data suggests a downward trend in homicide rates in the four West African countries considered in this article.

The downward trend in homicides

Figure 1 depicts the trends in homicide rates in Burkina Faso, Côte d'Ivoire, Niger and Senegal. The data was obtained from two sources: Petrini (2010) and UNODC (2014) for the 2002 data, and UNODC (2011, 2014) for the subsequent years. The tracking of the homicide rates over a ten-year period shows an overall downward trend in these four countries. The greatest declines occurred between 2008 and 2012, except in Niger, where they occurred between 2004 and 2008. The most dramatic decrease occurred in Côte d'Ivoire, where the homicide rate fell from 56.9 to 13.6 per 100,000 population, a decline of 43.3 points. The situation in that country is atypical. Between 2002 and 2011, Côte d'Ivoire was the site of a civil war that resulted in the country's partitioning. The loss of state authority in rebel areas and the disorganization of administration in government-held zones led to violence as a means for resolving private disputes. In a word, the absence of a functional justice system drove individuals to seek justice through vigilantism (Doumbia 2018).

Assuming this data is reliable, the overall decline in homicide rates in these four countries is indicative of a long term trend. Criminology offers an explanation for this trend based on routine activities theory (Cohen & Felson, 1979). According to this theory, a homicide occurs when there is convergence in a given time and place of a motivated offender (killer), a target (rival) and the absence of a capable guardian. Should any one of these conditions fail to obtain – i.e., the motive for murder, the presence of a rival and the absence of a capable guardian – the crime will not be committed. The motivations to commit homicide vary little from country to country. The pursuit of glory, power, women and honour are, today as in the past, the main reasons for killing around the world (Cusson, 2015). As conflict is part of human nature, an existence free of rivals is unlikely. On the first two fronts, we cannot assume marked differences between these countries. The remaining factor, the absence of a guardian, is a function of the adequacy of social controls (or the lack thereof).

Figure 1. **Trends in homicides in West Africa**



	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

In the case of Côte d'Ivoire, the staggering homicide rates were clearly due to political turmoil. With the end of the crisis came an improvement in the situation, thanks, in particular, to the restoration of administrative and police networks throughout the country, combined with a weapons collection program, as part of a process of demobilization, disarmament and reintegration (DDR) of former combatants. As for the four countries taken together, declines in homicide rates can be attributed, in part, to the steady and exponential growth in the private security sector since the beginning of the 2000s (Bryden, 2016). According to data from the Private Security Observatory, this sector employs more people than do the public security forces. In Côte d'Ivoire, for example, it employs over 70,000, and in Burkina Faso, over 30,000 (Observatoire de la gouvernance de la sécurité privée, 2018). In addition to these formal actors are informal actors, such as traditional hunters and ethnic and clan organizations, etc., which also play a role in security (Baker, 2008). In short, guardians exist who help to deter and prevent theft and fighting, and thereby, the homicides linked with such incidents. Their early interventions can help to stop the escalation of spousal violence, provided adequate follow-up also occurs. Last but not least, private security, as one of the leading employers, constitutes in itself a form of social prevention. In a situation of chronic unemployment, this industry provides many young people a way out of situations of economic vulnerability, a well-documented risk factor of violence. In spite of this trend, homicide rates in the four countries remain relatively high, well above those in European countries (1.5 per 100,000 population) for example. Reducing them further requires overcoming numerous challenges.

Challenges

Homicide is not an inevitability, and certain measures can reduce its prevalence. At the structural level, the fight against poverty and inequality is critical. There is a strong correlation between each of these two variables and the homicide rate (Ouimet, 2012; Van Dijk , 2008). That said, the social indicators in these four countries are far from stellar. The poverty level is generally abysmal. The best performing of the four countries, Senegal, ranks 163rd on the Human Development Index out of the 188 countries (UNDP, 2014). Inequality is high: the Gini index varies between 0.31 for the lowest score (Niger) and 0.43 for the highest score (Côte d'Ivoire). The prospect of the coming economic emergence of these four countries should provide the conditions and means for greater redistributive justice.

In terms of the current context, the pursuit of regional political stability is more urgent than ever. As the case of Côte d'Ivoire demonstrated, political conflicts create a situation of anarchy that encourages vigilantism and the spread of guns and drugs, which are facilitators of homicide. When the state collapses, sovereignty and the rule of law slip away (Zartman, 1995; Rotberg, 2004). In this regard, the mid-Sahel region in Senegal, Niger and Burkina Faso has become a hub for organized crime, where Al-mourabitoun terrorists and their associates engage in trafficking of every kind (UNODC, 2013; Zeïni, 2014). Control over arms and drug trafficking in the countries of West Africa is contingent on the pacification of terrorist-held zones.

At the organizational level, the upsurge in the numbers of private security actors, both formal and informal, is not without its problems as regards human rights and the prerogatives of public authorities. Better security governance, by means of a strategic prevention plan, which integrates public and private stakeholders and organizes their actions around a few common objectives, could foster better relations between the different entities and enhance their collective effectiveness (ICPC, 2016). Likewise, the use of new information technologies, cell phones and Facebook to name a few, offers opportunities to educate and create awareness about non-violence, as well as detect and report crimes; in the same vein, the use of an electronic wallet deprives attackers of potential gains. These electronic tools have enormous under-exploited potential.

Finally, there is the epistemological challenge. Research is needed to evaluate and improve security practices (Bowles, Akpokodje, Tigere, 2005; World Health Organization, 2014). As new security stakeholders and new practices emerge in the region – whether it be Kolweogo, a neighbourhood watch group in Burkina Faso, the community safety support agency (Agence d'assistance à la sécurité de proximité-ASP), a para-governmental agency in Senegal, or video surveillance of the Plateau, in the business district of Abidjan, Côte d'Ivoire – little independent research has been done to assess these initiatives. And yet, the best security solutions are those that bear the imprint of their local conditions (Crawford, 2009; UNODC, 2016). Given that the countries of West Africa share many traits, it is logical to assume that a solution that has proven effective in any one of these countries would be successful if applied region-wide.

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 The relationship between national homicide rates and the percentage of female homicide victims is characterized by a logistic distribution (based on 2015 data). In other words, it is represented by an inverse regression curve which accounts for over 40% of the variance (R^2 = 0,403; f= 29,688; p < 0;05). This supports the conclusion that the relationship between the homicide rate and the percentage of female victims is inversely proportional: the higher the homicide rate, the lower the percentage of female victims (r= -0.42; p<0,05)..

4 As a remedy to the major gaps in data, estimates were made using an econometrics methodology known as multiple imputation. These conclusions are derived from the resulting estimates.

5 This literature review was based on online searches conducted between January 2015 and October 2017 using two key word phrases: «crime prevention» and «community safety.» Two search engines were used: ProQuest and Google Scholar. After reviewing the titles of the documents in the search results, we compiled a list of 233 documents. Following a review of these documents, we narrowed our list to 65 scientific papers.

6 The total number of topics is 121, as a number of the 65 documents addressed more than one topic.

7 According to the study: "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 Significant means that the effect was statistically significant within a 5% error margin. On the other hand, the strength or weakness of an effect refers to the size of the effect on the variable to be explained. Thus an effect may well be both significant and weak.

References

Chapter 1. Trends in crime and its prevention

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. Retrieved from 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. Retrieved from 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. Retrieved from https://www.britannica.com/topic/glocalization

Bonilla, M. E. (2016). Community participation in matters of public safety in Bucaramanga and its Metropolitan Area. Pesented at 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. Retrieved from 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. Retrieved from 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

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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/International_Report/CIPC_5th-IR_EN_17oct_Final.pdf

ICPC. (2016b). La sécurité dans les transports publics terrestres. Montréal : Centre International pour la prévention de la Criminalité. Retrieved from http://www.crime-prevention-intl.org/uploads/media/Rapport_sur_la_securite_dans_les_transports_publics_FINAL_01.pdf

ICPC. (2017). National Prevention Strategies for Youth Violence: An International Comparative Study. Montreal: International Centre for the Prevention of Crime. Retrieved from http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/2017/National_Prevention_Strategies_for_Youth_Violence_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. Retrieved from 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. Retrieved from 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. Retrieved from 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.

UNODC. (2015a). Classification internationale des infractions à des fins statistiques. Vienne: Office des nations unies contre

la drogue et le crime. Retrieved from http://www.unodc.org/documents/data-and-analysis/statistics/crime/ICCS/ICCS_French_2016_web.pdf

UNODC. (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. Retrieved from https://www.unodc.org/documents/congress/Declaration/V1504152_French.pdf

UNODC. (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

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. Retrieved from https://www.unicef.org/jamaica/Overview_Report_(High-Res).compressed.pdf

Small arms survey. (2007). Guns and the city. Cambridge: Cambridge Univ. Press. Retrieved from 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. Retrieved from 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. Retrieved from 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). 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/

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

Emerging security actors and the downward trend in homicide rates in West Africa...

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/

UNODC. (2016). Recueil des règles et normes de l'organisation des Nations Unies en matière de prévention du crime et de justice pénale. Vienna: UNODC.

UNODC. (2011). Global study on homicide 2011. Vienna: ONUDC.

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

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

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.

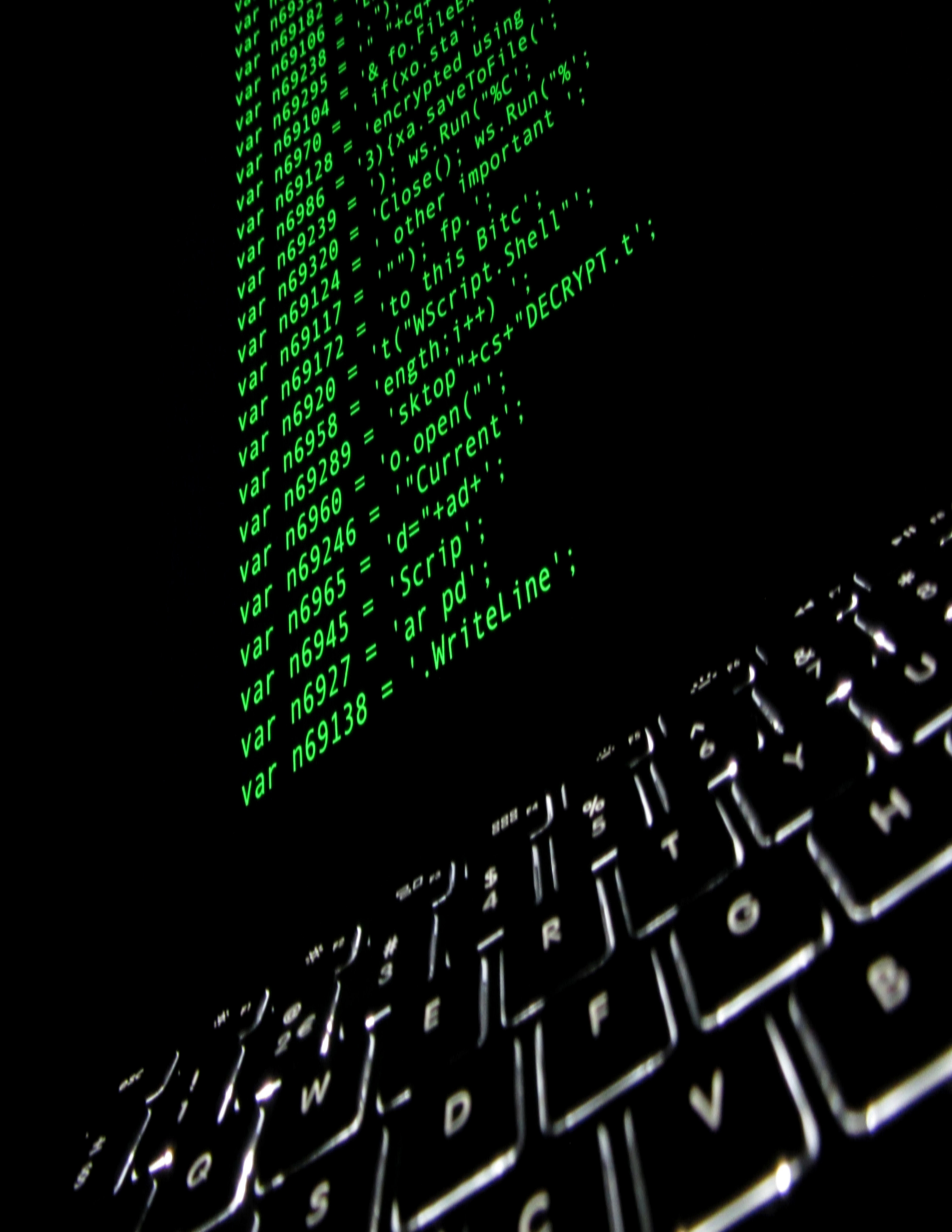
PNUD. (2014). Rapport sur le developpement humain 2014. Genève.

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

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

CHAPTER 2

CRIME IN A DIGITAL WORLD

In Chapter 2, we problematize our approach to cybercrime phenomena. To that end, we begin with an examination of cyberspace (i.e., the specific environment where cybercrime occurs) by specifically focusing on governance issues and factors of inequality. In the chapter's second section, we consider the difficulties intrinsic to quantifying cybercrime, difficulties which are structural, methodological and conceptual in nature. Finally, in the third section we propose a somewhat impressionistic global overview of cybercrime.

Introduction

The year 2017 was marked by the hacking of the website of Equifax, a giant American personal credit bureau. As a result, the personal information – date of birth, social security number, driver's licence or credit card number – of 147.9 million persons in the United States, Canada and the United Kingdom was compromised (Sweet, 2018). This meant, moreover, that it was potentially available on the Dark Web, i.e., in the unregulated corners of cyberspace. This creation of 147.9 million potential victims of fraud and identity theft, in the wake of several security breaches, constituted the biggest theft of such sensitive personal information in history. A dark scenario indeed. «On a scale from one to 10, this is a 10 in terms of potential identity theft» opined Avivah Litan, an expert in cybersecurity interviewed by the British newspaper The Independent (Griffin, 2017). This highly publicized affair raised several major issues. It was, in effect, emblematic of how cybercrime is forcing us to re-examine our ideas, practices and modes of governance on the internet, as well as in the "real" world.

Concerning the crime itself, we still know very little beyond the basic facts. And for good reason: the investigation into the causes of this event, and its ins and outs, was conducted by Mandiant, a private cybersecurity firm retained by Equifax. As a result, the publicly available information is quite limited. Nevertheless, we do know that it was a security flaw in Equifax's internet portal that led to the hacking of its website. This security flaw was discovered in March by the Department of Homeland Security and immediately brought to the company's attention, which subsequently offered its assurances that efforts were implemented to stop the intrusion (Wattles & Larson, 2017).

Two observations come immediately to mind. First, this affair shines a brutally harsh light on the vulnerability of the actors (public or private) who collect, store and use personal data. Their vulnerability to hacking translates, in turn, into increased vulnerability and exposure to cybercrimes for the individuals whose personal data is stolen. A New York Times editorialist wrote, bitingly: «Equifax, you had one job. Your only purpose as a corporation, the reason you were created and remain a going concern, is to collect and maintain people's most private financial data» (Manjoo, 2017). Secondly, it's important to underline the fact that the investigation was conducted internally, by a private firm; in effect, the public authorities were excluded from the role of crime investigation, which traditionally falls to them. Furthermore, the information on this incident, which concerned, after all, nearly 150 million potential victims, was managed by the company implicated, from the vantage point of corporate communications.

Also of concern was what happened after the crime, particularly in terms of crisis management. Following the completion of Mandiant's investigation, Equifax issued a statement explaining that a series of intrusions took place between May and July 2017, and that these were detected on July 29. However, it wasn't until September 7 that Equifax made this announcement and divulged the number of potential victims, i.e., over a month after it had discovered what happened, which is in itself problematic. The company offered potential victims the option of controlling access to their personal credit data during a one-year period, but left it to individuals themselves to carry out all the procedures necessary to secure their credit status with the four other main credit bureaus. Finally, Equifax made the divulging of information on a potential victim's individual risk of exposure to hacking conditional on the latter's abandoning of any individual or class action proceedings against the company.

This crisis and the manner in which it was handled raise a number of issues. In particular, two core observations warrant attention from a prevention perspective: 1) potential victims were left to their own devices; and 2) there is an absence of clearly established responsibilities on the part of the data collecting entity in the event of this type of security incident. For many critics, this surreal situation was enabled by the inadequacy of the regulatory frameworks in relation to hacking incidents (Turner, 2017).

Thirdly, there are a number of implications for the future. The first concerns the value going forward of certain types of data. In effect, any information that is so vulnerable and relatively easy to obtain can no longer serve as a reliable means of personal identification. As Nathaniel Gleicher, Head of Cybersecurity Policy under the Obama administration, stressed in a statement released a few days after the incident: "This breach might just have put the nail in the coffin of the idea that we can use personal identifiers like Social Security numbers as security factors" (Pierson, 2017). Secondly, there are the legal implications. As might be expected, a number of legal proceedings were brought which challenge the highly disputed clause that stipulates that potential victims' access to information on their post-hack vulnerability is conditional on the renouncing of any potential legal action against Equifax. Such proceedings have already taken the form of class action suits in Canada (Meckbach, 2018) and the United States (Harney, 2017), as well as other forms, including recourse to small claims courts (Murphy, 2018). These proceedings will likely set legal precedents on the matter of liabilities. Finally, in terms of legislation, developments may be in the offing in the United States, notably through the commitment of elected officials such as senator Elizabeth Warren who intends to use this event to promote stricter laws concerning the responsibilities of corporations that collect perso-

nal data. As the senator put it an interview with Vox in February 2018: "For years, Equifax and other big credit reporting agencies have been able to get away with profiting off using people's private info and doing so without their explicit permission. We need real consequences for when they screw up." (Stewart, 2018). Equifax has had to explain its management of personal data before the Senate Banking Committee and must henceforth collaborate with several American agencies, at the federal and state levels to not only clarify the details of the 2017 incident, but also to justify its subsequent actions. In addition, a draft bill, proposed by Democratic senators Warren and Warner, seeks to: 1) clarify the responsibilities of these data collection giants; 2) establish sanctions when incidents occur as a result of security deficiencies; 3) create a federal agency to oversee cybersecurity with a specific mandate to monitor the practices of credit bureaus; and 4) encourage private sector investment in cybersecurity (Stewart, 2018).

The Equifax affair highlights all of the major issues raised in connection with cybercrime, including: our **vulnerability** as individuals or as large public or private sector organizations; the **inadequacy of the frameworks for understanding, regulating and managing** practices developed in cyberspace, including those involving extremely sensitive information; the lack of clarity on actors' respective responsibilities; the emergence of **polycentric governance** model, in which public authorities no longer play the role of guarantor, adjudicator and protector of the rights and interests of individuals and organizations; and finally, the need to develop innovative approaches for governing cyberspace, preventing cybercrime and protecting potential or actual victims.

This chapter proposes then to provide an overview of "what we know" about cybercrime today. First, we will examine cyberspace as the highly singular environment that it is, in an endeavour to identify which of its characteristics most influence how cybercrime and cyber-victimization occur and develop within it. In particular, we will closely consider the questions of inequalities in cyberspace access, digital skills and usages. Next, we will offer a geographic overview of cybercrime which, in the absence of good data, will largely consist of a survey of what information is available. Finally, we will take a closer look at the principal implications and major issues, in terms of prevention.

Cyberspace: Governance, inequalities and the implications for crime

Cyberspace is a system formed by interactions between connected devices, interactions which may take the form of data or information transfers. As such, cyberspace is both virtual and physical in nature (Malecki, 2017). The internet's growth in all spheres of modern life constitutes an aspect of the globalization of trade as well as the advent of what the sociologist Manuel Castells calls the "information age" (Castells, 2002). Cyberspace has grown by leaps and bounds due to developments such as the democratization of internet access, the boom in mobile accessibility through smartphones and, more recently, the spread of the internet of things.

Cyberspace constitutes far more than a support for, or extension of, the "real" world: it is a distinct environment with specific characteristics. According to researcher Wanda Capeller (2001), an implication of this shift in environment is that the deviant and criminal activities which develop in it are both extensions of the real world (when illegal activities invest in and adapt to cyberspace) and departures from it (when criminal activities take advantage of the opportunities offered by this new environment). Consequently, a key to understanding cybercrime is understanding cyberspace's functioning and characteristics, in particular its governance model, i.e., the system of actors and processes which condition how it is regulated. Cyberspace governance is articulated around three essential types of actors: 1) those who develop, operate and administer the physical infrastructure, which enables connection between devices and the storage of virtual data; 2) those who provide access to cyberspace; and 3) those who provide the services enabling the most important uses (data storage, social media, content platforms, cybersecurity).

This governance model constitutes a direct challenge to the Westphalian paradigm, which is premised on the central role of the State, as well as to the key concepts and notions traditionally associated thereto, such as the rule of law, security, borders, human rights and sovereignty. Moreover, this situation is further complexified by rapid technological advances and the attendant consequences on cyberspace access, usages and governance. As a consequence, state institutions are struggling to adapt and offer effective solutions (Liaropoulos, 2017).

Accordingly, cyberspace lends itself, it is argued, to a model of governance which transcends the Westphalian State and traditional borders, in favour of global governance based on a cooperative decision-making model where state and non-state actors must collaborate in order to address challenges beyond the scope of their respective capacities and actions (Finkelstein, 1995). A central precept of this model is that cyberspace must turn to the core actors mentioned above, which, for the most part, are from the private sector.

This latter point in particular has crucial implications for cybercrime prevention. In effect, from its very outset, cyberspace was designed as both a platform for commerce and a libertarian political project, as attested in the 1996 "Declaration of the Independence of Cyberspace," which rejected all state intervention or control (Electronic Frontier Foundation, 1996). This libertarian utopia underlies a number of the characteristic arguments expressed in current debates on cyberspace governance where the notion of regulation by public sector authorities is opposed by a conception founded on a libertarian notion of the common good.

However, with the democratization of access and usages, it is the major private sector actors who have largely monopolized decision-making and governance in cyberspace, thanks to their capacity to provide access to cyberspace and the tools enabling its different uses. The libertarian utopia has become a capitalist reality. These private actors are, however, localized in given states,

as is their infrastructure. As such, they are subject, to a certain extent, to national state jurisdiction. Consequently, the project of a multi-actor model of governance, characterized by the equitable representation of the interests and importance of all users and stakeholders, remains a major challenge, one that is far from forming a consensus, much less becoming a reality (Liaropoulos, 2017; Pereira, 2016).

The governance of cyberspace is concentrated in the hands of a small group of actors. This situation implies a number of major challenges in terms of cybercrime and cybersecurity :

- How do private actors, central in the governance of cyberspace, envisage security for all, particularly regarding the most vulnerable users (individuals, vulnerable groups, victims)?
- How are the priorities in the fight against cybercrime determined? For example, what is the weight accorded to crimes prejudicial to private interests vs. crimes against persons, especially highly vulnerable persons (e.g., child pornography, violence against women, hate crimes, etc.)?
- What form should intervention take in the areas of cyberspace not regulated by the principal private or public actors (i.e., the so-called Dark Web)?
- How should public policy and legislative regulation, two essential instruments in the fight against crime and for protecting victims, be adapted to the realities of cyberspace and its actors?
- How to promote partnerships between the public and private sectors to guarantee the security of all users equitably and in the common interest?
- How, finally, are fundamental individual and collective rights, such as the freedom of expression and political liberties, to be guaranteed?

In order to better understand the links between cyberspace and crime, it's important to first examine the transition from the real world to the virtual world: how is it operationalized and what are the consequences in terms of criminal phenomena? There are a number of ways of looking at this question. We choose to do so from a prevention perspective, which requires the identifying of the connections between criminal activities and various criminogenic factors, including first and foremost inequality issues.

Cyberspace and inequality:

In contrast to the internet's foundational ideals of accessibility and democratization, cyberspace is in fact characterized by a digital divide, particularly regarding the issues of access, skills and security. These three issues, moreover, are crucial factors in cybercrime, from the point of view of both perpetrators and victims.

Stansbury (2003) distinguishes four principal types of inequality: the access divide, the skills divide, the economic opportunity divide and the democratic divide, which in turn influence, according to her, how individuals use cyberspace. Other authors favour a taxonomy based on the theory of technological resources appropriation, which distinguishes inequalities in four successive dimensions of access: motivation, physical and material access, digital skills and usages (Dijk, 2012). These inequalities are also known as "digital divides," a term employed in the plural to underscore their multi-faceted and multi-factoral character. Originally, the term digital divide referred firstly to issues of access (Warschauer, 2004), secondly to digital skills (Hargittai, 2011) and thirdly to usages (van Dijk & Hacker, 2003).

The current state of knowledge and body of literature on these questions is still in its infancy, as is the case with all cyberspace related issues. That said, very dynamic research is being done on the digital divides and their links with real world inequality factors. In the interests of a concise discussion of the major research trends, we have opted to focus more particularly on the first digital divide, which, moreover, is better documented. Very brief descriptions will then be given of the second and third digital divides before we analyze the relationship between these digital divides, taken as a whole, and cybercrime.

The first digital divide: access to cyberspace

First of all, it should be underlined that access to cyberspace per se is deeply unequal, in the first instance for technological reasons: in the absence of network infrastructure and/or devices to go online, cyberspace remains out of reach. In practice, the different types of access from broadband to mobile data services and everything in between, including cyber cafés and public access points, such as schools, encompass a range of heterogeneous means of differentiated access. In this sense, there is not a cut and dried "digital divide" between those who have access and those who do not, as this term in fact signifies a complex set of situations characterized by varying degrees of ease of access (Warschauer, 2004).

This digital divide, defined by differences in the ease of access to cyberspace, parallels most of the conventional inequality factors found in the real world. The level of development, an individual's social and economic status, age, gender, place in the public space, access to services and level of education are all pertinent indicators regarding access to cyberspace. Moreover, these factors are just as relevant in terms of "traditional" criminal activities, in relation to both offenders and victims (ICPC, 2005, 2010, 2011, 2012a, 2012b). Consequently, in addressing cybercrime prevention it is crucial to first examine the inequality factors, which characterize cyberspace.

1. The digital divide and development inequalities

Global economic inequalities have had a considerable impact on how access to cyberspace has developed in different countries. As an essential aspect of globalization, the internet has mirrored

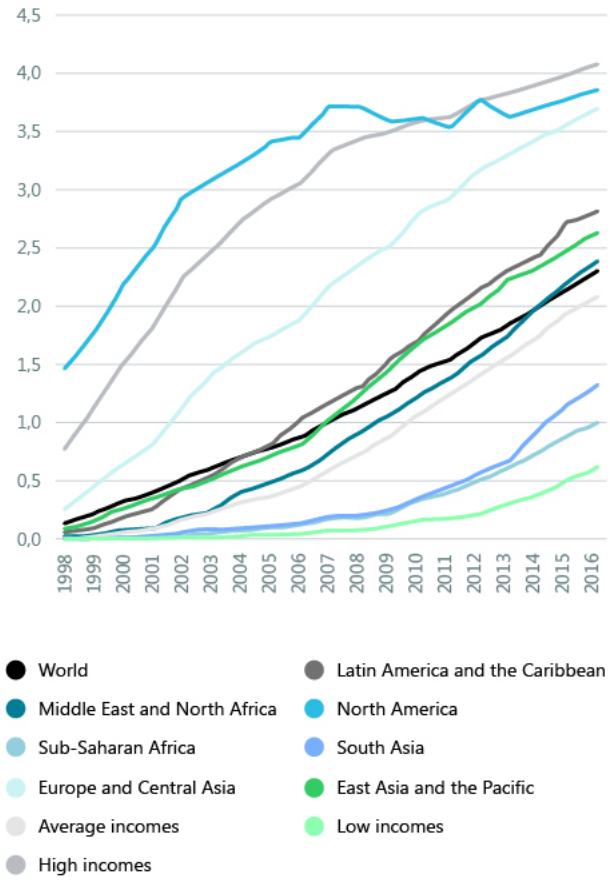
the dynamics of the latter broader phenomenon, particularly in terms of the regional differences in its development. In effect, the internet was born and initially developed in the West and the wealthiest countries, prior to spreading further afield via the main channels of the globalization process: urbanization and economic development. The relationship between internet penetration and economic development is illustrated in the diagram below.

PA number of observations may be drawn from the above diagram. First of all, the expansion in access to cyberspace at the turn of the century did not close the existing gaps between countries at different levels of economic development. Far from it, as these gaps actually widened. The less economically developed countries, particularly in Sub-Saharan Africa and South Asia, have been left on the sidelines of this technological revolution. Thus, although growth in Internet access has accelerated in these regions in recent years, particularly due to the boom in access via mobile telephones, internet penetration rates continue to lag significantly. According to the International Telecommunication Union, 17.5% of the inhabitants of the less developed countries had internet access in 2017, vs. 6% in 2012 (International Telecommunication Union, 2017c).

A second interesting observation may be made regarding cyberspace "seniority": web users from Western countries and other wealthy countries have had longer experience navigating cyberspace, which, as a consequence, was developed and shaped by and for them. This had a major impact on the character of the second wave in internet access, which opened cyberspace to the emerging countries, that is to say the middle classes of high growth emerging economies and, to a lesser extent, those of the less developed countries.

Thus, as regards the conditions and characteristics of this new cyber environment, the first digital divide not only concerns issues of access, but also indirectly affected issues of ownership, usages and digital skills due to the formative imprint made by the initial users of cyberspace. In a word, the first digital divide directly conditioned the second digital divide.

Figure 2.1. **Trends in Internet penetration rates per region and national income level**



Source: World Bank (2017)

2. The digital divide and social and economic inequalities

Inequalities in access are highly apparent in country-to-country comparisons. This observation must not, however, mask the inequalities within societies and countries. Interestingly, whereas socioeconomic inequalities are absolutely central factors in conventional criminological and sociological approaches, the scientific literature which examines how such inequalities are expressed in cyberspace tends to show that they have a much more complex and indirect influence on the issues of access, digital skills and usages (van Deursen & van Dijk, 2013).

In effect, several studies conducted in rich Western countries concur in finding greater internet use among the least advantaged economic classes (Fuchs, 2009). In particular, children and youth from less advantaged backgrounds use the internet more than other children and youth. This, in conjunction with less parental supervision, reinforces pre-existing inequalities, notably in relation to the chances of academic success (Camerini, Schulz, & Jeannet, 2017). This finding is particularly crucial for understanding the links between socioeconomic factors and cybercrime. In effect, an economically disadvantaged background, when combined with a lack of supervision of leisure activities and a greater risk of school failure, may be indicative of higher criminogenic risk factors.

However, this finding should be qualified, inasmuch as it is specific to studies done in the richest countries where issues of access are less salient. In emerging countries and in less developed countries, economic and social determinants continue to have a major impact on cyberspace access, digital skills and usages (Fuchs & Horak, 2008). Moreover, a crucial distinction must be made regarding the urban-rural divide in matters of access (Alzouma, 2013). As noted above, in developing countries, globalization and its characteristics, including democratized access to cyberspace, is a process that affects urban areas first and foremost.

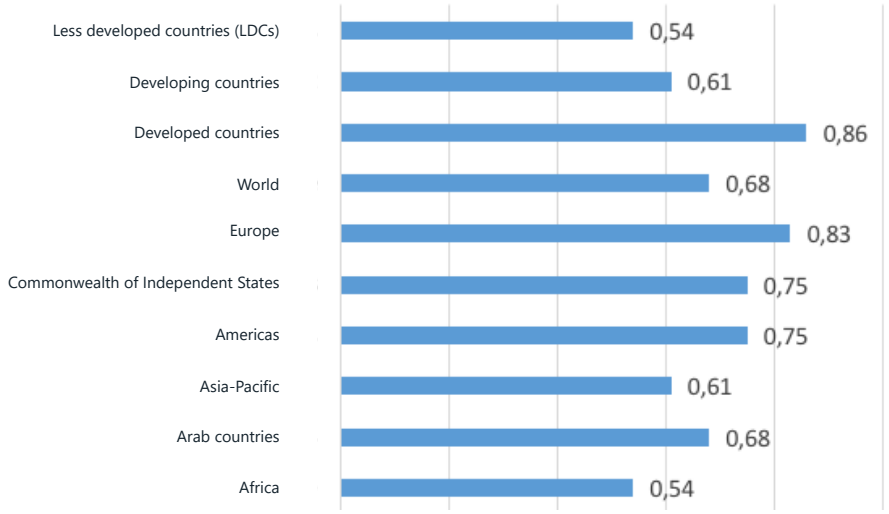
3. The digital divide and socio-demographic characteristics

Although economic factors are important in the formation of digital divides, other factors, such as generational issues, gender, education, disabilities, membership in a minority, etc. also play roles which are no less important. In that light, we will now examine the following aspects: 1) the relationship between youth and the rise of cyberspace, particularly in emerging countries; 2) the gender factor in internet access and; 3) the complex links between education levels, digital skills and usages, and vulnerability.

The digital revolution and the advent of cyberspace are often seen in generational terms with a clear demarcation existing between technological "natives" and their elders. In fact, the dynamics in play are more complex and encompass a range of inter-related factors (Helsper Ellen Johanna & Eynon Rebecca, 2013). For example, it's important to distinguish between different contexts, particularly in terms of economic development. The diagram below highlights the relative importance of younger generations in cyberspace as a function of their country's level of economic development.

As the above diagram indicates, in the developing world, inter-

Figure 2.2. **Ratio between the 15-24 age group's internet penetration rates and its share of the total population**



Source : International Telecommunication Union (2017c)

net use is disproportionately high among youth. This is particularly the case in the less developed countries, especially in Africa and Asia. This generation gap is less marked in the richest and most wired countries.

It should be noted that this expansion in internet access among youth remains profoundly unequal in global terms: in effect, 94% of youth aged 15-24 in developed countries are internet users vs. 67% of their peers in the developing world and only 30% in the less developed countries (International Telecommunication Union, 2017b). The widespread perception of an ultra-connected "Generation M" only applies to the youth of the wealthiest countries, as their counterparts in the emerging world still face unequal access.

In addition, whereas youth are at the heart of the cyberspace revolution, this paradigm shift has, to an extent, left their elders behind: thus, in OECD countries, the internet penetration rate is 95% in the 16-24 age group vs. just 63% for the 55-74 age group (OECD, 2017). However, the greatest generational inequalities between Generation M and their elders is not found in Western countries, but rather in the emerging world.

These generational factors must be understood in conjunction with another major dimension in relation to inequalities: gender. The diagram below indicates the gender differences in internet access in the world's major regions, as well as those attributable to the level of development.

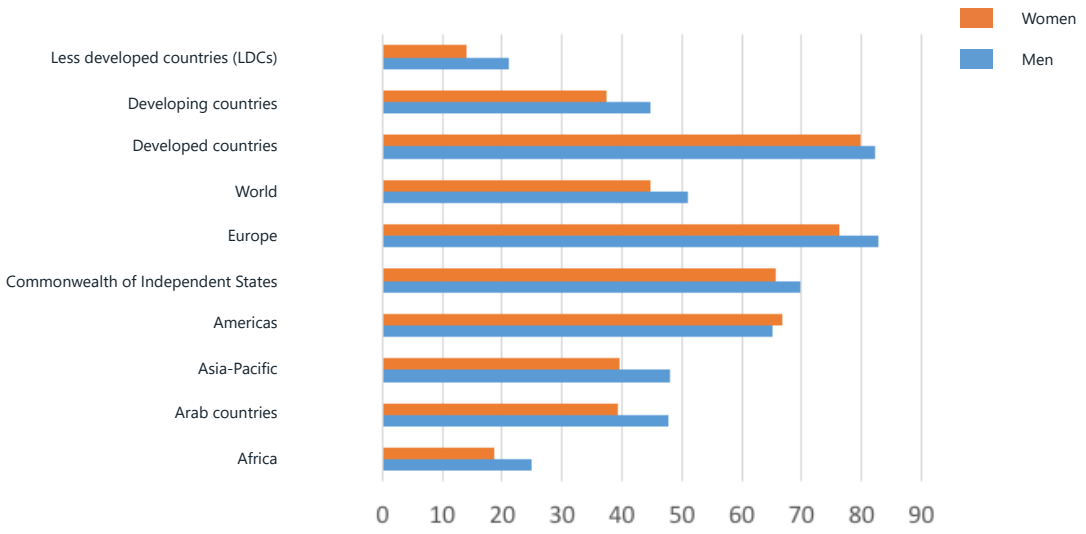
The repercussions in cyberspace of the gender inequalities observed in the real world are, yet again, entirely evident, with the notable exception of the Americas. Furthermore, the most marked differences are found in the emerging world and in the less developed countries, as was the case in relation to generational differences. This observation confirms preceding observations and indicates that real world inequalities have a more significant impact in regions where the digital divide is wider.

The second and third digital divides: inequalities in digital skills and usages

These real world inequalities also impact digital skills and usages. In other words, even in situations of equivalent access, certain web users face inequality factors which affect their capacities to understand and master technological tools, their ways of surfing cyberspace, the activities they engage in and the tools they use while online (van Dijk & Hacker, 2003). The classic inequality factors (economic development, individual social and economic inequalities, education, gender, age) are also in play in relation to the second and third digital divides. As a result, they have been the subject of a number of recent studies.

Van Deursen and van Dijk, for example, (2010) highlight the decisive importance of education levels in the acquisition of the skills necessary to take full advantage of the opportunities offered by internet access. Blank and Lutz (2016) went beyond the question of unequal access to benefits by also addressing the issue of exposure to harm. Interestingly, their study shows that the most educated internauts and those most concerned by privacy issues in cyberspace are more exposed to harm than other categories of

Figure 2.3 **nternet penetration rate per gender and by region**



Source : International Telecommunication Union (2017)

web users, particularly their least technologically advanced peers. This correlation between a more sophisticated level of knowledge and usages and a greater vulnerability to cybercrime is not only observed among individuals, but is also characteristic of organizations and States: in effect, as Speer (2000) stresses, the States most dependent on information and communication technologies are also the ones most exposed to the risks of hacking.

Cyberespace, inequalities and cybercrime

According to Majid Yar,

> "The Internet should not be viewed as simply a piece of technology, a kind of 'blank state' that exists apart from the people who use it. Rather, it needs to be seen as a set of social practices – the internet takes the form it does because people use it in particular ways and for particular purposes." (Yar, 2006, p. 6)

It's clear that cyberspace constitutes a distinct reality with its own specific characteristics. The characteristics of the real world do, however, influence how users navigate and function in cyberspace. As such, they also impact the factors influencing cybercrime and cyber-victimization. Nevertheless, as this influence is indirect, we must rethink our analytical approaches and comprehension of cybercrime phenomena by taking into account the particular environment that is cyberspace.

The question then is to determine what effects these digital divides and inequality factors have on cybercrime phenomena: in other words, do the social, cultural, economic and political factors underlying unequal access to cyberspace, knowledge, digital skills and usages have a decisive influence on the life paths of cybercrime offenders and victims? For example, youth who make massive use of cyberspace are particularly vulnerable to cybercrime. Regarding crime in the real world, it's well known that victimization and delinquency are intimately connected processes, especially among young people. In effect, victimization and the exposure to criminal and violent activities constitute important risk factors in the development of these types of behaviour (Margaret Shaw, 2001; WHO, 2015). One hypothesis, then, is that there exists a link between greater youth access to cyberspace and higher risks of victimization and/or delinquency.

Bert-Jaap Koops (2010) proposes a vision of risk factors which focuses on the opportunities generated by cyberspace's intrinsic characteristics. In short, rather than further rehashing the issue of how real world factors influence the development of criminal activities in cyberspace, for Koop the real question is: how does cyberspace provide opportunities for such activities? This approach leads him to posit 12 cybercrime risk factors: global reach, deterritorialization, flexible networks, anonymity, distant interaction, data manipulability, automation of processes, scale effects, the capacity to aggregate large numbers of insubstantial gains, the information economy, structural limitations to capable guardianship (i.e., social control and monitoring) and, finally, rapid innovation cycles.

It's important to emphasize that research on the relationships between "real" world inequalities and the abovementioned digital divides, on the one hand, and the phenomena of cybercrime (Kigerl, 2012, 2016) and cyber-victimization, on the other, remains a newly emerging field of study (Halder & Jaishankar, 2016; Jaishankar, 2011; Jaishankar & Halder, 2011), particularly with respect to cyberviolence and the victimization of the most vulnerable groups (Nicola Henry & Anastasia Powell, 2016).

For researchers, the question of cyberviolence, currently a central concern in criminology, is on the cutting edge of their research agenda. Moreover, from the point of view of both knowledge generation and cybercrime prevention, it constitutes the major issue confronting decision-makers, one which we will examine in greater detail in Chapters chapters three and four.

Defining and measuring crime in the cyberspace age

The very definition of cybercrime constitutes a fundamental debate in criminology today (Yar, 2006). Generally speaking, there are two basic definitional approaches, premised on radically different epistemological perspectives on the very nature of crime in cyberspace. According to one view, cyberspace mirrors the physical world and, as such, allows for the continued, if adapted, utilization of the principal theories in criminology. In contrast, the second school of thought advocates a new approach to cybercrime, based on its sui generis nature (Stratton, Powell, & Cameron, 2017). In Chapter three, we will turn our attention to these debates and to the current criminological research on cybercrime.

Nevertheless, although criminologists may still be grappling with the fundamental challenge of defining terms in a totally new field of study, the urgency and importance of the existing criminal phenomena in cyberspace are such that the authorities must forge ahead and define the appropriate legal and policy frameworks in response. In particular, one of the major implications of cybercrime is that it radically redefines the notion of place and transforms the relationship between the perpetrator of a crime and its victim. In effect, in cyberspace, a physical person residing in one place in the real world may commit an unlawful act that targets one or more victims located in entirely different geographical locations. In terms of investigations and legal proceedings, this means that several jurisdictions are de facto implicated, a reality which demands multi-faceted coordination to ensure an effective response, including: 1) cooperation between their respective law enforcement agencies and justice systems; and 2) the harmonization of their respective legal

frameworks (Grabosky, 2004).

In light of this urgent situation, international institutions have a fundamental role to play in developing commonly accepted definitions to buttress and facilitate the development of national frameworks as well as an appropriate international response. According to the United Nations Office on Drugs and Crime (UNODC), the notion of cybercrime lumps together a jumble of disparate acts more than it describes a specific category of offences. In practice, public agencies base their policy actions on one of two major approaches: 1) a restrictive object-centred definition (i.e., criminal acts targeting computers and their contents) or 2) an inclusive definition focused on modus operandi (i.e., criminal acts involving, in whole or in part, the utilization of online electronic devices). In its 2013 report, the UNODC recommended, in relation to the fight against cybercrime, the adoption of an inclusive definition to facilitate the adapting of legislative and legal frameworks to the rapid technological evolution characteristic of this phenomenon (UNODC, 2013). We will address this issue in depth in the next chapter. The task at hand in this chapter is to focus on the question of data, another major dimension of cybercrime-related issues.

Measuring cybercrime: a "mission impossible"?

The first difficulty in measuring cybercrime is two-fold: first of all, cyberspace is composed of activities and actors interconnected in a hyper-complex system, which is impossible to measure objectively; secondly, cybercrime activity is often difficult to detect, even by its victims (Cobb, 2015).

The second difficulty in measuring cybercrime arises from the nature of governance in cyberspace, which is multi-polar, atomized and largely unstructured. There are a number of major implications to this governance model: 1) private actors predominate in the production of data on cybercrime; 2) public sector bodies play a peripheral role in the collection and production of such data; and 3) the scale, presumably vast but unknown, of grey data and unreported events.

In general, there are two mains sources of data available for assessing global trends. The first source is comprised of private sector actors, mainly large companies and consulting firms active in the field of cybersecurity (e.g., Norton, Symantec, PwC, Ponemon, McAfee, et al). Their data focuses on: 1) the issues encountered by their target market, in particular the business community; and 2) the specific types of crime which their cybersecurity services are meant to counter, such as data theft, various types of hacking and intrusions, and fraud. However, a number of authors raise doubts regarding the accuracy of the data collected by major cybersecurity firms and the transparency of the motivations behind the production of their reports (Levi, 2017). The second category of sources includes agencies which may be governmental (e.g., the FBI), multi-governmental (e.g., Europol) or international (e.g., the UNODC). These studies generally target specific geographic regions and are fewer in number. Nevertheless, they are invaluable because they cover a broader range of criminal activities, including sexual exploitation, cyberviolence, organized crime and cyber-terrorism. It's interesting to note that both categories of studies accord increasing importance to victimization surveys and surveys on usages and users' feeling of security in cyberspace.

The principal issue encountered in measuring cybercrime is that it is massively under-reported and under-counted. Dark figures are predominant, i.e., the vast majority of unlawful and criminal acts committed in cyberspace are never recorded or counted (Yar, 2006). As Freyssinet emphasizes,

> "no reliable statistical study presently exists which can measure the scope of cybercriminal phenomena, whether this is due to definitional issues (…) or to the low propensity of victims to file complaints (…) Therefore, should official statistics rise in the future (…) it would be incorrect to attribute this to a significant increase in the number of such events, rather than to advances in the collective quantification of these problems." (Freyssinet, 2010, p. 28)

In addition, a number of obstacles exist regarding the reporting of cybercrimes, especially to government institutions. In particular, the question of data theft – often involving the massive quantities of personal information that private sector actors gather on the users of their services – constitutes a thorny issue in terms of cybercrime reporting. In part, this is because the collection of such data, along with the responsibilities of businesses regarding the attendant security issues, remains subject to little regulatory oversight. As a result, businesses tend not to divulge information on cyberattacks, in part to protect their reputations, but also to guard against any legal proceedings which may be brought by clients indirectly prejudiced by the theft of their data (Pereira, 2016). In this context, it is currently very difficult to assess trends regarding these crimes. In effect, it is estimated that 80 to 90% of the hacks resulting in data theft are never reported (Medina & Molist, 2017).

To date, only a few countries have adopted legislation making it a statutory requirement for private actors to report incidents in which they've been the victims of hacking or data theft. The United States and the European Union have adopted laws stipulating the mandatory reporting of incidents of this type to individuals whose data is vulnerable and may have been compromised. In Canada, this type of obligation should enter into effect during 2018 (Connolly, 2018).

As for other types of cybercrime, notably those targeting individual users (such as phishing[9] and ransomware[10] type frauds), mechanisms to facilitate reporting by individuals, such as hotlines or online mechanisms, do not exist or are insufficient. Moreover, the lack of consensus on which acts constitute cybercrime also leads to confusion in terms of the classification and measurement of reported offences. In effect, each country has its own definitions and classification systems. Furthermore, in any given country, cybercrimes may often be recorded as "traditional" offences such as fraud (UNODC, 2013).

In addition to measuring the number of incidents and the recourse to victimization surveys, there is another approach to measuring cybercrime that consists of attempting to assess its economic cost. The principal advantage to this approach lies in its capacity to track the real world impact of such activities, albeit only in rough orders of magnitude. Alas, the methodological and operational difficulties of this type of measurement exercise are such that, currently, it seems impossible to rely on such assessments (Gañán, Ciere, & van Eeten, 2017). In effect, due to the hypercomplexity of cybercrime activities and their economic impacts, this approach is beset by a number of limitations in terms of: 1) the identification and delimitation of the effects to be measured (e.g., whether to include security related costs); 2) reliable data collection; and 3) methods of analysis. A recent study conducted by a RAND Corporation research team demonstrated that the wide variations in these types of estimates reflect differences in methodology (Dreyer et al., 2018). In 2014, the Centre for Strategic and International Studies estimated the total cost of cybercrime as somewhere between 375 and 575 billion dollars (Center for Strategic and International Studies, 2014). As for Microsoft, it advanced the figure of 500 billion dollars in 2017 and the cybersecurity firm McAfee followed suit with an estimate of 600 billion dollars for 2018 (Chalfant, 2018).

An attempt at a categorization of trends in cybercrime

Annual trends in cybercrime are first and foremost identified and disseminated by the major cybersecurity firms, which produce reports primarily concerned with the unlawful activities affecting the private sector. These reports largely focus on the trends in cybercrime technologies and modus operandi. The unlawful activities that increased in 2017, and which will likely continue to increase in 2018, included hacking techniques (targeting devices, data and accounts), malicious software, ransomware, various types of fraud and identity theft, as well as, particularly since 2017-2018, the boom in fake news and microtargeting (Deutsche Telekom, 2017).

Norton's 2017 annual survey corroborated the prevalence of similar trends among individual users. In effect, among the 44% of its individual clients who reported having been victimized by cybercrime in the preceding year, the most frequently reported criminal and unlawful activities were, in order of importance: a virus infection of an online device (53%), banking fraud (38%), a hacked account (34%), business fraud (33%) and email fraud (32%), including phishing and virus infections caused by spam (Norton - Symantec, 2017).

As for the technological trends in cybercrime, three categories of activities stand out: 1) malicious software, which particularly affects connected devices; 2) phishing attacks, especially for the purposes of identity theft; and 3) attacks on data accessibility, by means of distributed denial of service attacks (DDoS) or ransomware (Medina & Molist, 2017).

The boom in mobile telephone use has spawned a corresponding boom in cybercrimes targeting smartphones. This has a particular impact on emerging countries where this mode of communication is an essential vector of development. The emerging world is also particularly affected by other forms of cybercrime, especially fraud. Thus, the three countries most victimized by phishing are China, Brazil and Algeria (Forcepoint, 2016). Symantec reports a rapid growth in cybercrime activities targeting mobile telephones. Thus, between 2015 and 2016, there was a 105% increase in viruses identified as having been specifically developed for smartphones (Norton - Symantec, 2016).

It's worth noting that in economically developed countries there exists a correlation between the decrease observed in "traditional" crimes, especially property crimes, and the growth in online crime. Although links of causality have yet to be clearly established, this correlation suggests that the growth in cybercrime may be connected, at least in part, to a shift in criminal activities from the real world towards cyberspace (Weulen Kranenbarg, Holt, & van Gelder, 2017)

It's interesting to note that this type of criminal activities may be measured in two different ways. One option is to observe the number of specific types of a given technology (e.g., ransomeware), identified over a period of time by a cybersecurity firm (this number is easily determined as it is published in the different cybersecurity reports mentioned above). Another possibility is to measure their intensity or frequency of use, which may vary considerably. For example, in the case of ransomware, a stabilization was observed in their number (at least among those detected), as well as in the number of ransomeware families, between 2015 and 2016. On the other hand, estimates of the number of ransomware attacks blocked showed a large increase from 0.4 million in 2015 to 1.6 million in 2016 and 3 million in 2017 (Symantec, 2018). This shows that whereas this technology has apparently stabilized, the intensity of this type of activity is increasing.

A second category of trends concerns activities directed against persons, such as cyberviolence, cyberstalking and hate speech. Although these offences also exist in the real world, they acquired a very different scope, form and consequences in cyberspace (an issue addressed in Chapter 3). Online interactions are characterized by anonymity and depersonalization. This has contributed to a notable disinhibition regarding violent behaviour in cyberspace (Zweig, Dank, Lachman, & Yahner, 2013).

The groups victimized in cyberspace by these types of violence reflect the diversity of those victimized in the physical world and include, notably, women and sexual, ethnic and religious minorities in general (Peterson & Densley, 2017). Two groups are particularly affected by cyberviolence. In effect, cyberspace is a particularly propitious terrain for violence against women and girls (Pasricha, 2016). Among adolescents, cyberstalking and cy-

berviolence, including in dating contexts, are rife on social media, which, today, constitute "a new vector for violence among youth" (Patton et al., 2014).

Cyberviolence can take different forms. Moreover, particular expressions may reflect specific geographical, social and cultural contexts. In general, cyberviolence in non-Western countries has not been sufficiently studied. That said, there are several noteworthy exceptions. In India, for example, many studies have been published on the subject in recent years, particularly regarding violence against women in cyberspace (Halder & Jaishankar, 2016; Jaishankar & Halder, 2011; Pasricha, 2016). Deplorably, there has been very limited scientific research on the prevalence or etiology of the different forms of cyberviolence (Diamond & Bachman, 2015). Nevertheless, several forms of cyberviolence are the subject of a burgeoning literature, including, notably, the issue of adolescents and cyberstalking, the infiltration of gangs in social networks, the strong presence of hate groups, and terrorist propaganda and recruitment (Peterson & Densley, 2017).

Furthermore, legal frameworks and penal codes differ greatly from country to country in terms of how they address this type of activities (UNODC, 2013). This constitutes a major obstacle to the production of harmonized data at the international level. Finally, these types of violence are rarely reported, as attests a study conducted in the United States by the Pew Research Center. According to the results of this survey, 41% of adult respondents had experienced online bullying, but only 48% of these victims took an action in response, such as reporting the offence to the content platform, adjusting their browser settings or modifying their usage (Pew Research Center, 2014).

Who are the perpetrators? Who are the victims?

Upon considering the issue of who commits unlawful, criminal or deviant acts in cyberspace, a certain reality becomes readily apparent: no advanced skills or technological know-how are required today to commit many of these criminal acts (UNODC, 2013). In effect, any individual with an internet connection can engage in criminal or unlawful activity. The range of possibilities is vast. There are of course major inherent constraints to any exercise in measuring cybercrime activities. That said, in 2013, the UNODC estimated that 80% of cybercrime actions were connected, in one way or another, to a form of organized crime (UNODC, 2013). In effect, cyberspace has been infiltrated by different forms of organized crime, due either to a shift in their activities towards the online universe or to the emergence of new opportunities in cyberspace.

Who, then, are the victims of cybercrime? The usual answer is that any user of a connected device is a potential victim. However, in light of the multiplicity of crimes and modus operandi found in cyberspace, it's simply not possible to identify a standard profile of the cyber victim. That said, it is worth highlighting certain characteristics.

In its annual survey, Norton estimated that 978 million individuals, out of a total internaut population of 1.8 billion, were victims of some form of cybercrime in 2017, the most common forms being virus infections, bank fraud, hacked email or social media accounts, commercial fraud or phishing (Norton - Symantec, 2017). It's worth stressing that, although an important technological vector is present in the majority of these criminal activities, human error is also a key determinant. In effect, according to the latest statistics of the European Network and Information Security Agency (ENISA), 90 to 95% of the fully completed cyber-attacks in the world were enabled by successful phishing (European Union Agency For Network and Information Security, 2018). According to the same survey, users retain a high degree of confidence (between 76 and 82%) in the capacity of the private sector to securely manage their personal information. At the same time, over 41% affirm that they are less confident than before in their government's capacity to manage this same responsibility.

The Global Economic Crime Survey, a report produced by Pricewaterhouse Coopers, consists of a worldwide survey conducted in the private sector. The latest edition indicated that cybercrime has become the second most frequently reported economic crime by businesses, following an 8 percent increase between 2014 and 2016. It is, in effect, a growing concern for the private sector. It's interesting to note, however, that only 37% of the businesses surveyed had prepared a cybercrime response plan. Half of the respondents questioned the capacity of government authorities to cope with the cybercrime incidents affecting them (PwC, 2016). In the private sector, vulnerability to cybercrime is primarily an issue affecting small and medium-sized enterprises (Ponemon Institute LLC, 2016). For example, small and medium-sized businesses constitute the principal target of so-called BEC scams (Business Email Compromise), an adaptation for the private sector of the notorious Nigerian[11] scam, as they account for 38% of the total number of businesses targeted (Symantec, 2016).

If one considers all unlawful activities committed in cyberspace, cybervictimization rates exceed those of so-called "traditional crimes" (UNODC, 2013). This observation is corroborated by the different cybersecurity reports, which describe rapidly increasing levels of crime and victimization (International Telecommunication Union, 2017a; Norton - Symantec, 2016, 2017; Ponemon Institute, 2017; PwC, 2016, 2018; RSA, 2016; Symantec, 2018). Nevertheless, it's important to nuance this conclusion, particularly as cybercrime encompasses activities such as virus infections or attempted email scams, i.e., very common incidents which, in most cases, are dealt with by standard IT protection systems or by the user's exercise of his own good judgment.

A systematic review of cybervictimization surveys in Europe indicates that the volume of serious offences and crimes committed in cyberspace is far less than the volume of "cybercrime" taken as a homogeneous mass encompassing all incivilities, offences and crimes, without distinction. Thus, it appears that only 0.6 to 3.5% of users reported that they were victims of online commercial fraud, 0.4 to 2.2% in the case of banking fraud and 0.4% for

other types of fraud (including "lonely heart" and advance fee scams), 3% were victims of the most serious forms of cyberharassment, and 1.3 to 5.8% were victims of hacking (Reep-van der Berg & Junger, 2018).

Another interesting finding in terms of understanding cybervictimization phenomena is that revictimization rates vary enormously depending on the type of cybercrime. For example, a victimization survey conducted in England and Wales by the Office of National Statistics and the Home Office indicated that on average, only 16% of fraud victims were subsequently revictimized (Levi, 2017). In contrast, the victims of revenge porn[12] experience a process of repeated revictimization affecting every sphere of their lives (Bates, 2015). Finally, as mentioned above, cybervictimization rates are higher in less developed countries (UNODC, 2013), as well as among the most frequent and knowledgeable users of cyberspace.

Nevertheless, all of these major trends must be seen through the prism of our limited knowledge and our inability to measure, even in rough orders of magnitude, the scope of cybercrime phenomena. In this regard, Jardine (2015), in the exercise of normalizing several absolute measurements of cybercriminal acts, clearly demonstrated the skewed readings of reality often induced by statistical trends. Jardine identified several factors that render problematic the meaning and reliability of these statistics : 1) the complexity of cyberspace and its actors renders it very difficult to measure internet phenomena and, thereby, establish quantifiable benchmarks for normalization purposes; 2) cyberspace's rapid qualitative and quantitative evolution, which is intrinsic, renders any non-normalized trend absolutely illegible over time; and 3) the absence of a reliable and standardized system of cybercrime data collection, which means that studies must rely on very mediocre and unrepresentative data. Jardine analyzed and normalized 13 trends. These normalizations produced the following results: 6 normalizations indicated an improvement in the situation despite trends indicating a deterioration; 6 showed a greater improvement in the situation than that indicated by the absolute (non-normalized) trends; and only one normalization confirmed the trend initially indicated by the absolute measurements.

The spatial distribution of cybercrime

A geographical analysis of cybercrime represents a very challenging enterprise, as: 1) trends evolve rapidly; 2) cybercriminal activities are highly diverse; and 3) their geographic allocation varies depending on the type of crime considered. With that caveat in mind, let's now consider, for the purposes of establishing rough estimates, Symantec's proposed annual ranking of the countries that "produce" the most cybercrime activity. In 2016, the top ten in terms of the volume of global cybercrime activity were: the United States (23.96%), China (9.63%), Brazil (5.84%), India (5.11%), Germany (3.35%), Russia (3.07%), the UK (2.61%), France (2.35%), Japan (2.25%) and Vietnam (2.16%), (Symantec, 2018). It should be noted that this evaluation focused on a small number of activities and that the methodologies underlying this type of study include too many limitations to be considered absolutely reliable. In any event, it's important to underline the strong correlation between the countries which produce the most cybercrime and those counting the most victims. In 2015, the Red24 risk management consultancy produced a report identifying the countries most affected by cybercrime (the United States, Russia, China, Hong Kong, India, Brazil, the UK, the Netherlands, Germany and Norway) and those from whence the most cyberattacks originate (Russia, China, Eastern Europe, Romania, Brazil, Nigeria, Vietnam, Indonesia, South Korea and the United States). Evidently, the countries that produce the most cybercrime are also the ones that suffer the most damage (Red24, 2015).

The spatial distribution of cybercrime can be measured in two ways: it can be based on the physical localization of the perpetrator or, alternatively, that of the victim (Kigerl, 2012). Depending on the nature of the unlawful activity, either of these approaches may be more relevant. Thus, for activities such as phishing, spamming or the usage of botnets[13], the country of origin is more useful. On the other hand, for acts of cyberviolence it may be more pertinent to measure the spatial distribution of victims.

Moreover, the spatial distribution of perpetrators, victims and the different types of unlawful activities is very closely connected with the digital divides and inequalities characterizing cyberspace, which we discussed at the beginning of this chapter. In this light, Alex Kigerl (2016) proposes an interesting typology of what he calls "cybercrime countries." Based on data per country, in particular the data provided in the reports of the major international cybersecurity firms, Kigerl classified countries as a function of: 1) the crime rates for certain types of cybercrime; 2) their characteristic types of cybercrime; and 3) macro factors such as per capita income. This exercise produced 4 main categories of countries.

- **Category 1** includes "low cybercrime countries" and is essentially comprised of the nations most affected by the digital divide, notably in terms of access to cyberspace. This cluster is largely comprised of less developed countries.
- **Category 2** includes "advance fee fraud countries." This category includes a very heterogeneous set of countries (such as Iceland and Nigeria) where cybercriminal activity centres around the least sophisticated frauds, technologically speaking. Kigerl's analysis focuses on the non-technological aspects of these crimes, which enable individuals with limited skills to engage in highly remunerative criminal activities (e.g., the celebrated so-called Nigerian 419 scam, analyzed in chapter 3).
- **Category 3** includes the countries characterized by non-serious forms of cybercrime, such as non-fraudulent or infected spam, software piracy or infringements on intellectual property. This group is comprised of the most economically developed and wired countries (i.e., those on the "right side" of the digital divides).

- **Category 4** is comprised of the "phishing scam" countries, a group that actually includes 40% of all countries studied, and which is characterized by major cybercriminal activity in every category, especially fraud (levels are equivalent to those of category 2 re advance fee scams), infected and fraudulent email, and phishing.

What makes this study particularly interesting is that it represented an attempt to construct a preliminary framework for assessing correlations between macro-factors and cybercriminal activities.

In the following sections, we provide an overview of the specific dynamics and key issues in each of the world's major regions. It's important to bear in mind the highly disparate nature of the available information on this subject. This absence of harmonized data is a major obstacle to comparisons between different regions.

a) Africa

In Africa, conditions are particularly favourable to the development of a dynamic cybercriminal sector. In effect, information and communication technologies are rapidly expanding, technological infrastructures are weak, legal frameworks inadequate and capacities in the area of national security deficient (Mark Shaw, 2018). Finally, it's important to underscore the crucial lack of data on cybercriminal phenomena in Africa.

In 2014, the United Nations Economic Commission for Africa observed that cybercrime activities were expanding more rapidly in Africa than elsewhere (United Nations Economic Commission for Africa, 2014). Nevertheless, Africa still accounts for a minor share of global cybercrime activity: in terms of malicious activities (cyberattacks, malwares, email scams, phishing, bots and command and control centres), less than 3% of the total volume worldwide originates in Africa (Symantec, 2016). Cyberscams remain a very common problem in Africa: 55% of the world's BEC type emails, for example, originate in Nigeria or South Africa (Symantec, 2016). Moreover, African cyberfraud is evidently undergoing a process of complexification, as attests a trend towards more elaborate fraud scenarios, which mainly target businesses (Trend Micro & Interpol, 2017).

Software piracy is another source of cybercrime in both Africa and the Middle East. It's worth noting that pirated copies account for 57% of the software utilized in these two regions vs. the world average of 38% (Business Software Alliance, 2016). Pirated copies of software, which constitute ideal vectors for malware, account for a very large proportion of the continent's IT infrastructure, particularly in its most dynamic economies (84% in Algeria, 81% in the Ivory Coast, 78% in Kenya and Senegal, 74% in Tunisia and 66% in Morocco) (Business Software Alliance, 2012).

South Africa, Nigeria and North Africa stand out as cybercrime hotspots compared with other African countries. In general, it's evident that the prevalence of cybercriminal activity in a given African country corresponds to its rate of internet penetration, which in turn is a function of its level of economic development. Africans themselves are particularly victimized by cybercrime. In South Africa, 67% of the adult respondents participating in Norton's 2016 annual survey reported that they were victimized by cybercrime, during the preceding year, vs. the global average of 48% (Norton - Symantec, 2016).

In 2013, 47% of South African smartphone users reported they had been the victims of some form of cybercrime activity targeting their mobile device (Norton - Symantec, 2013). This is a major problem, as it is in Africa where smartphone use for making money transfers is the most common (Symantec, 2016). Furthermore, according to estimates the number of mobile phone users should continue to increase rapidly in Africa, with the number of users projected to reach 504 million in 2020, compared to 301 million in 2013 (GSMA, 2015). Thus, individuals, businesses and, more broadly, Africa's economies are very significantly affected by cybercrime, which costs, for example, nearly $500 million per annum in Nigeria, the continent's largest economy with a GDP of $521.8 billion (Shiloh & Fassassi, 2017).

b) Latin America

In Latin America organized crime has moved into cyberspace on a massive scale, whether it's to develop new sectors, such as online fraud, or to facilitate its traditional activities, particularly in support of various types of illicit trafficking and money laundering (Clavel, 2016). Indeed, the organizational and operational strength of organized crime in Latin America, in conjunction with the weakness and vulnerability of regional infrastructure and IT security, is such that it is producing a highly critical situation where criminal organizations dispose of technical means and skills equal or superior to those of governments and security agencies (Observatorio de la ciberseguridad en América latina y el Caribe, 2016). At the end of the day, the fight against cybercrime in Latin America is intrinsically linked to the fight against organized crime (Trend Micro - Organization of American States, 2013).

In recent years, Brazil has become an international cybercrime hotspot "at the epicenter of a global cybercrime wave," in terms of both perpetrators and victims (Muggah & Thompson, 2015). In 2015, Brazil was the second most affected country globally in terms of malicious software and fraud targeting banking transactions (Kaspersky, 2015). Brazil's Computer Emergency Response Team (CERT) recorded a 197% increase in the number of reported cybercrime incidents during 2014, 40% of which concerned attempted fraud (Diario do Comercio, 2015).

According to Brazil's Department of Security (Departamento de Segurança), Brazilian small and medium-sized businesses are the principal targets of these activities (65% are so affected vs. 30.8% for big companies), notably due to their lower levels of security (Folha de S. Paolo, 2015). Furthermore, Brazil ranks first

in the world in terms of infections of mobile telephones by malicious software. Mexico, which is second place in Latin America, ranks 4th worldwide in this regard. These rankings are an indication of the particularly high degree of vulnerability found in emerging countries (Malwarebytes, 2017).

In effect, a specific cybercriminal milieu has developed in Brazil, which operates less in the Deep Web[14] than in open cyberspace, through platforms such as conventional social media. Populated by particularly young cybercriminals, this Brazilian milieu has crystallized around fraud and malicious software targeting the banking sector (Trend Micro, 2015).

c) The Asia-Pacific region

In Asia, cyberspace is expanding very rapidly. As are, in turn, cybercriminal activities. In effect, with the most dynamic economic growth rates in the world and the most rapidly increasing internet penetration rates, Asian internauts accounted for 55% of users worldwide in 2016, according to World Internet Statistics. Nevertheless, the situation in Asia is far from uniform, notably in terms of absolute numbers of users, penetration rates and levels of economic development. One notes, for example, that China and India alone account for over half of the web users in Asia. Penetration rates vary greatly between the most wired countries, such as Japan, South Korea, Australia, New Zealand or Taiwan, and countries whose levels of development and large marginalized rural populations slow the pace of internet penetration, such as India, Pakistan or the countries in Indochina (Broadhurst & Chang, 2013).

It is foreseeable that the magnitude of cybercriminal activities committed against both the private sector and individuals will parallel and exploit this growth. It has been estimated that Asian organizations, public and private, face an 80% higher risk of cyberattacks than other victims (Oliver Wyman, 2017). Moreover, according to the cybersecurity firm LogRh ythm, for Asian businesses this is a growing threat. In effect, its latest surveys indicate that in 2016 90% of Asian businesses were the victims of some form of cybercrime, vs. 76% in 2015 and 66% the year before (Lewis, Weinland, & Peel, 2016). In 2017, the firm ESET estimated that 54% of its small and medium-sized business clients (located in Singapore, Hong Kong, India, Thailand and Japan) had been the victims of data hacking in the previous three years. India (73%) and Hong Kong (61%) were the most affected, and Japan the least (29%). In addition, the same survey showed that the risk of an attack is correlated with the size of the business: 70% of the largest companies in the category were the victims of hacking vs. 37% of the smallest businesses (ESET, 2017).

Emerging Asian countries such as Vietnam or Malaysia are playing an increasingly important role in the cybercriminal scene, both as the place of origin and as the target of such activities (Chang, 2017). There are a number of reasons for this development, including: 1) the emergence of their connectivity in cyberspace; 2) their rates of economic growth; and 3) regional geopolitical issues such as the tensions in the South China Sea (Boudreau & Chau, 2016).

d) The United States, China, Russia and the disappearance of the distinctions between cybercrime and cyberwar

Although our work does not focus per se on the multiple geopolitical dimensions of cyberspace, it's important to identify several countries where cybercrime is intrinsically linked with questions of national security, most notably the United States, China and Russia. In effect, these three countries share a number of characteristics: 1) they are IT powerhouses which have entered cyberspace as a strategic geopolitical sphere and developed particularly sophisticated offensive and defensive capabilities; 2) they are hotbeds of cybercrime where much of the world's cybercriminal activity has taken root; and 3) they are primary targets of cybercrime, whether such activity is directed against their governmental institutions, private sectors or citizens. It's interesting to note that the conceptions crystallizing around these questions have revived the geopolitical schema of the Cold War era. Thus, in its report on cyber-attacks, the research team at FireEye identified 4 blocs: Asia, the former Soviet bloc, the Middle East and the United States (Geers, Kindlund, Moran, & Rachwald, 2017).

In the United States, cybercriminal activities are widely considered a geopolitical threat, whether they target the private sector or the public sector, and regardless of their motivations. In 2017, James Comey, then Director of the FBI, clearly expressed this conflation by stating that "there are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese" (Cook, 2014, p. 1). The IC3 has corroborated this rising trend in criminal activities targeting the private sector in the U.S.: its records indicate an 11% increase in complaints in just two years (between 2014 and 2016) and an increase in declared losses from $80,000 to $1.33 million (Insurance Information Institute, 2017).

The United States is an absolutely essential actor in the global cybercrime landscape in three principal respects: 1) in terms of the volume of cybercrime, 2) in terms of victimization; and 3) in terms of the responses thereto. First of all, individual American victims accounted for 143 million of the 978 million victims counted by Norton in its latest report, and suffered $19.4 billion of the total estimated losses of $172 billion (Norton - Symantec, 2017). Furthermore, data theft is a rapidly growing issue for American companies: between 2016 and 2017, the Identity Theft Resource Center recorded a 44.7% increase in the number of reported identity thefts (Insurance Information Institute, 2017). Thanks to the statutory obligation imposed on private actors to declare these types of incidents, we have a more reliable image of the situation in the U.S. The principal types of cybercrime reported by the IC3 (the Internet Complaint Center, the FBI's internet complaint desk) are as follows: various types of fraud, theft of personal data, fraudulent emails, cyberbullying and threats

(Federal Bureau of Investigation - Internet Crime Complaint Center, 2016). According to the same report, the most significant financial losses incurred were due to different types of fraud and the theft of personal data.

Cyberspace has emerged as a new strategic priority for post-Soviet Russia, which has developed a particularly sophisticated system of convergence and collaboration between cybercriminal circles and the government. In recent years, the Russian cybercriminal milieu has undergone a major process of restructuring, consolidation and expansion (Stoyanov, 2015). This sector benefits, moreover, from considerable complacency on the part of the national authorities (Cybersecurity Intelligence, 2015). According to estimates, Russia accounts today for about 35% of total cybercrime revenues (Lewins, 2017). Highly specialized and technologically very advanced, the Russian cybercriminal milieu has demonstrated great effectiveness in its two priorities: generating profits for cybercriminals and advancing Russian strategic interests (Galeotti, 2011).

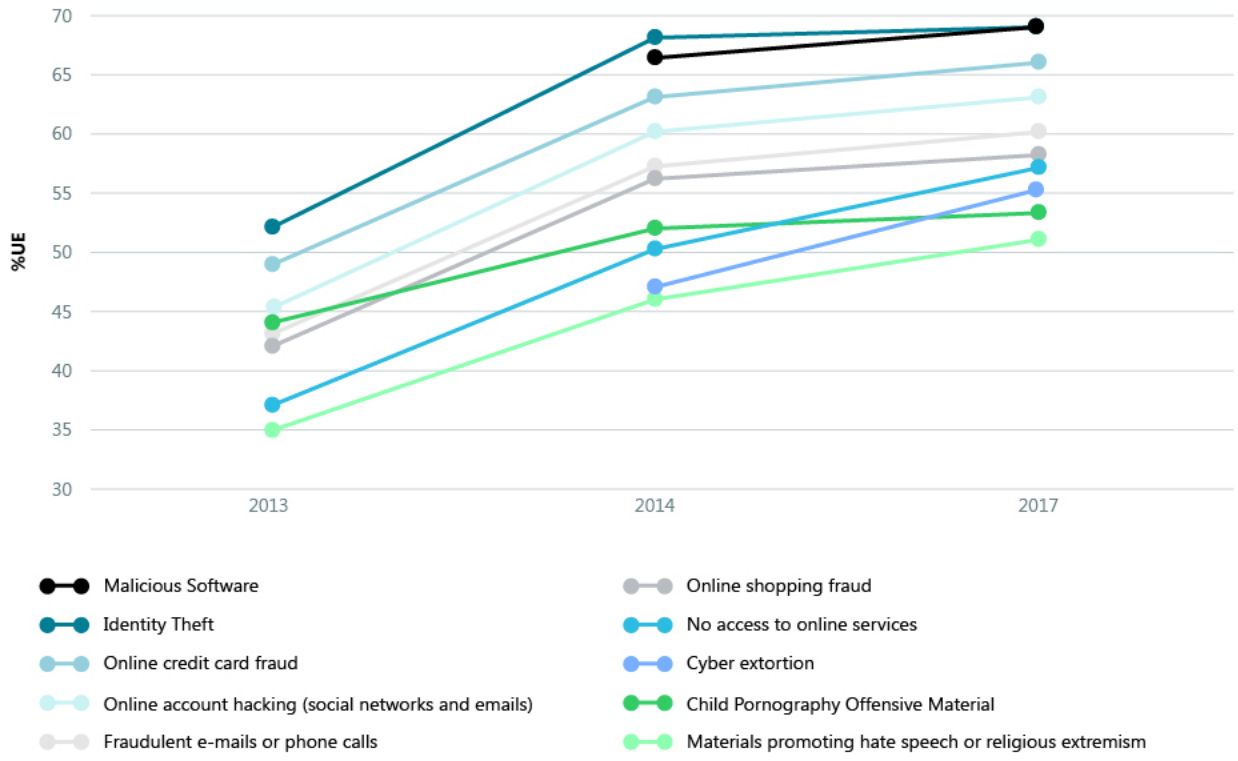
Finally, in the Asian context, China constitutes a focal point of cybercrime, both as the place of origin of illicit activities and in terms of victimization (Microsoft, 2017). In effect, Chinese internauts and enterprises are particularly vulnerable and victimization rates are high, notably in the country's most developed provinces where incomes and internet penetration rates are higher than in the rest of the country (Cheng, 2017).

This category of country, which considers cyberspace a strategic terrain for power projection, is not limited to the three nations mentioned above. Other countries, notably North Korea and Iran, also stand out as places with favourable conditions for the emergence of a vibrant cybercriminal milieu, i.e., access to skills, limited repression and complacency on the part of the authorities (McAfee, 2018).

e) Western Europe and Canada

In Europe, particularly in the countries of the European Union, better information exists and is readily available. This situation is due to: 1) the existence of reporting mechanisms and the statutory obligation to report cybercrimes; 2) Europol's commitment to fighting cybercrime and its efforts in terms of analysis and knowledge production; and 3) the existence of solid Eurobarometer surveys on usages, the feeling of insecurity and victimization in cyberspace. The most recent Eurobarometers on cybercrime were carried out in 2013, 2014 and 2017.

Figure2.4. **Trends in risk perception among European users concerning ten types of cybercrime**



Source: Eurobarometer (2017)

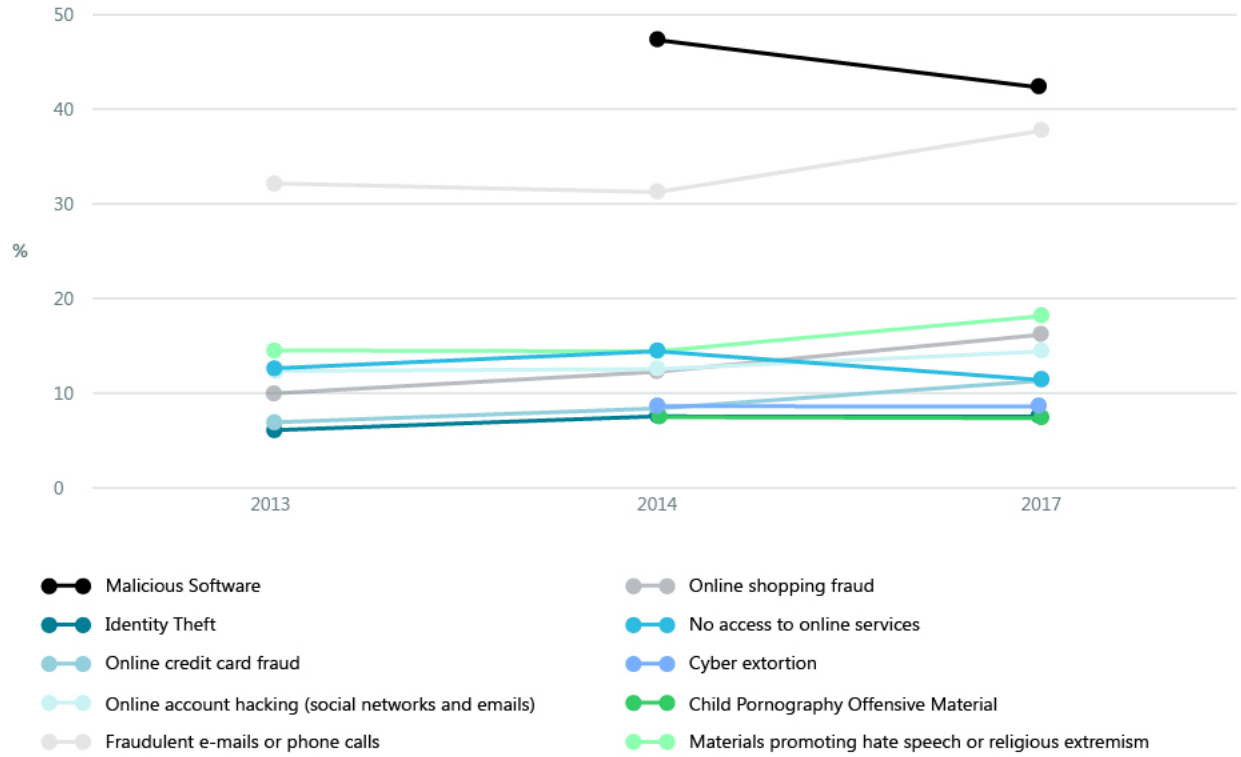
Concerns over the possibility of victimization in cyberspace have very markedly increased since 2013, particularly regarding fraud and identity theft. It's quite interesting that the biggest increase (approximately 15%) was observed between 2013 and 2014. Subsequently, the level of concern stabilized between 2014 and 2017 (with annual increases on the order of 2-3%). The largest increases in concern between 2014 and 2017 were in relation to crimes that received major media coverage during the same period: ransomware (up 8%) and attacks targeting online banking services (up 7%). It's interesting to note that hate crimes and the promotion of terrorism on the internet are subjects of steadily increasing concern: 35% in 2013, 46% in 2014 and 51% in 2017.

The Eurobarometer's survey data on victimization rates is particularly interesting in that it indicates a low to moderate prevalence and increase in the most frequent crimes such as commercial or banking fraud, phishing, the hacking of accounts, ransomware and identity theft. This data is particularly interesting when compared with the levels of concern mentioned above inasmuch as they clearly indicate that although European internauts' feelings of concern regarding their online security have greatly increased over the last five years, the prevalence and growth of these crimes remains low. This phenomenon is discussed in Chapter 1 in the context of our analysis of the public's feelings of insecurity.

Finally, the three consecutive surveys indicate that internauts primarily turn to the police when victimized by a cybercrime, particularly in cases of identity theft, blackmail or ransom demands, sex crimes or bank fraud. Private actors, such as the relevant internet site, online merchant or internet provider, may also be contacted, notably in cases of commercial fraud, fraudulent software or hacking (Eurobarometer, 2017).

In Canada, police data confirm the existence of a rising trend in cybercrime, as the number of reported incidents has increased 45% since 2014. Moreover, over half of small and medium-sized enterprises have been victimized by cybercrime activities (McAfee, 2018). According to the Canadian Chamber of Commerce (2017): "Cybercrime extracts 15-20% of the $3 trillion global internet economy, and Canada loses 0.17% of GDP to cybercrime, which is equal to $3.12 billion/year" (Canadian Chamber of Commerce, 2017). In 2017, a Canadian business faced, on average, nearly 10 cyber-attacks, 20% of which compromised highly strategic information (Scalar, 2018). However, it's interesting to note that the so-called Generation M, composed of persons under 35, seems less likely to be victimized by illegal activities on the internet, with a victimization rate of 42% vs. the global victimization rate of 60% and that of 69% in the United States (Norton - Symantec, 2017).

Figure 2.5. **Trends in the victimization rates of European users for ten types of cybercrime**



Source: Eurobarometer (2017)

Conclusion: What are the main issues in cybercrime prevention?

What conclusions should one draw from this chapter? First of all, cybercrime is not a simple undifferentiated phenomenon. It encompasses a heterogeneous set of unlawful activities committed in cyberspace. Consequently, it's very difficult to draw any conclusions whatsoever, given the diverse and heteroclite nature of the issues, actors, and dynamics in play. Next, it should be emphasized that, from the vantage point of prevention, this incoherent jumble cannot be conceived of in terms of a clearly defined object amenable to specific actions. In effect, we know little or nothing about the processes and factors underlying cybercriminal activities – a rather thorny and fundamental question, which is the subject of the next chapter. Furthermore, it's very difficult to make reliable and accurate measurements and estimates of the various different cybercrime activities and their consequences. Finally, the principal public and private actors see the challenges posed by cyberspace from a security-oriented perspective (as do users, for that matter), rather than from the vantage point of prevention. This a matter we will discuss in depth in cChapters 4 and 5.

In closing, let's nevertheless return to a key aspect which, in our view, must constitute a foundational consideration in relation to cybercrime prevention policy and practices: the question of collective and individual liberties, as well as privacy issues, vs. the need to redefine the legal and institutional frameworks regulating these matters in the age of cyberspace and mass surveillance.

In their landmark book, Singer and Friedman (Singer & Friedman, 2014) underline the fact that, over the last decade, governments have favoured a security-centric conception of cyberspace. According to these authors, cybersecurity is now the priority which guides relations between governments and private actors in cyberspace, as the former work to develop the institutional and legislative tools required to compel the latter to collaborate in their efforts (re surveys, legal procedures, surveillance and control). In relation to cybercrime, this conception views cyberspace as "ungovernable, unknowable, a cause of vulnerability, inevitably threatening, and a home to threatening actors," to whom it confers many advantages (David Barnard-Wills & Debi Ashenden, 2012, p. 116).

One of the principal issues in the fight against cybercrime today resides in the challenge of redefining the balance between individual liberties and the right to privacy, on the one hand, and the requirements of security and surveillance on the other. At the heart of this issue, two key questions are a matter of considerable debate. First, regarding personal data, to what extent should the authorities have access to such data when it is collected by private third parties? Second, what are the appropriate legal and regulatory frameworks for encryption techniques?

This security-oriented perspective is inseparable from the present context, in which three phenomena with major cyber related implications cast long shadows: terrorism, "hacktivism" and cyberwars. This perspective is also very much a reflection of a certain lack of knowledge concerning cyberspace and its dynamics, often remarked among government decision-makers and legislators.

In Chapter 4, our analysis leads us to examine an approach that is universally favoured today in the face of cybercrime issues, i.e., risk management (as opposed to crime prevention-based approaches). Wanda Capeller underscores the shift from a risk society – the term developed by sociologist Ulrich Beck in 1986, in the wake of the Chernobyl nuclear disaster – to a virtual risk society. This approach has decisive implications in terms of how public, private and individual decision-makers act in response to cybercrime. In particular, risk management implies that the response and responsibility for action essentially falls to the potential victim. It is thus incumbent on individual users and businesses to take measures to protect themselves. This is diametrically opposed to a comprehensive vision of crime prevention.

This absolutely fundamental difference is not without a number of major implications. First of all, regarding offenders, prevention efforts no longer focus on the need to comprehend and mitigate the social, environmental and personal factors underlying the development of criminal life paths and the commission of deviant and unlawful acts. For victims, notably those from the most vulnerable groups such as children, women or sexual, religious and ethnic minorities, prevention efforts essentially amount to modifying their internet practices and usages to minimize the risks of victimization. However, from an ethical perspective, such an approach may well constitute a restriction of these actors' rights and freedoms. Clearly, were such approaches to be advocated in the real world, they would be justifiably criticized, particularly in the absence of prevention efforts targeting potential offenders.

Nevertheless, recent developments indicate a trend towards a more multi-faceted handling of security in cyberspace, which increasingly integrates prevention and education-based measures (Malecki, 2017). That said, the present context does not yet support the construction of an evidence-based approach, as evidence remains rare, fragmentary and subject to rapidly changing conditions. Consequently, public sector action in response to cybercrime must develop the means required for evidence-based public policy as a first step in the construction of a truly preventative approach.

Contribution

Interrupting the Pipeline of Cybercrime Emergence: From Motivated Offenders to Cyberattacks

Alex Kigerl
Ph. D, Assistant Research and Professor of Criminal Justice and Criminology
Washington State University
USA

There is a pipeline of stages that must pass before there can be a victim of cybercrime. The potential offender must be motivated to commit an offense, they must be technically capable of attempting a cyberattack of some kind, their attack must successfully reach its target without being blocked by defensive technologies (e.g. spam filters, anti-virus software), and often there is a human element which requires a final human recipient falling prey to the cyberattack that reaches them. Along this pipeline, each stage presents itself with an opportunity for one or more strategies for cybercrime prevention.

There are structural and societal conditions that appear to relate to cybercrime, or environments that seem to foster motivation to commit cybercrimes (e.g. unemployment, internet users per capita). Once an offender is sufficiently motivated and capable, legal and technological deterrent efforts may persuade an offender to desist, reduce the severity of attacks, or redirect attacks elsewhere. The attacks themselves can be nullified via preventative technologies or user education about computer safety. And lastly in the pipeline, existing cybercriminals can be prosecuted and incapacitated, preventing subsequent attacks until the void that the offender has left is filled with new motivated offenders.

Certainly, the optimum solution would be to leverage prevention efforts at the first stage, preventing motivated offenders from emerging in the first place via structural changes, incentives, and opportunities. Unfortunately, research pertaining to this stage is underdeveloped. Most of the efforts to intervene along these stages have been targeted towards technological defenses, designing security software to detect network intrusions, spot and quarantine malware, block malicious spam from reaching millions of recipients, and flagging blacklisted internet domain names.

The next most common effort to combat cybercrime targets the final possible stage of prevention: incapacitation via legal punitive measures. Legal means to combat cybercrime are more difficult than combating traditional forms of street crime, as cybercrime does not respect borders between nations, let alone borders between the varying legal jurisdictions a cyberattack may cross. Compelling law enforcement residing in the cybercriminal's home country to assist with prosecution is often not possible, as many nations will not cooperate. Offenders are also more difficult to trace, as they can obscure their identities and location via a myriad number of technological means. Gathering evidence also requires more technical sophistication from the investigators.

However, research relating to the first stage of the pipeline has gained momentum over the years, exploring macro-level variables that seem to relate to and predict cybercrime activity. Yet, from a prevention perspective, it should be noted the uncertainty surrounding the causal chain of ordering between the macro-level environment the cyberoffender resides in and the offender's subsequent tendency to commit crimes in cyberspace. Does the environment create motivated offenders, do motivated offenders contribute to the environment, does some third variable cause both, or all of the above?

Much of the macro-level explorations of cybercrime have focused on nation-states as the unit of analysis. One such application used a clustering approach to categorize countries according to their profile of cybercrime activities (Kigerl, 2016). Namely, four categories of countries have been identified so far: lower cybercrime countries, advance fee fraud countries, phishing attack countries, and nonserious cybercrime countries. Low cybercrime countries are, of course, the least active in terms of cybercrime rates, but also tend to have the lowest GDP and internet connectivity. Advance fee fraud countries, which specialize in fraudulent email tactics such as Nigerian scams to convince an unwitting victim to wire an "advance fee" in exchange for some deal being offered, have only somewhat low GDP and internet connectivity levels. Advance fee fraud tends to require little technical sophistication, as it mostly relies on social engineering rather than malware or other automated attacks. Nigeria is one such country classified by the algorithm as an advance fee fraud nation.

Phishing specialist nations, which attempt to defraud a victim by stealing sensitive credential information such as banking passwords by masquerading as the recipient's bank, tend to have higher levels of wealth and internet connectivity. Phishing scams tend to be more technically sophisticated attacks. They rely on spoofed websites designed to match their legitimate website counterpart as perfectly as possible and record user keystrokes or filled form data submitted by the victim. These include nations such as Russia. Finally, nonserious cybercrime nations specialize in mostly spam and digital piracy and have the highest GDP and number of internet users. These include nations such as the United States and China, with large populations and a large number of internet-ready PCs.

This last category, nonserious cybercrime countries, may equally likely be a target as a source of cybercrime activity, as they have a large population of internet-connected devices and internet users, both of which offenders may desire to direct their attacks. Spam tends to be sent from botnets, which are computers infected with malware that can send spam on the spammer's behalf in bulk, as often the spammer has control of thousands of such infected machines. Since wealthier nations have more internet-ready computers, they tend to be the best suitable tar-

gets. Also, nations with greater technological infrastructure and political freedoms are more likely to report malware infections (Holt, Burruss, & Bossler, 2016). Also, at the state level, within the United States, internet use at home is associated with a greater frequency of identity theft (Song, Lynch, & Cochran, 2016).

The number of internet users per capita in a nation is highly predictive of cybercrime rates within that nation, whether the cybercrime activity in question is caused by offenders residing in the same nation or the nation is simply a channel through which the offender transmits an attack. Wealth and economic prosperity plays a more complex role with regards to cybercrime, however. Email spam can be divided into marketing messages intended to sell a product, fraudulent emails, or malicious emails intended to infect the recipient with malware. Marketing spam tends to be highest in nations with high GDP, fraudulent spam tends to originate from nations with lower GDP, and malicious spam can originate from a nation regardless of GDP (Kigerl, 2018). Again, many strategies for perpetrating fraud rely on social engineering, requiring less in the way of expensive technology and computer equipment to pull off. Email fraud has fewer barriers to entry, so poorer nations may be more likely to specialize in this form of cybercrime.

Unemployment can also interact with the number of internet users. By themselves, unemployment tends to reduce the amount of cybercrime originating from a nation, whereas internet connectivity tends to increase cybercrime attacks (Kigerl, 2012). However, the two variables are closely intertwined: nations with very high unemployment also tend to have fewer internet users. When there are exceptions, the resulting impact on cybercrime activity is different. For instance, across all nations that have high internet connectivity, unemployment takes on a positive influence over cybercrime. That is, higher unemployment is associated with higher rates of cybercrime, but only when internet connectivity is also high. Obviously, cybercriminals must be internet users and must be technically skilled to a sufficient degree to engage in cybercrime. When a nation has many internet users but high rates of joblessness, then it is possible that the situation creates more motivated offenders or technically skilled individuals who cannot generate an income from legitimate means. They may turn to cybercrime as a replacement for a legal income.

Identifying the biggest offenders at the national level when it comes to cybercrime may also depend on whether cybercrime is measured in absolute terms or as a rate based on population size within a nation. When measuring digital piracy and software counterfeiting activity as a rate based on the population size of a country, smaller, poorer, and less technologically developed nations have higher digital piracy rates, but lower absolute piracy activity (Kigerl, 2013). When piracy was measured as the absolute number of incidences within a nation, wealthier nations with more internet users accounted for most of the crimes. This suggests that a greater percentage of the populace is engaging in digital piracy in smaller, less wealthy nations, but overall most of the piracy activity originates from wealthier, more connected, countries. Poorer nations have fewer internet users, but internet users who reside in those poorer countries, have a larger incentive to rely on piracy, since the cost of purchasing software and movies legally is beyond their means. However, in wealthy nations, the sheer volume of internet users means that, in absolute terms, more will turn to piracy, simply because there are more internet users.

The research in this area is young, but so far yields some ideas about next steps for further research and also what interventions might be possible even now to prevent cybercrime by targeting some of these associated macro-level variables. Prevention of cybercrime can be targeted at any point along the pipeline of cybercrime emergence. So far most of the efforts have focused near the end-point along the pipeline after some harms from the offense have already occurred. It would be beneficial to marshal additional efforts of prevention towards the early stages of cybercrime development as well.

Contribution

The insufficient nature of cybercrime statistics

Benoît Dupont and Anne-Marie Côté
Professor, University of Montreal
Scientific Director of the Smart Cybersecurity Network (SERENE-RISC)
Canada Research Chair for Security, Identity, and Technology
Canada

Cybercrime now receives considerable attention from the media and is a source of constant concern amongst the public, which is increasingly aware of the emerging digital risks associated with the range of online services enhancing modern life. As such, cybercrime has undoubtedly become the twenty-first century's representative type of criminal activity. Governments, business and consumers worldwide cannot but be concerned in light of the numerous threats imperilling personal information, the lifeblood of the digital economy (Côté et al., 2016). It is, however, surprising to note the discrepancy that exists between, on the one hand, the alarmist messages about cybercrime from governments and businesses, reflecting its objective importance, and on the other, the lack of reliability and robustness of the statistics used to quantify the harm inflicted and underpin the calls for urgent action.

The term cybercrime, now in common use, indirectly contributes to this quantophrenia (Sorokin, 1959). This semantically ambiguous catchall term, applied to everything from the distribution of child pornography to computer hacking to online fraud and a range of attacks designed to render sites unavailable, raises numerous uncertainties and questions regarding the actual meaning of the term (UNODC, 2013). This confusion is made greater still by the fact that the technical complexity inherent in much online crime is such that its inner workings are beyond the ken of all but a select few. It follows that the public discourse on cybercrime draws heavily on statistics of a highly problematic nature, origin and quality. (Côté et al., 2016; Flôrencio and Herley, 2013). Thus, in a context of ever more abundant cybercrime statistics, what is needed is a critical examination of the origin and validity of this data.

The following are among the main criticisms of cybercrime statistics: the influence of private cybersecurity businesses, which produce data using opaque methodologies to create a feeling of insecurity susceptible to generate commercial interest in their products and services (Dupont, 2016); the frequent use of opinion surveys drawing on a limited pool of respondents to quantify the prevalence of an unevenly distributed phenomenon (Furnell, Emm and Papadaki, 2015); the lack of comparability of statistics collected by disparate actors relying on highly diverse analytical methods; the irregularity of data collection intervals, which hinders rigorous analysis of developing cybercrime trends (Reep-van den Bergh and Junger, 2018); the difficulty of accounting for criminal behaviour which involves both online and offline components (Levi, 2017); and victims' systematic under-reporting of cybercrime to the police (Caneppele and Aebi, 2017).

Moreover, criticisms of cybercrime statistics and their production methods have also led to consideration of the indirect effects that imprecise measurement may have had on the quantification of overall crime levels. Thus, some authors have theorized that the sharp drop in traditional crime rates observed in Western countries since the mid-1990s should be analyzed as the result of the interaction of traditional criminal activity with emerging forms of digital crime (Tcherni et al., 2016). Without presenting definitive evidence of this mutation, it is undeniable that the present volume of cybercrime, which, depending on the country, accounts for one third to one half of all crime, casts serious doubt on the dominant criminological narrative positing a sharp decline in crime over the last twenty years or so (Caneppele and Aebi, 2017). In other words, the lack of reliable statistics on cybercrime may have led to two decades' worth of faulty conclusions regarding overall crime rates.

In the UK, the Office for National Statistics attempted to remedy this situation, an endeavour which proved indicative of the inexactness that characterized cybercrime statistics until relatively recently. The measurement method adopted for the 2015 edition of the national victimization survey found that, in addition to the expected 6.5 million incidents of traditional crime, there were 7.6 million incidents of cybercrime and fraud involving a digital component. The result: an unanticipated doubling of the country's annual volume of crime (TNS, 2015). There is no evidence to suggest that this situation is unique to Great Britain; on the contrary, the increasing availability of more robust statistics points to a comparable trend in the majority of Western countries (Reep-van den Bergh and Junger, 2018).

The scientific community's methodological criticisms directed at cybercrime statistics are not merely academic. Now that governments worldwide are adopting ambitious cybersecurity strategies, often armed with legal and regulatory provisions for preventing and controlling cybercrime, which may include budgets mobilizing hundreds of millions, if not billions of dollars, the repercussions of using faulty statistics are far from trivial (Anderson et al., 2012; Dupont, 2016). Public, parapublic and private organizations, including insurance companies and the media, are unable to provide political and economic policy makers, and public opinion, with a sufficiently accurate depiction of the range of relevant problems to inform and drive evidence-based responses.

Two examples will serve to shed light on this observation. The first deals with the impact of cybercrime, rather than the mere quantification of the number of incidents thereof. While recent victimization surveys can, with a satisfactory degree of exactitude, measure the number of individuals and organizations af-

fected by the various forms of cybercrime, the extent of the financial losses incurred and the cost of system and data recovery is extremely difficult to assess. Anderson et al (2013) therefore distinguish between the volume of cybercrime on the one hand, and its impact on the other, as measured by analyzing criminal proceeds, the indirect losses borne by operators of the computer systems exploited by attackers and the investments required to protects digital infrastructure from future attacks. As the authors point out in their attempt to evaluate the cost of cybercrime as rigorously as possible, the present state of scientific knowledge does not, at this time, make it possible to assess these four variables. It follows that strategies to combat cybercrime rely more on intuition and quite superficial data than on the type of modelling that would enable the optimization of policy outcomes.

Our second example illustrates how academic researchers from a variety of disciplines can successfully join forces with private sector analysts to produce cybercrime statistics which, rather than muddying debates, help to inform them. A joint initiative of Austrian computer scientists, Canadian criminologists, the Anti-Phishing Working Group and Go Secure (a Canadian cybersecurity firm) was able to track financial flows to the cybercriminals exploiting ransomware[15] schemes (Paquet-Clouston et al., 2018). This team found that the 35 most active ransomware families had, in the 2013-2017 period, received just over 12 million dollars in ransoms paid in bitcoin, and that the three most successful groups of cybercriminals received 88 percent of these gains. This data shows that the ransomware problem, although the focus of intense media coverage in 2017 and 2018, is probably less catastrophic than reported. This data also serves to orient the public authorities responsible for cybercrime prevention and investigation towards interventions focusing on the small group of criminal actors clearly identified as responsible for the vast majority of the damages, direct or indirect.

These two examples illustrate to what extent it is becoming necessary to integrate cybersecurity firms in the cybercrime quantification efforts of public statistics offices. While we have noted that cybersecurity companies may, at times, instrumentalize the data they publish for their own purposes, it cannot be denied that their unique tools of observation and analysis are valuable mechanisms for measuring cybercrime trends on an international scale. Combined with the data from more traditional victimization surveys and police statistics, this data could be used in a disinterested manner to generate an accurate assessment of cybercrime and, thereby, enable more selective and effective interventions in prevention and law enforcement.

Notes

9 "Phishing is a general term for e-mails, text messages and websites fabricated and sent by criminals and designed to look like they come from well-known and trusted businesses, financial institutions and government agencies in an attempt to collect personal, financial and sensitive information" (RCMP, 2018).

10 A ransomware is a type of malicious software which highjacks a user's data by blocking the latter's access to it on his or her computer or mobile device until the user pays a ransom.

11 A definition of this type of crime is given in the section on fraud, in Chapter 3.

12 The term "revenge porn" refers to the online dissemination of pornographic material produced in a private context, without the consent of the person appearing in it. Typically, this involves intimate images or videos. The vast majority of the persons victimized are women or young girls.

13 The term botnet refers to a set or network of automatically executed web robots, which can be exploited to remotely control all infected computers/servers.

14 The "Deep Web" refers to all non-indexed webpages, which, in fact, includes most of cyberspace. Although the majority of these pages are not platforms for fraudulent activities, a certain fraction of the Deep Web does host such activities, in which case one speaks instead of the "Dark Web," which refers to pages hosting completely unregulated content.

15 A type of malicious software that encrypts the victim's files, coercing the payment of a ransom in exchange for the decryption key.

References

Chapter 2. Crime in a digital world

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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from https://papers.ssrn.com/abstract=1738223

Levi, M. (2017). Assessing the trends, scale and nature of economic 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. Retrieved from 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, from 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. Retrieved from 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. Retrieved from http://www.latimes.com/business/la-fi-equifax-freeze-20170908-story.html

Ponemon Institute. (2017). 2017 Cost of Data Breach Study. IBM Security.

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, from http://www.sci-dev.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. Retrieved from 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. Retrieved from 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, from 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

Interrupting the Pipeline of Cybercrime Emergence: From Motivated Offenders to Cyberattacks

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.

The insufficient nature of cybercrime statistics

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.

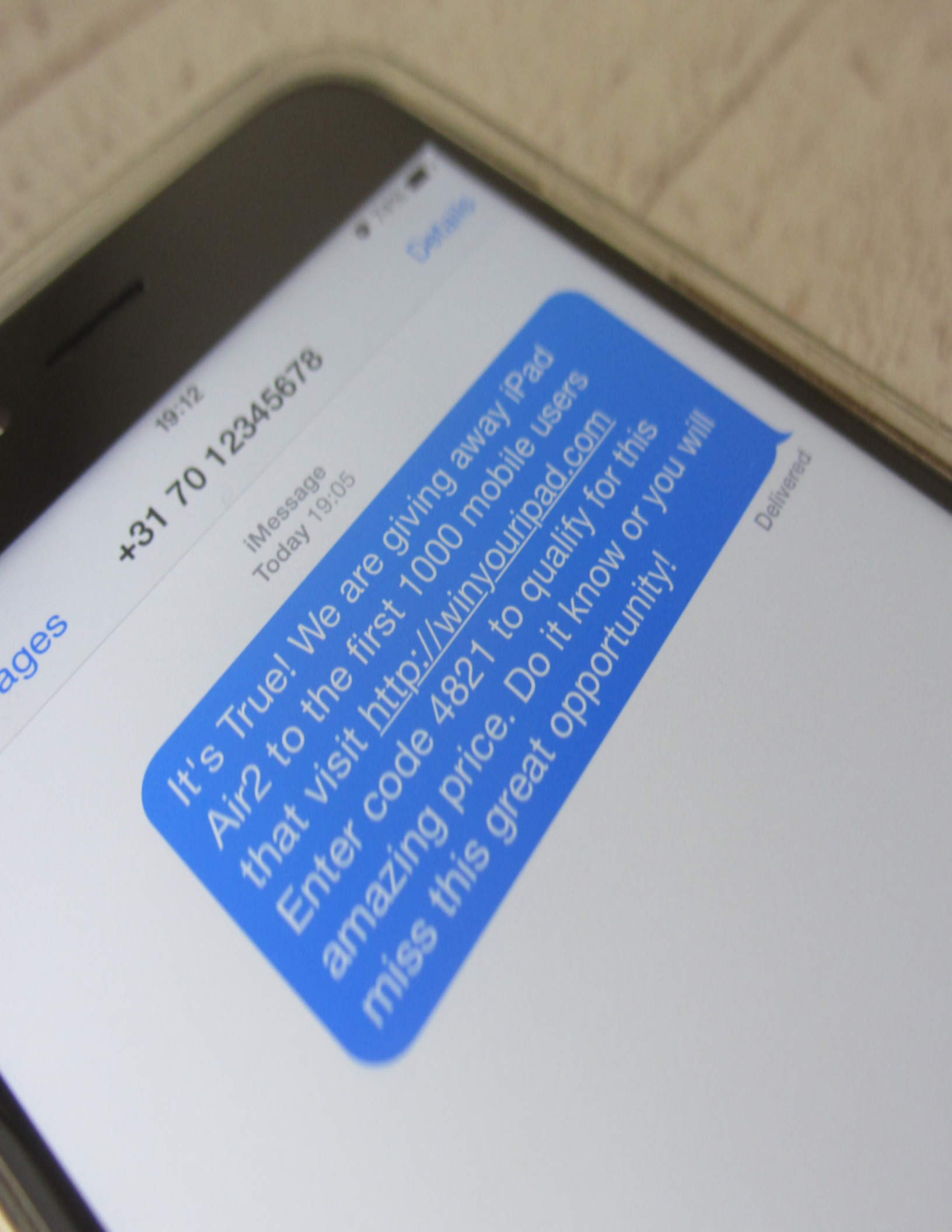
Reep-Van Den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime Science, 7(1), 5.

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

CHAPTER 3

CYBERCRIMES, CYBERCRIMINALS AND CYBERVICTIMS

Chapter 3 proposes an overview of current criminological research on cybercrime. What is meant by the term cybercrime? What is known about the different types of cybercrime? Who are the perpetrators and who are the victims? These are the questions on criminologists' research agendas. Additionally, as scholars endeavour to answer these questions, they are simultaneously seeking to determine whether criminology's traditional theories on delinquency and victimization are useful in the new environment that is cyberspace or whether new approaches are needed to better apprehend this subject. Consequently, our first step will be to examine the different definitional perspectives in the scientific literature, as well as the principal theories applied for understanding the various types of cybercrime.

Introduction

The massive development of information technologies, in conjunction with the internet's specific characteristics, greatly influence contemporary social interactions (Holt & Bossler, 2014). In so doing, they simultaneously create new opportunities for both legal activities and criminal and deviant activities (Yar, 2006). In effect, as Grabosky et al (2001) point out: crime and criminals are opportunistic. Having reminded us of that fundamental principle of criminology, they then report that the explosive growth of information technologies and the internet have indeed increased the opportunities for crime.

In effect, the internet's relative anonymity, its ease of use and its transnational and borderless character are all features, which enable criminals to envisage crime opportunities (Quéméner and Ferry, 2009; Prates et al., 2013). Criminals exploit the characteristics of cyberspace, which make it possible to disseminate information widely, rapidly and inexpensively (Bryant and Bryant, 2014). Wall (2005) has identified a list of six internet related factors that have an impact on delinquent and deviant behaviours. The first factor is globalization, which enables criminals to commit offences beyond traditional borders. However, as globalization impacts law enforcement and policing culture at the local level, this has led some observers to speak of glocalization. Wall also cites the impact of distributed networks. This factor has enabled new opportunities in terms of business relations and networking, even as it has engendered new opportunities for victimization. In effect, the flow of continuous information is such that it is difficult to identify and comprehend new forms of risk. The internet's dual synoptic and panoptic[16] nature also has an impact on criminal behaviour in that it creates facilitates the targeting of new victims. In effect, a criminal is now able to monitor a potential victim and commit a crime without being in physical contact with him or her. The internet therefore creates the possibility of asymmetric relations between the offender and the victim. Such asymmetric relations, moreover, can increase the opportunities for multiplying very small scale criminal acts, which escape the attention of the police and the justice system, and elicit no action on their part, precisely because they are so small, even though these incidents represent significant criminal activity, when considered globally. Furthermore, every transaction effected on the internet leaves a data trail. This fact, combined with privileged access to technology enjoyed by some, enables the creation of highly enviable "data doubles." Although the existence of virtual identities is very useful to law enforcement agencies, it also generates new opportunities for identity theft. Finally, in addition to the changes in the nature of opportunities for crime, the internet also induces transformations in the organization of criminal behaviour. Thus, lone individuals are capable of committing major crimes in cyberspace, which would be beyond their means (financially and organizationally) in the real world. In effect, thanks to technology and the internet, lone offenders can now go online to commit crimes on a global scale.

It's important to note, however, that the mass media is responsible for today's widespread awareness of the internet's criminal dimensions and of cybercrime in general (Wall, 2001; Yar, 2006; Leman-Langlois, 2006). The resulting media representations tend, however, to not only produce an erroneous picture of the real situation, but also lead to an over-reaction on the part of the public and policymakers (Yar, 2006). Citing the example of child pornography, Pansier and Jez (2001, p. 88) remind us that the internet has not increased the number of pedophiles. It has "only facilitated the setting up of new branches of already established networks and made it easier for their members to share files." According to Leman-Langlois (2006), the phenomenon of cyberterrorism exhibits all the characteristics of a moral panic, as defined by Cohen (see box 3.1). In effect, as Leman-Langlois observes, the media and political reaction is disproportionate in comparison with the "infinitesimally small number of empirically observable acts" (p. 64).

Box 3.1. **The moral panic as defined by Cohen (2002, p.1)**

"Societies appear to be subject, every now and then, to periods of moral panic. A condition, episode, person or group of people emerges to become defined as a threat to societal values and interests; it's nature is presented in a stylized and stereotypical fashion by the mass media; the moral barricades are manned by editors, bishops, politicians and other right-thinking people; socially accredited experts pronounce their diagnoses and solutions; ways of coping are evolved or (more often) resorted to; the condition then disappears, submerges or deteriorates and becomes more visible. Sometimes the subject of the panic is quite novel and at other times it is something which has been in existence long enough, but suddenly appears in the limelight. Sometimes the

panic passes over and is forgotten, except in folklore and collective memory; at other times it has more serious and long-lasting repercussions and might produce such changes as those in legal and social policy or even in the way society conceives itself."
According to Stanley Cohen, a moral panic is a socially constructed problem in which the real facts are exaggerated, in particular by the media which become known as "agents of moral indignation" (Frau-Meigs, 2010).
A moral panic develops in accordance with a linear sequential model with three successive phases:
The first phase is the warning phase. The panic has yet to appear, but the media, experts, politicians… start making connections between a number of different events and, in so doing, sound the alarm about a looming threat to society, which until that point was "peaceful and orderly" (Leman-Langlois, 2007).
The second phase corresponds to the impact phase. All events are then interpreted according to a single dominant narrative. The authorities begin implementing surveillance and security measures, which further increases public feelings of insecurity and menace in the face of a phenomenon perceived as particularly dangerous.
The third and final phase is the response phase. The debate is launched and moral entrepreneurs strengthen their positions by defining what is "good" and what is "evil."

In light of the difficulties intrinsic to measuring criminal activities in cyberspace, discussed in the preceding chapter, and in the face of this media fuelled moral panic (Yar, 2006; Leman-Langlois, 2006), criminology has turned its attention to these issues to help us better understand cybercrime. In effect, the objective of criminology is to describe, comprehend and explain the nature of criminal phenomena. Thus, for two decades now, researchers in criminology have been studying "the impact of technology on the practices of offenders, factors affecting the risk of victimization, and the applicability of traditional theories of crime to virtual offences" (Holt and Bossler, 2014, p. 21).

In this chapter, we will examine the relevant studies in criminology and their contribution to our knowledge of this phenomenon. First of all, as we shall see, there is no broad consensus on the notion of cybercrime in the scientific research community, a fact which does not facilitate a clear understanding of subject to be studied. Moreover, this lack of consensus has implications in terms of data collection. Next, we will examine the dominant criminological theories with a view to better understanding certain types of cybercrime. Finally, as it is unrealistic to effect a comprehensive review of each type of crime in cyberspace – due to the diversity of their forms and specific expressions – we have instead chosen to focus on three types of cybercrime: hacking, cyberfraud and cyberviolence. Hacking is an illustration par excellence of cybercrime's novelty as its very existence would be impossible without computers and the internet. Our understanding of this emerging crime remains in its infancy. Cyberfraud is the form of cybercrime that affects the greatest number of victims and globally is presently ranked third overall (Carignan, 2015). Finally, we chose to study violence in the virtual world, as it constitutes one of the more rapidly growing categories of cybercrime. It is of course important to remain abreast of the findings of research to ensure the implementation of effective public policies in terms of prevention.

Cybercrime: Definitions and taxonomies

Debates around the definition of cybercrime

Beyond the multiple methodological problems encountered in empirical studies on cybercrime, the very first difficulty arises at the definitional level (Diamond and Bachmann, 2015). In effect, notwithstanding the growing research on the subject, the notion of cybercrime remains "incomplete and heterogeneous" (Prates et al., 2013, p. 5). Thus, the definition used to describe the concept of cybercrime varies depending on whether a researcher comes from the field of political science, law, sociology or criminology (Brown, 2015). There are almost as many definitions as there are researchers. As cybercrime refers to "complex and sometimes elusive phenomena" (Goodman and Brenner, undated, p. 12), this diversity in approaches does not facilitate comprehension. There is no universally accepted definition of cybercrime at this time (Ngo & Jaishankar, 2017).

Be that as it may, difficulties in developing a consensus definition occur regularly in criminological research on a variety of subjects. For example, debates often arise concerning whether to utilize legal definitions in studying crime. In effect, what is deviant or criminal in one country is not necessarily so in another and vice versa. Consequently, whereas certain criminologists prefer to eschew legal definitions, deeming them somewhat artificial, others see no difficulty in basing their analysis on the legal definitions of criminal acts.

As Wall (2001) points out, the notion of cybercrime does not in fact pertain to a specific legal term. Moreover, not only are criminologists unable to base their study of cybercrime on a legal definition, but they also confront an additional challenge: studying a phenomenon which takes place in an entirely new environment, previously unknown to them.

In essence, the major conceptual debate in criminological research amounts to determining whether cybercrime constitutes a new form of crime or whether it refers to already existing types of crime which have taken new forms in a new environment. In response, a number of different approaches have emerged in the literature.

For David Wall (1998), certain forms of crime in the virtual world have their counterparts in the real world. He offers the example

of fraud, observing that this infraction, whether it is committed in the virtual world or the real world, remains the same; consequently, it's not the offence which changes but rather the environment where it occurs, which is new. Thus, for Wall, cybercrimes may be considered "old wine in a new bottles." That said, there do effectively exist crimes, such as hacking or computer intrusions, which are entirely dependent on new technologies and the internet. These infractions may therefore be considered "new wine in new bottles," as they could not be committed, or indeed exist, without the advent of the computer and the internet.

Peter Grabosky (2001) also sees virtual crime as "old wine in new bottles." This author studied the question from the standpoint of offenders' motivations. In his view, these motivations, whether in the real world or the virtual world, are unvarying: "greed, lust power, revenge, adventure and the desire to taste 'forbidden fruit'» (p. 244). To these may be added the intellectual challenge of mastering this complex system. According to Grabosky, while these motivations are not new, there is a novel element: the capacity of these new technologies to facilitate their realization.

In parallel with this vision of the concept of cybercrime, it has been observed that access to a pool of potential victims in a world of connected devices, along with the number of internet users, in conjunction with the anonymity characteristic of cyberspace, have, taken together, fundamentally changed criminal processes such that for certain observers cybercrime is "new wine without bottles" (Holt and Bossler, 2014).

Bryant and Bryant (2014) contribute another point of view to this discussion. For them, all crimes are situated on a continuum, which includes traditional crimes on one side and digital crimes on the other. In effect, according to their findings, many crimes exhibit both traditional and digital features. In practice, the existence of a clear dichotomy between the two types is quite rare. Finally, according to Yar (2006) cybercrimes represent a new type of criminality which differ completely from crimes committed in the real world (Simion, 2009).

At the end of the day, as Lusthaus (2013) argues, it's not clear whether this conceptual discussion is particularly useful in helping us to better grasp the functioning of cybercrime or, for that matter, the behaviour of cybercriminals. For Lusthaus, it's not necessarily useful to get bogged down in categorizing new crimes vs. old crimes if our principal interest is in identifying the structure, organization and characteristics of cybercriminals. In his view, the principal question is to determine how these new technologies have (or have not) changed the nature of crime. Nevertheless, he recognizes that such an approach could generate still more confusion. In effect, based on this perspective, cybercrime could encompass every type of crime, due to technology's penetration in all of our daily activities.

Clearly, defining cybercrime is an eminently difficult task, which remains an open question. Researchers agree that cyberspace and computer technologies are being used to facilitate criminal acts and deviance (Holt and Bossler, 2013). However, they do not necessarily agree on which types of crimes should be categorized as cybercrimes. The difficulties inherent in grasping the notion of cybercrime are, in effect, amplified by the fact that it pertains to an entire gamut of illicit and illegal activities rather than to a simple undifferentiated reality. As we shall see, several taxonomies have been developed in the research community with a view to providing a more complete picture of what is encompassed under the notion of cybercrime.

Cybercrime taxonomies

According to Wall (2007), the evolution of cybercrime has passed through three stages. In the first stage, prior to the 1970s, cybercrimes largely consisted of traditional crimes, assisted in some fashion by the use of a computer.

In the second stage (after the 1970s), the advent of new technologies and computer networks enabled a gradual increase in the distribution and globalization of traditional crimes. Finally, the third stage is characterized by crimes which would never have existed without the internet. They are sui generis cybercrimes, which exist independently of other types of crimes.

Thus, the usual approach envisaged for defining the various types of cybercrimes is based on the distinction between "computer-assisted crimes" and "computer-focused crimes" (Furnell, 2004; Yar, 2006). The former refer to "traditional" crimes, which found a second life in cyberspace, including, for example, fraud, pornography and money laundering. The second category concerns crimes that developed with the birth and evolution of the internet and would not exist without it, i.e., crimes such as hacking or virus attacks. This type of classification focuses exclusively on the role played by technology and is based on a utilitarian perspective (which is generally favoured by the law enforcement community). However, from the perspective of criminological research, it is somewhat limited as it obscures the victim-offender relationship, which for criminologists, is fundamental in the scientific study of criminal offences. As a result, several authors have worked to develop more operational taxonomies, from the vantage point of research.

Wall (2001) was one of the first authors to reflect on and develop a cybercrime taxonomy, which remains, to this day, the most complete and widely recognized cybercrime classification system in the research community (Holt, 2009; Holt & Bossler, 2014). Wall identified four categories of cybercrime:

i. **Cyber-trepass** – crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses.

ii. **Cyber-deceptions and theft** – stealing (money, property), e.g. credit card fraud, intellectual property violations (a.k.a. "piracy").

iii. **Cyber-pornography** – breaching laws on obscenity and decency.

iv. **Cyber-violence** – doing psychological harm to, or inciting physical harm against others, thereby breaching laws rela-

ting to the protection of the person, e.g. hate speech, stalking.

Leman-Langlois (2006) proposes an objective taxonomy founded on two characteristics: the role of computer networks in the commission of the criminal act and a periodization of when different offences were criminalized (see Table 3.1). .

Alkaabi, Mohay, McCullagh, & Chantler (2010) propose a cybercrime taxonomy based on three components: the role played by the computer, the nature of the crime and the context surrounding it. It may be summarized as follows:

i. **Type I crimes** include crimes where the computer, computer network, or electronic device is the target of the criminal activity and is composed of four sub-categories:
   a. unauthorized access offences such as hacking;
   b. malicious code offences such as dissemination of viruses and worms;
   c. interruption of services offences such as disrupting or denying computer services and applications such as denial of service attacks and Botnets; and
   d. theft or misuse of services offences such as theft or misuse of someone's Internet account or domain name.

ii. **Type II crimes** include crimes where the computer, computer network, or electronic device is the tool used to commit or facilitate the crime and is composed of three sub-categories:
   a. content violation offences such as possession of child pornography, unauthorized possession of military secrets and intellectual property offences;
   b. unauthorized alteration of data or software for personal or organizational gain such as online fraud; and;
   c. improper use of telecommunications such as cyberstalking, spamming and the use of carriage service with the intention or conspiracy to commit harmful or criminal activity.

For these authors, as a computer may play a number of different roles in certain crimes, a given crime could be classified as belonging to more than one category. In addition, beyond the issue of establishing a classification system based on the type of crime and the role computers play in the commission of a crime, it is crucial, in their view, that a taxonomy of cybercrime be completed with contextual information such as the offender's main motivation (individual or political, for example), his connection with the victim, and the type of victim affected by the crime (individual, private business, government agency or infrastructure). Finally, Bryant and Bryant (2014, p. 25) classify cybercrimes in accordance with their degree of novelty and digital complexity (see Table 3.2).

As we have just seen, the lack of definitional clarity and consensus around the term cybercrime hinders the harmonizing of research efforts and leads to researchers adopting their own definitions as a function of their own specific research interests and areas of focus.

And yet, the elaboration of a universally accepted definition has fundamental implications for real issues.

Table 3.1. **An objective taxonomy of cybercrime, according to Leman-Langlois (2006)**

Role of networks/cyberspace	Period when criminalized	-
	Traditional crimes (pre-internet)	Emergent/imminent crimes (post-internet)
Trigger	N.A.	Distributed attacks; virtual vandalism
Multiplier	Child pornography; identity theft; fraud	File sharing; spam
Accessory	Deception; terrorism and sabotage	Terrorism (support)

Tableau 3.2. **Bryant and Bryant's classification (2014)**

	Increasing digitality	
Increasing novelty	Traditional crimes, few digital crime features, other than digital forensics, e.g., burglary of a building	Traditional crimes with some digital crime features, e.g., credit card fraud
	Digital crimes with some traditional crime features, e.g., hacking using social engineering to gain a password	Digital crimes, few traditional features, e.g., DDoS attacks

Issues arising from the absence of a shared definition

The absence of a commonly accepted taxonomy of cybercrimes clearly hinders international efforts to identify, report and monitor trends regarding this phenomenon (Alkaabi et al., 2010). Thus, according to Furnell (2001), a consensus on how to classify cybercrimes is both essential and imperative. A harmonized classification system for cybercrime would facilitate the fight against this phenomenon, both at the individual level, as well as in terms of the competent agencies and organizations.

The benefits of a coherent and complete taxonomy of the crimes occurring in cyberspace would be felt on many levels, including information sharing, precise reporting of cybercrime incidents, cooperation on current investigations, long term cooperation in the fight against cybercrime and, finally, in the harmonization of the relevant legislation and regulatory frameworks (Alkaabi et al., 2010).

Ngo and Jaishankar (2017) advance similar arguments. For them, it is essential today – and not just in the future – that the different types of cybercrimes be properly defined and classified. First of all, this would enable all stakeholders, be they researchers or technical or legal experts, to employ a common language, thereby facilitating discussions and the implementation of effective collaboration. Moreover, simply have a common vocabulary would facilitate determining the scope of the problem. Consensus on definitions and classifications would also bolster law enforcement agencies, and the justice system as a whole, in their efforts to investigate, combat and prevent these types of crimes. Finally, such a consensus would make it easier to forecast cybercrime's future trends and formulate new solutions in response.

As Wall reminds us (2017, p. 23), more often than not, the term cybercrime tends to be used "metaphorically and emotionally rather than scientifically and legally." Several terms such as cybercrime, computer-related crime, high tech crime or digital crime, for example, are used interchangeably (Simion, 2009), thereby confusing matters when the task at hand is to better understand this phenomenon. Moreover, research on cybercrime focuses principally on the prevalence of different types of crimes and is often lacking in sound theoretical foundations (Kerstens and Veenstra, 2015). That said, certain researchers are working to develop a clearer picture of the situation by applying longstanding criminological theories. The resulting findings could serve to guide public policy from a prevention perspective.

Box 3.2. **Applying traditional theories to explain cybercrime**

Only a small number of studies on cybercrime have sought to determine whether traditional theories in criminology can help us to understand the participation of certain individuals in criminal acts in cyberspace (Kerstens et Veenstra, 2015). Essentially three positions are held on this subject, all of which directly originated from the debates around the definition of the term "cybercrime," discussed above.

According to Kerstens and Veenstra (2015) Grabosky (2001) sees online and offline behaviour patterns as fundamentally similar. Consequently, for Grabosky traditional theories in criminology are entirely applicable, in particular the routine activity theory.

Yar (2005) also takes the routine activity theory as his point of departure. However, he stresses the differences between the real world and the virtual world as he em-

phasizes the key role of technological innovation. Finally, Jaishankar (2008), who emphasizes the interdependence of the virtual and real worlds, favours, as we shall see below, the development of a specific theory to explain cybercrime.

The traditional theories in criminology most often applied by current research on cybercrime are Sutherland's differential association theory (1947), the techniques of neutralization, identified by Sykes and Matza (1957), and the general theory of crime, largely based on low self-control, advanced by Gottfredson and Hirschi (1990). The routine activities and crime opportunities theory of Cohen and Felson (1979) remains the most frequently cited theory for explaining the commission of criminal acts (Bernier, 2016). We will now summarize these different theories before considering their applicability in relation to cybercrime.

Learning-based theories

Sutherland's differential association theory (1947) concerns the knowledge and habits an individual assimilates in his environment and through his relations with other persons. Sutherland posits that an individual learns new ways to envisage the world, as well as how to behave through contact with his peers. Thus, an individual will not only imitate what he sees, but will also "learn to interpret the actions and the social and material context around him in a manner conducive to the commission of criminal acts" (Leman-Langlois, 2007, p. 80). In effect, criminal behaviour is learned and not innate. Learning comes from communication with other persons where such communication may be verbal or physical or take other forms such as by providing an example or imparting an attitude. Small groups are the most propitious contexts for learning because it is in such settings where the individual is most apt to identify with others. Criminal behaviour is learned via contact with persons that the individual trusts, respects or has befriended. Moreover, such learning goes beyond crime techniques per se, as it mainly concerns perspectives (i.e., values, motivation, attitudes and rationalizations) favourable to the commission of criminal acts. In effect, far from being a simple theory of imitation, differential association chiefly concerns the adoption of interpretations, symbols and attitudes (Jaquith, 1981).

Sykes and Matza (1957) developed an explanatory model for crime along the same lines as learning-based theories, based on the fact that practically everyone feels morally obliged to respect the law, including criminals. Thus, when an individual commits a crime, he needs to justify and rationalize his behaviour. These justifications, which are called techniques of neutralization, are learned from one's contact with peers. Sykes and Matza highlighted five techniques: denial of responsibility, denial of harm, denial of the victim, condemnation of the condemners (the police are corrupt, the system is hypocritical, etc.) and appeal to higher loyalties (e.g., towards a friend).

According to most criminologists, it's highly probable that criminal conduct precedes such justifications. Consequently, techniques of neutralization are apparently not a cause of crime, but are instead used as a means of evading potential punishment.

An integrated theory

Gottfredson and Hirschi (1990) proposed to synthesize the state of knowledge in the field then known as the etiology[17] of delinquency. As Ouimet explains (2009), their ambition was to explain all criminal behaviour patterns, as well as a number of different types of deviance, in all times and places. Their approach was premised on two postulates: criminals are rational beings and crime is but another manifestation of a common problem. Basing their synthesis on rational choice theory and social control theory, they then integrated into their model a theory of personal control. Thus, for these authors the primary etiological factor in crime is the individual's capacity to control his impulses and desires. According to Gottfredson and Hirschi, weak self-control is principally explained by the absence or inadequacy of socializing forces, in particular good parenting practices. In effect, according to Gottfredson and Hirschi, good self-control depends on three factors: parental supervision, recognition of inadequate behaviour and the capacity to intervene with the child. As such, weak self-control may be entirely explained by nurture as opposed to nature. Individuals with weak self-control are generally characterized by greater impulsiveness, thrill-seeking, an appetite for risk, a preference for physical activities over intellectual ones, little tolerance for frustration and a propensity to express frustration physically.

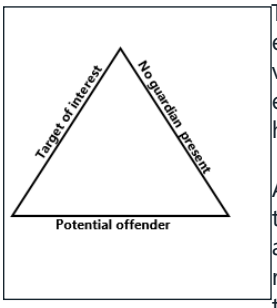
A meta-analysis by Pratt and Cullen (2000) confirmed that low self-control is a good predictor of delinquent behaviour, albeit insufficient in and of itself to explain delinquent etiology.

The economic theory of crime

Cohen and Felson (1979) studied the variations in crime rates by analyzing crime statistics in the United States between 1960 and 1990. Rather than focusing on the specific characteristics of offenders, they propose an approach based on the circumstances in which criminal acts take place. They see crime from the perspective of economic analysis. Their basic premise is that crime is a rational activity. In effect, according to them, the criminal is a rational being who does a cost-benefit analysis before committing an offence. Thus, if the crime's cost (risk) is less than its potential benefit to the offender he will commit the crime. Furthermore, the period studied by Cohen and Felson was characterized by an increase in the quantity of goods in circulation, which signified greater opportunities for theft. Moreover, this same period saw

a significant increase in the economically active population, particularly with the major influx of women into the labour force, a development which led to more homes going unwatched during working hours.

It follows then, that variations in crime rates are explained by three factors: the presence of a crime opportunity, the presence of an individual ready to seize the opportunity and the absence of a guardian.



This theory offers good explanations for repeat victimization and the existence of crime hotspots.

According to these authors, crime can be avoided provided one removes any one of the three preconditions facilitating the commission of an offence. A good crime prevention solution, then, is to act on one of these three factors. In effect, this theory, among others, is the basis for situational prevention approaches, which posit that acting on the crime opportunities environment may dissuade criminals from committing offences.

Today, other theories are also being studied to explain cybercrime, in particular theories based on psychology. Although this body of research remains quite limited, these psychological approaches will enrich current knowledge in the pursuit of better understanding of cybercriminals and their victims.

As we shall see below, by confronting the above theories with different cybercrime phenomena, researchers are clarifying and identifying the characteristics of both offenders and victims, particularly in relation to the commission of certain types of cybercrime.

Hacking

Box 3.3. **Two cases of computer hacking**

The Ryan Cleary affair
In May 2013, Ryan Cleary, a 19 year-old British "hacker," received a thirty-two month prison sentence for participating in a number of computer attacks against various law enforcement and intelligence agencies. These attacks included the hacking of the websites of the CIA and of Britain's Serious Organized Crime Agency (SOCA). Although Cleary confessed his membership in LulzSec, an organization of hackers known, notably, for penetrating the computer systems of Sony and the United States Senate, this group has always denied Ryan Cleary's involvement in their activities.

The young hacker's method was to organize distributed denial of service attacks (DDoS) which aim to make an online service unavailable by overwhelming it with useless traffic. DDoS attacks now represent a real threat because they are extremely difficult to counter and increasingly easy to implement.

Ryan Cleary, who has been diagnosed with Asperger's syndrome and agoraphobia, claimed that he acted out of altruistic motives, at least in part, as he sought to challenge powerful interests and demonstrate that, contrary to the conventional wisdom, the confidential data stored by large companies and organizations is not sufficiently secure.

After his arrest, Cleary was publicly exposed by Anonymous, which published his name, address and telephone number in a revenge attack. In effect, Cleary had hacked the AnonOps group's website and exposed over 600 nicknames and IP addresses.

The Kane Gamble affair
On April 20, 2018, Kane Gamble, an 18 year-old British adolescent, was sentenced to two years of detention and the seizure of his computer equipment in its entirety for having hacked the accounts of several high level American government officials. The young hacker confessed to committing ten infractions of computer security legislation, between June 2015 and February 2016.

In particular, he succeeded in obtaining numerous confidential documents from the email account of former CIA director John Brennan regarding military and intelligence operations conducted in Afghanistan and Iran. He also succeeded in taking control of the iPad of Brennan's spouse. Jeh Johnson, the former U.S. Secretary of Homeland Security, was also targeted, as were certain advisors of former President Barack Obama, former FBI Deputy Director Mark Giuliano and the Justice Department's IT systems.

Gamble boasted of having implemented call forwarding to divert the communications of James Clapper, former Director of National Intelligence, towards the Free Palestine Movement, and of having engineered the "biggest hack of all time" by hacking the identities of 1,000 FBI employees, as well as that of the police

officer responsible for shooting Michael Brown in Ferguson, Missouri.

The Crown argued that, taken as a whole, these acts were intended as political support for the Palestinians, were motivated by the death of innocent civilians and were also a way to protest against police violence and racist acts. However, according to the defence, these actions were merely a series of pranks, carried out by a naive adolescent suffering from autism.

Just as the notion of cybercrime is rather vague and corresponds to a wide range of acts, the term hacking is likewise a generic term associated with a variety of distinct activities (Yar, 2006). Décary-Hétu (2013) wonder, moreover, whether the abuses of language around this notion have not, at the end of the day, so denatured it as to render it meaningless.

Definition of hacking

Leeson and Coyne define hacking as follows:

> "'Hacking' refers to multiple activities. It includes, for instance, breaking passwords; creating 'logic bombs'; e-mail bombs; denial of service attacks; writing and releasing viruses and worms; viewing restricted, electronically-stored information owned by others; URL redirection; adulterating Web sites; or any other behavior that involves accessing a computing system without appropriate authorization." (2014, p.207)

Leeson and Coyne's definition is very detailed indeed. In contrast, the vast majority of researchers are content with a more restrictive definition in which hacking is conceived of as "unauthorized access to a computer" (Brenner, 2001, p. 2; Taylor 1999).

Based on this definition, Décary-Hétu (2013) identifies three distinct techniques utilized by hackers: decoding, hacking and social engineering.

Decoding concerns the deciphering of passwords (or the attempt to do so) to gain access to an IT system (Rowan, 2009). Hacking is understood as the act of taking advantage of poorly written code or mistakes made by programmers. Whereas hacking and decoding utilize technological means, the third technique, social engineering, utilizes the human factor. In effect, this technique is defined as "the process of using social interactions to obtain information about a victim's computer system" (Winkler and Dealy, 1995, as cited by Décary-Hétu, 2013, p. 4).

With this definition as their point of departure, researchers have worked to develop more sophisticated sociological profiles corresponding, respectively, to hackers and their victims.

Hacker taxonomies and characteristic profiles

1) Taxonomy

A focus of studies on hacking has been to identify and differentiate the various categories of hackers. To that end, two major approaches have been followed. One emphasizes what motivates hackers to commit criminal acts, the other focuses on their degree of technical knowledge.

Rogers (1999) was one of the first to develop a taxonomy that categorized hackers in accordance with their technical capacities, barely eight years after the birth of the WWW. He identified, at that time, four groups:

i. senior hackers, who have no criminal intent, are mainly interested in the technology and believe that all information should be free;

ii. "script kiddies" who use pre-written software to carry out attacks but lack the knowledge necessary to understand what they're doing or to create other tools;

iii. professional criminals who are full-time hackers, earn their living by hacking and are contracted by governments, companies and organized crime; and

iv. programmers who produce the malicious code the other three groups use for hacking.

Taxonomies based on hackers' motivations focus on the goals behind their actions. Researchers emphasize hackers' motivations because they see them as rational actors[18] who consciously choose to engage in illicit activities in the hopes of earning income or gaining satisfaction (Yar, 2006). Five motivations emerge from a review of the literature: recognition, money, ideology, curiosity and technical challenges. According to the data collected during a study by Décary-Hétu (2013), a sixth motivation may be added: altruism. The altruistic hacker is an individual who supposedly seeks to help others by identifying flaws in their systems and then subsequently alerts them to the existence of these issues. While this type of individual may contribute to making systems more secure, the fact remains that they are not authorized to engage in such actions and are, consequently, subject to prosecution in a court of law.

Finally, in 2006, Rogers proposed a hybrid taxonomy, based on both hackers' motivations and their technical capacities. This exercise resulted in the identification of nine categories:

i. novices who use automated tools and seek to make a name for themselves;

ii. cyber-punks, at a slightly higher level, who have some knowledge of programming and seek money and fame;

iii. internals who attack their employers out of revenge;

iv. petty thieves, mainly motivated by money, who make the transition from the real world to the virtual world in pursuit of their targets, such as banks and credit card companies;

v. virus writers/coders;

vi. old guard hackers, heirs of the mentality of senior hackers, who seek intellectual stimulation;

vii. professional criminals who specialize in computer crime in pursuit of financial gains;

viii. the information warrior who seeks to destabilize decision-making centres and is motivated by patriotism; and

ix. the political activist.

As many authors have observed (Yar, 2006, Leeson and Coyne, 2014), there exists a wide variety of hackers, characterized by diverse motivations. As a result, Décary-Hétu (2013) underscores the inherent difficulties in the exercise of developing a characteristic hacker profile. In his view, it seems more realistic to envisage profiles as diverse as those applicable to more traditional offenders.

Nonetheless, certain studies have focused specifically on profiling hackers in order to better understand their prevalence and the causes of their behaviour.

2) Characteristic hacker profiles

Researchers have sought to comprehend the causes explaining hackers' behaviour by studying the relevant contextual and personal factors.

In terms of contextual factors, researchers have tackled the subject from two different angles: peer influence and family influence.

Regarding peer influence, Holt and Bossler (2014) observe that the first approach favoured by qualitative studies was to examine hackers' behaviour by applying theories of learning, notably Sutherland's theory of differential association (1947). These studies demonstrated a correlation between hackers' peer relations and their participation in hacking. Contact with peers who engage in hacking teaches individuals that hacking is an acceptable activity, thereby increasing the likelihood that they themselves will become hackers.

Furthermore, with peer contact hackers learn to use what Sykes and Matza (1957) called techniques of neutralization in order to excuse or justify their actions. Essentially, hackers either pretend that their actions cause no harm or that the fault lies with the victims who are guilty of deficient programming and IT security skills. That said, in practice it's very difficult to clearly distinguish between hackers' ex ante motivations and their ex post facto justifications (Taylor, 1999).

Regarding family influence, studies have drawn on Gottfredson and Hirschi's theory of weak self-control (1990). This area of research is still in its infancy and it's not clear whether a link exists between weak self-control and hacking (Holt and Bossler, 2014). Much research remains to be done in light of the numerous behaviours underlying hacking. However, Holt et al. (2012) have begun to detect a link between weak self-control, peer relations and hacking. Higgins (2005) has demonstrated that although weak self-control is connected with software piracy, social learning remains a better explanatory factor for this type of activity. He advocates combining the theory of weak self-control with the theory of social learning as the way forward towards a better understanding of the problem.

Regarding the personal factors leading individuals to engage in hacking activities, the only point of consensus found in the literature is that the vast majority of hackers are male (Décary-Hétu, 2013; Taylor, 1999). Indeed, certain authors estimate the male to female ratio at 99:1 (Taylor, 1999). Hackers are also mostly young persons under the age of 30 (Leeson and Coyne, 2014; Décary-Hétu, 2013). According to Sterling (1994), most hackers start at a young age and quit hacking in their early twenties. It would seem, then, that gender and youth are both explanatory factors in relation to hacking (Taylor, 1999). In addition, most hackers are Caucasian.

Other factors leading an individual to participate in hacking activities have been identified. Exposure to technology at a very young age, via video games for example, is an important factor. In addition to an avid interest in technology, it has been demonstrated that hackers have an above average aptitude for self-management, as well as, in certain cases, antisocial traits. Finally, hackers are apparently more creative persons with superior analytical and decision-making capacities (Holt, 2007; Taylor, 1999).

Findings on other sociodemographic characteristics, such as educational or occupational profiles, vary widely in accordance with sampling techniques (Décary-Hétu, 2013). Pontell and Rosoff (2009) found that computer crimes such as hacking are more common in the higher social classes.

Many of the studies on the causes of hacking mainly focused on rather simple forms of hacking. However, while there remain many unanswered questions about the latter, still less is understood about the more complex forms of hacking (Holt and Bossler, 2014).

Hacking victim profiles

Computer hacking affects individuals as much as it does businesses and governments. However, it's quite difficult to determine the characteristics of potential individual victims as little is known about them. In contrast, because attacks against businesses or governments are, by definition, greater in scale, they are heavily covered by the media. On the other hand, we know that a large number of attacks against businesses or even governments are never revealed due to the risk of reputational damage.

There are major deficiencies in the data on individual victims because the latter do not report hacking incidents to the competent authorities, either due to a lack of knowledge or because victims lack confidence in the likelihood of action from the justice system. To remedy this problem, criminologists have turned to victimization surveys. However, studies on hacking are usually done with sample groups composed of students and are, therefore, somewhat limited. (Holt and Bossler, 2013).

The principal method for learning more about hacking victims has been to apply the theory of routine activities developed by Cohen and Felson. These studies have not established any correlation between age and the risk of being victimized by hacking. This is contrary to what criminologists regard as a known victimization risk factor in the context of traditional crimes. Women are apparently more affected by hacking and malware infections. However, this data is insufficiently robust to draw conclusions regarding the specific targeting of categories of victims, particularly since hackers are known to generally target a very wide pool of potential victims as opposed to specific individual targets. Another finding: persons who commit cybercrimes are apparently at a greater risk of becoming victims in turn. This, it would seem, is particularly true of individuals who make illegal downloads or consume online pornography (Weulen Kranenbarg, Holt and van Gelder, 2017).

Finally, there is still little solid proof concerning the efficacy of anti-virus software, for example, or firewalls against hacking. Nor, for that matter, do good IT skills necessarily protect against the risk of being victimized by hacking. In fact, such skills may even be a risk factor insofar as individuals with good technical skills are more likely to engage in risky behaviour when surfing the internet (Van Wilsem, 2013).

Computer fraud

Box 3.4. **The "Nigerian scam"**

Mike, a Nigerian conman

Phishing is one of the most notorious computer fraud techniques today. The principle is simple: a victim receives an email or telephone call designed to trick him into taking certain actions that provide the conman with various types of personal information, which the latter then uses to obtain money from the victim. The Nigerian scam, also known as the 419 scam, is an extremely widespread variation, particularly popular among criminals based in Africa. The victim is promised a very large sum of money upon payment of various "necessary" fees (Cukier, Nesselroth and Cody, 2007). However, following the payment of said "advance fees," communications continue between the scammer and the victim, during which the latter is constantly asked to pay additional fees before he can collect the promised sum of money. This process continues until the victim stops making payments (Dyrud, 2005). This is an extremely effective technique which remains surprisingly productive, despite the constant and increasing efforts to raise public awareness. In effect, according to the FBI, 1,200 companies were scammed in 2014, to the tune of 180 million dollars, vs. 5,800 companies in 2015 when total "profits" reached 570 million dollars.

Thanks to this technique "Mike," a 40-year old Nigerian conman succeeded in swindling over 60 million dollars from hundreds of victims on the internet, including $15.4 million from a single victim. A head of a transnational network with approximately forty members in Nigeria, Malaysia and South Africa, Mike was arrested by Interpol with the assistance of the Nigerian authorities in August 2016. Mike and his accomplices passed themselves off as princes, heirs to great fortunes or high-ranking officers in the military wishing to make an urgent transfer of funds abroad. To facilitate the transfer, they requested the assistance of their victims in exchange for a promise to pay a commission. First, the "prince" would request the payment of an advance fee (supposedly to pay legal fees, customs charges, taxes, etc.), as well as banking particulars and personal identification to facilitate the money transfer. The latter information would then be used by the scammers to steal their victim's identity and empty his bank accounts.

This network also used the famous "CEO scam," which consisted of hacking the account of a high level company executive and then using this hacked account to send a message to an employee directing him or her to effect a quick transfer of monies to a specific bank account. To carry out this scam, Mike's network hacked the email accounts of small and medium-sized enterprises worldwide, particularly in India, Australia, Canada, Malaysia, Thailand, Romania, South Africa, etc. The stolen money would then be laundered by contacts in China, Europe and the United States who produced bank statements to mask these flows of illicit funds.

Fraud has always existed. However, the explosion in internet usage has vastly multiplied the opportunities for this type of crime, as criminals now have access to a far greater pool of potential victims. As the internet increasingly expands as a venue for commerce, it simultaneously develops as a vector for fraud (Grabosky, 2001). Cyberspace may, in effect, be considered a particularly "fertile ground" for this type of crime (Fried, 2001).

As with many other cybercrimes, the lack of reliable data is a serious obstacle to the analysis of online fraud (Yar, 2006, Holt and Bossler, 2014). The variety and scope of online fraud are difficult to determine for a number of reasons. The lack of reporting, the absence of an international consensus on how to classify different types of fraud, the mixture of methods characterizing many types of fraud (both online and off) and the lack of published data and information on cyberfraud from national agencies are all obstacles to a better understanding of the phenomenon (Button, McNaughton Nicholls, Kerr and Owen, 2014).

Furthermore, online fraud is closely connected with hacking (Holt and Bossler, 2014). This increases the number of actors and actions which must be taken into consideration and, consequently, complicates the already difficult challenge of apprehending perpetrators.

Definition and taxonomy of internet fraud

Fraud may be defined as a "false representation by means of a statement or conduct made knowingly or recklessly in order to gain material advantage" (Martin, 2003, p. 1). In effect, fraud victims are dispossessed of property or money through disinformation or deceit. Internet fraud (or cyberfraud) is thus a general term, which does not refer to a specific type of act, but instead encompasses a variety of acts.

Wall (2007) has elaborated a very detailed taxonomy of internet fraud, which includes:

i. Market arbitrage frauds targeting
   a. government and other monopolies in
      - medicine
      - perfume
      - cigarettes
      - online betting and casinos
   b. advertisers (click fraud)
   c. users (e.g., premium rate number scams)

ii. Frauds associated with the advent of the online economy
   a. targeting consumers
      - auction scams
      - subscription scams
      - vacation rental scams
      - easy credit scams
      - exotic investment fraud
   b. targeting aspiring actors

iii. Advance fee frauds
   a. The Nigerian scam
   b. lottery prize scams
   c. dating site sams

Ryan, Lavoie, Dupont and Fortin (2011) focused specifically on fraud using social media. They distinguished two main types: elaborate frauds and identity theft. Elaborate frauds are, in turn, broken down into four sub-categories: breaches of trust, property rental fraud, frauds based on misrepresentation or forgeries, and unauthorized offers of services.

Ryan et al (2011, p. 7) define an elaborate fraud as "an act of deception committed with the intent of making a profit, but which does not entail identity theft."

Koops and Leenes (2006, p. 556) define identity theft as: "fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent."

There are multiple methods for committing fraud, including phishing and hacking. Phishing is an act of deception in which impersonation is used to obtain information from a target (Lastdrager 2014, p. 8). Conmen use this technique in an attempt to obtain personal information, often by sending a fraudulent email. Another method is social engineering, a method of hacking defined above.

Internet scammer profiles

On the internet conmen gain greater flexibility in setting up their schemes and achieve more success in convincing their victims. In effect, people are more easily influenced in non-face to face situations. Moreover, technology not only somewhat diminishes the quality of interactions, it also facilitates the desindividuation[19] of one's interlocutors (Warschauer, 2003). The anonymity afforded by the internet is such that an individual may lose control and adopt behaviours that he or she would not adopt in another context. This perceived anonymity of the internet contributes to online disinhibition. People have far fewer limits in cyberspace (Suler, 2004).

According to the findings of Ryan, Lavoie, Dupont and Fortin (2011), internet scammers are slightly younger than their victims. Perpetrators of elaborate scams are apparently older than those involved in identity theft. As with the majority of crimes committed in cyberspace, most scammers are male. Women cyberfraud perpetrators are more inclined to engage in identity theft than in elaborate frauds.

A high degree of technical skill does not seem to be necessary in cyberfraud. Carignan (2015) observes that the majority of internet frauds are apparently committed by cybercriminals from Africa and the Arabian Peninsula, as pointed out in the preceding chapter. Carignan's study is among the few to focus on profiling cybercriminals in terms of their places of origin. Drawing on Cohen and Felson's theory of routine activities, Carignan's findings suggest that factors such as access to employment, economic inequalities, internet speeds and access to IT equipment, which differ around the world, all have an impact on a criminal's opportunities to commit fraud.

In effect, if one considers the "YahooBoys[20]," as young Nigerian conmen were dubbed, it's clear that online fraud was seen as a means of subsistence and that unemployment was crucial in drawing ever greater numbers of youth to cybercrime (Adeniran, 2008; Tade and Aliyu, 2011).

Internet fraud victim profiles

Online fraud has become a major problem in many countries, with victims numbering in the millions. Research often overlooks cyberfraud victims in comparison with other types of crime victims (Button, McNaughton Nicholls, Kerr and Owen, 2014).

This neglect may be due, in part, to the low reporting rates of online fraud. According to the literature, the explanations for these low reporting rates are the same as for fraud in the offline world: victims blame themselves for falling into a trap; they feel embarrassed; and they don't know where to file a complaint, especially when only a minor monetary loss is incurred.

What makes cyberfraud different, whatever particular form it takes, is that the victim is actively implicated in the commission of the act. This fact contributes significantly to the shame victims feel when they later ask themselves why they were so naive. Victims also tend to have a feeling of guilt as, in their view, they helped the conman to succeed (Burgard and Schlembach, 2013).

The majority of fraud victims are individuals. Private businesses are in second place, followed by governments (Carignan, 2015).

Regarding individual victims, although certain characteristics have emerged from the research on the subject, researchers have not identified a typical, generally applicable profile for online victims. This is due to the wide variety of types of internet fraud. Their efforts have, instead, focused on specific types of fraud with the object of analyzing the victimization risk factors specifically associated with different types of fraud.

Ryan, Lavoie, Dupont and Fortin (2011) identified certain sociodemographic characteristics of the victims and offenders involved in frauds committed on social media. They found that this class of fraud affects men and women equally. Victims are apparently older (average age: 33.3) than perpetrators. According to Reyns' study on identity theft (2013), men and older persons are more likely to be victims than women and younger persons. Higher income individuals are also more likely to be victims of identity theft than individuals with an annual income under $90,000 CAD.

Reyns' study (2013) also tested the applicability of Cohen and Felson's theory of routine activities. His results show that persons who use the internet for email or to send text messages and/or do online banking have a 50% greater risk of being victims of identity theft. Individuals who engage in online shopping and make downloads have a 30% greater risk of victimization. These results corroborated those of Koops and Leenes (2006) for whom all such routine behaviour patterns are risky activities which expose users to the threat of identity theft.

Van Wilsen (2013) studied consumer fraud by applying Gottfredson and Hirschi's theory of weak self-control. He found that persons with weak self-control are at greater risk of victimization.

It's worth noting, however, that many authors do not consider the routine activities approach to be the best general framework for studying online fraud. For them, research should instead continue to focus on identifying the risk factors most associated with this kind of crime (Ngo and Paternoster, 2011).

In addition, it's interesting to note that with online banking fraud there does not appear to be a pattern in terms of who constitutes the "ideal" victims. Whether one becomes a victim is, in a sense, a matter of happenstance and context. In effect, as conmen continually adjust their modus operandi as a function of events, this affects who they end up targeting. Of course, whether a cyberfraud succeeds or not also depends on gaining the trust of the "client" or taking advantage when the latter is not paying enough attention (Jansen and Leukfeldt, 2016).

As offenders rely more on social engineering than on their technical skills, there is limited scope for preventing this type of cybercrime using technological solutions. Consequently, the superior policy option, according to Ryan et al. (2011), is to educate users and raise their awareness with frequent public alerts on the risks of online fraud.

Finally, standardized data collection could facilitate the prevention efforts of anti-fraud organizations.

Cyberviolence

Box 3.5. **The hacking of intimate photos**

Christopher CHANEY

Between November 2010 and October 2011, a 35-year old American named Christopher Chaney used information available on the blogs of different celebrities to guess the passwords of their Google or Yahoo email accounts. He succeeded in hacking approximately 50 email accounts, including the accounts of Scarlett Johansson, Mila Kunis, Christina Aguilera and Renee Olstead. This gave him access to countless emails, photos and confidential documents.

Two women acquaintances were also victimized by his cyberattacks. In one case, Christopher Chaney sent his father intimate photos of a former colleague at work. This type of cyberviolence generally has very serious consequences for the victims. In this instance, one victim has been afflicted by deep anxiety and panic attacks ever since while the other has developed strong depressive tendencies and paranoia. According to these women, Christopher Chaney is a cruel and frightening man whose actions have caused irreparable damage to their lives.

Similarly, Christina Aguilera, Mila Kunis and Scarlett Johansson all agreed to publicly testify against this offender in the hope of raising public awareness about this kind of cyberviolence. Christina Aguilera acknowledged that no compensation will ever diminish the feeling of insecurity caused by this attack on her privacy. Scarlett Johansson spoke of the humiliation and shame felt when Christopher Chaney leaked nude photos of her. As for the actress and singer Renee Olstead, she testified in court that she had attempted suicide.

Although Christopher Chaney apologized for all of his actions and acknowledged a feeling of compassion for his victims, the facts revealed a man with a clear voyeuristic streak, aggravated by obsessive compulsive behaviour. In December 2012, he was sentenced to 10 years of criminal detention. According to U.S. District Judge S. James Otero, "these types of crimes are as pernicious and serious as physical stalking.

Research is beginning to focus on cyberviolence, particularly regarding how the internet is being used to facilitate these types of acts (Holt and Bossler, 2014). The popularity of electronic media in combination with the dizzying growth in mobile telephone use is increasing the risk of being involved in cyberviolence, either as a victim or as an offender (Smith, Mahdavi, Carvalho, Fisher, Russell, and Tippett, 2008; Holt and Bossler, 2014).

Wall (2001) defines cyberviolence as the online distribution of harmful, hurtful or dangerous material. As with other cybercrimes discussed above, cyberviolence is a generic category encompassing a variety of acts, including bullying and stalking (also called harassment). The latter two are the most frequently referenced, as well as the best documented (Holt and Bossler, 2014).

Dubé and Drouin (2015, as cited by Bernier, 2016) define cyberharassment as the utilization of information and communication technologies (ICTs) to establish virtual communication with another person, on an iterative basis, to commit repeated acts of psychological violence. Electronic harassment consists of threatening, insulting, harassing or hurting individuals via electronic means of communication such as email and cellphones (Beran and Li, 2005).

Cyberstalking can take the form of undesired sexual propositions, sexual harassment, voyeurism, obscene comments and spam (Behm-Morawitz and Schipper, 2015). One particular form which is becoming very common is "revenge porn." This consists of the online (and occasionally offline) dissemination or sharing of explicit images of an individual – without that person's consent – by his or her partner, ex-partner or by hackers (Hall, 2017).

Cyberbullying is defined as "any behaviour performed through electronic or digital media by individuals or groups that repeatedly communicates hostile or aggressive messages intended to inflict harm or discomfort on others" (Tokunaga, 2010). Cyberbullying can take various different forms, including direct aggressions, which entail the victim's participation, and indirect aggressions, which affect the victim in a more circuitous manner (Willard, 2005).

Willard (2005) identifies seven forms of aggression which may be associated with cyberbullying:

i. Online harassment involves sending multiple hurtful messages, via email or text messages, directly to the person targeted;

ii. Flaming consists of personal attacks, aimed at a person or group of persons on a social media, which are published to punish those holding a certain opinion rather than engage them in good faith debate;

iii. Putdowns involve the publication or sharing, with other persons on a given social media, of intentionally harmful or false material (false rumours, manipulated images, embarrassing video compilations, etc.) about the person targeted;

iv. Outing consists of making public – sometimes falsely pretending to do so inadvertently – private or embarrassing information (publication of personal contact info, compromising photos, revelation of a secret relationship, etc.) about the person targeted;

v. Cyberstalking occurs when an individual causes distress to the person targeted by repeatedly requesting the latter's attention in an inappropriate or undesired way or by monitoring his or her online activities with the goal of facilitating an encounter with the person targeted;

vi. Impersonation happens when the aggressor pretends to be someone else to spread harmful material or utilize the targeted person's identity to manipulate his or her social relations; and

vii. Exclusion is the unjust or unnecessarily cruel ejection of a member of an online group.

Welsh and Lavoie (2012) argue that cyberbullying and cyberharassment are variants of cyberharassment, with age as the parameter for differentiating between them. Thus, whereas cyberbullying describes a specific category of cyberharassment involving children and youth, cyberharassment per se applies to adults (Miller, 2006, Welsh and Lavoie, 2012).

Offender profiles

As with cyberfraud, the lack of face-to-face contact with the victim often leads to the latter's dehumanization. As a result, the aggressor allows him or herself to use far more extreme and offensive language (Bernier, 2016). Bullying implies a power relationship in which the bully dominates the victim. The internet's very structure and the anonymity that it affords (Bourque,

2012) are highly conducive to the proliferation of these kinds of power relationships. It has been shown, moreover, that this kind of power relationship is generally imposed by a social media "friend" rather than by a complete stranger (Mishna, Wiener & Pepler, 2008).

Cyberbullying mostly involves young adolescents. Furthermore, whereas traditional bullies are generally boys, in cyberspace girls apparently engage in bullying as frequently as boys do (Cappadocia, Craig and Pepler, 2013).

Getting even and letting off steam are the two principal motivations behind the various forms of cyberbullying (Shariff, 2009, p. 35).

Researchers have found an apparent connection between bullying behaviour and weak self-control. However, this connection does not appear to be as strong in cyberbullying as it is in traditional bullying (Kerstens and Veenstra, 2015). Individuals who participate in an act of cyberbullying experience a feeling of impunity. Nevertheless, it has been demonstrated that these young persons also show empathy.

Good computer skills as well as a knowledge of cyberspace are generally correlated with a risk of being a bully or harasser (Chehab, 2016).

Moreover, young bullies and harassers are apparently themselves victims of bullying and harassment, both online and offline (Kerstens and Veenstra, 2015). It's also worth noting that the quality of parental supervision influences the online behaviour of juveniles. Youth who regularly discuss their web surfing habits with their parents are half as likely to victimize their peers (Ybarra and Mitchell, 2004).

Finally, revenge porn is committed by individuals seeking to exercise power and control over their victims. The work of Hall and Hearn exemplifies a new research program that focuses on analyzing the characteristics of this type of offender. Their analysis indicates that, beyond vengeance as a justification for this kind of act, what is really at issue in such cases is a reaction to the emasculation men feel when they lose power in their relationship (Hall, 2017).

Victim profiles

More girls than boys are victims of some form of harassment during their online interactions (Cappadocia, Craig and Pepler, 2013; Wade and Beran, 2011). According to Holt and Bossler (2008), simply being a woman increases one's chances of being harassed online by 2.75 times and triples the risk of being the object of sexual advances.

Holt and Bossler (2008) sought, as did Reyns, Henson and Fisher (2011), to demonstrate that a number of connections can be made between the theory of routine activities and cyberstalking victimization. In effect, someone who spends a lot of time in online chat-rooms, and avidly uses social media and email, is a person who would constitute a "good" target, thereby satisfying one of the three factors necessary for the commission of a criminal act. Apparently, possessing IT skills is only a protective factor for men. Furthermore, anti-virus and other security software do not apparently guard against the risks of cyberstalking victimization as such software only serve to protect against attacks on one's computer. A woman who indulges in deviant behaviour online, such as hacking/software piracy, or has friends who do so, considerably increases her risks of falling victim to cyberstalking and bullying. Likewise, the risk also rises if one uploads photos online and adds unknown persons to one's social network profiles.

Cyberviolence, cyberstalking and cyberbullying have devastating impacts on victims' lives. Blaya (2011) reports that cyberviolence may have a more serious impact than traditional violence. In effect, because cyberstalking or cyberbullying can take place anywhere and at any time, one's home is no longer a safe refuge. Furthermore, the identity of an online bully or harasser is not necessarily known to the victim. As a result, the latter may live in constant fear of a possible encounter with this unknown bully or stalker. Victims of cyberviolence experience serious psychological consequences, including a greater risk of depression or suicide (Holt and Bossler, 2014).

There is a pressing need today to strengthen prevention of this type of crime. To that end, researchers must first assess the impacts of existing prevention plans (a subject which we will discuss in the next chapter).

Conclusion

The object of this chapter was to examine the current state of criminological research on cybercrime. A better understanding of the relevant personal and contextual risk factors is a prerequisite to more effective and better targeted prevention measures. First of all, we observed that although cybercrime is not a new reality, much research work is still needed to better understand this phenomenon – a phenomenon whose scope and the speed with which it emerged are such that they pose major challenges to both academia and decision-makers.

The first problem discussed was the lack of consensus on how to define cybercrime, an issue which has downstream implications for the entire research process. In effect, in the absence of a common definition for cybercrime in general, and for the various types of cybercrime in particular, different research studies will necessarily produce somewhat disparate data, which is problematic from the perspective of making evidence-based international comparisons. This lack of comparable evidence-based results does not in turn contribute to the development of efficient public policies or to the implementation of effective partnerships.

Furthermore, research is rather limited and largely confined to developed countries, despite the fact that internet use is now a truly global phenomenon (Carignan, 2015). Next, we observed that the current theories in criminology are principally based on sociological approaches, although there is an emerging body of research that draws more on psychology, but which is still in its early stages of development.

Finally, the three types of cybercrime studied in this chapter faithfully reflect the complexity of cybercrime issues. Given this complexity, it is very difficult, if not indeed nearly impossible, to identify specific profiles characteristic of either perpetrators or victims. Moreover, the risk factors associated with the internet (see box 3.6) only add to the difficulties intrinsic to research in this area.

The emergence of cyber criminology, defined as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space" (Jaishankar, 2007, p. 1), may contribute to remedying the various problems encountered by research on cybercrime today.

Box 3.6. **Internet risk factors (Koops, 2011, p. 740)**

1. The internet has a global reach, enabling perpetrators to look for the most vulnerable computers and victims anywhere in the world without having to leave home or the next-door Internet café (Yar, 2005, p. 421).

2. This leads to deterritorialization, which implies that cybercrime is almost by definition international, with consequent legal challenges of jurisdiction and cross-border co-operation.

3. The organization of cyberspace allows for decentralized, flexible networks in which perpetrators can (loosely) organize themselves to divide labour or to share skills, knowledge, and tools (cf. infra, section 3.3).

4. Cyberspace facilitates anonymity, at least for perpetrators who have the knowledge and make some effort to use anonymization tools (…). However, also less tech-savvy perpetrators are (or feel) relatively anonymous when they operate at a (large) distance from behind an IP number, email address, or scam Facebook profile that is often not easy to trace to a specific individual (Sandywell, 2010, p. 44).

5. The internet enables distant interaction with victims, removing potential social barriers that perpetrators face in physical, person-to-person interaction; cybercrime thus involves "anonymous, networked and rhyzomatic relations between perpetrators and victims" (Sandywell, 2010, p. 44).

6. The virtual environment facilitates manipulability of data and software with minimal cost (Sandywell, 2010, p. 44) because it is based on digital representation (allowing for copying without loss of quality, and altering without visible traces) and because the Internet was built as an open infrastructure with intelligence at the end points to foster innovation by end-users.

7. Moreover, this environment allows for the automation of criminal processes, where one piece of software launched on the Internet can replicate and attack millions of computers at the same time – but also over longer periods of time – and where basic software such as a sample virus can be easily customized by so-called "script kiddies" to create a new virus (Wall, 2007).

8. The question of scale is important as well, as cybercrime can blow up the scale of a crime from a minor nuisance, when taken as an isolated incident, to a major harm once it acquires a global and permanent reach (Franks, 2010).

9. Similarly, this explosion in scale allows for aggregation of a large number of insubstantial gains, for example, through "salami" techniques; this de minimis problem may be one of the biggest challenges of cybercrime since it reduces incentives to report, investigate, and prosecute the crime (Wall, 2007).

10. Cyberspace facilitates an information economy where information has become a valuable asset, both in the legal market and the black market (Wall, 2007, p. 32).

11. Cyberspace poses structural limitations to capable guardianship that can serve, in the real world, as a social or technical obstacle to the commission of a crime (Yar, 2005, p. 423).

12. Finally, the particularly rapid innovation cycles in cyberspace allow for new techniques and tools to be developed in short periods, which facilitates circumventing existing countermeasures and the creation of new vectors and criminal activities.

Contribution

Cyber Criminology and Space Transition Theory: Contribution and Impact

Karuppannan Jaishankar
Professor
Raksha Shakti University (Police and Internal Security University)
International Journal of Cyber Criminology
International Journal of Criminal Justice Sciences
India

Introduction

Cyber space has been exploited by many fields of study; however, criminology was too late to explore this space and address the new form of criminality called cyber crime. I found a new academic sub-discipline of Criminology called «Cyber Criminology» in 2007, with the launch of a journal; the International Journal of Cyber Criminology (www.cybercrimejournal.com). I academically coined the term «Cyber Criminology» and defined cyber criminology as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space" (Jaishankar, 2007a, para 1). As an academic discipline, cyber criminology encompasses multidisciplinary field of inquiry - criminology, sociology, psychology, victimology, information technology and computer / internet sciences. "At its core, cyber criminology involves the examination of criminal behavior and victimization in cyber space from a criminological or behavioral theoretical perspective" (Jaishankar, 2010, 2011; Ngo & Jaishankar, 2017, p. 4; Jaishankar, 2017).

Space Transition Theory of Cyber Crimes: A unique Theory to further the discipline of Cyber Criminology

There are many scholars who attempted to address the causation of cyber crimes with traditional theories such as Social Learning Theory, Routine Activities Theory and Drift and Neutralization theory. However, they were not fully successful in their explanation of cyber crimes, as the cyber space is altogether a new space and cyber crime is a new form of crime (Yar, 2005; Jaishankar, 2007b, 2015). The Space Transition Theory of Cyber Crimes (2008) was propounded by me because I found that there is no theory that is specifically created to address the causation of cyber criminality. I first presented this theory at the John Jay College of Criminal Justice, The City University of New York, USA, in 2007. Later, I published this theory as a chapter in a book titled «Crimes of the Internet» edited by Frank Schmalleger and Michael Pittaro (2008), and published by Prentice Hall, USA (Jaishankar & Chandra, 2017).

The Space Transition Theory of Cyber Crimes (2008) advances the field of Cyber Criminology. «Space Transition Theory" is an explanation about the nature of the behavior of the persons who bring out their conforming and non-conforming behavior in the physical space and cyber space (Jaishankar, 2008, pp. 292-296). Space Transition Theory argues that, people behave differently when they move from one space to another" (Jaishankar, 2008, pp. 292-296; Jaishankar & Chandra, 2017).

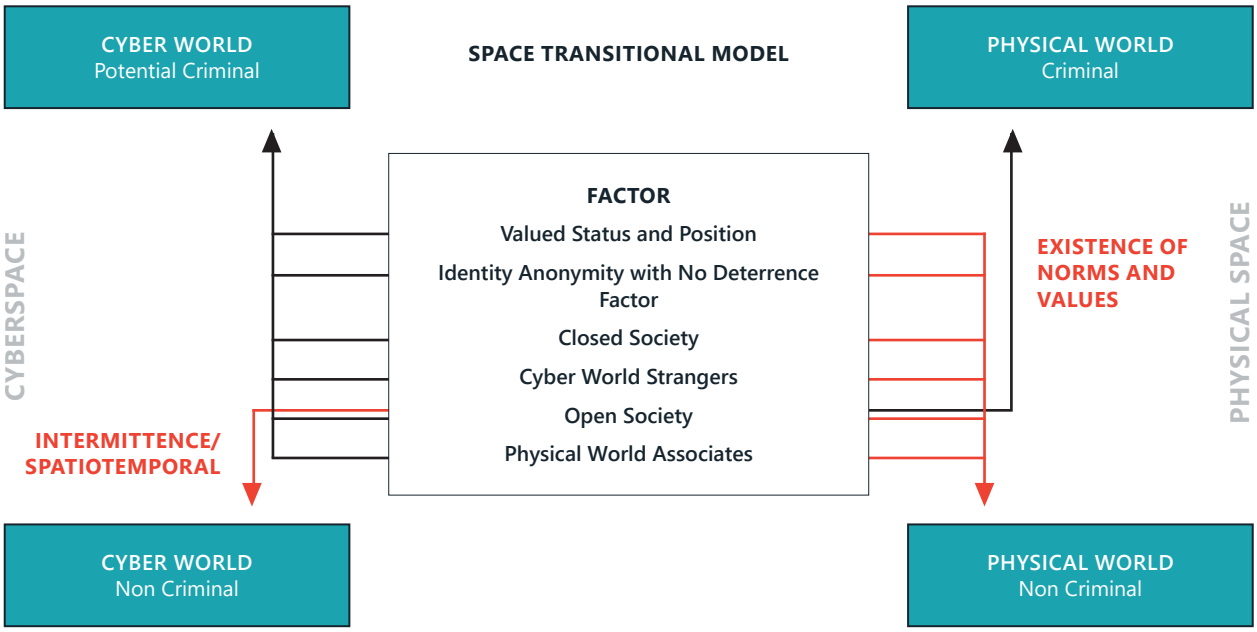
Propositions of Space Transition Theory (Jaishankar, 2008)

1. Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.
2. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime.
3. Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well.
4. Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.
5. (a) Strangers are likely to unite together in cyberspace to commit crime in the physical space. (b) Associates of physical space are likely to unite to commit crime in cyberspace.
6. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.
7. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cyber crimes.

Issues of Testing Space Transition Theory

This theory is empirically tested by few scholars: Zhang (2009), Danqua and Longe (2011) and most recently by Kethineni, Cao and Dodge (2017). Danqua and Longe (2011) tested the Space Transition Theory in Ghana. "They found that space transition theory is more applicable in cyber-trespassing, cyberdeception and theft, and cyber-pornography than cyber-violence (Kethineni, Cao and Dodge, 2017, p. 7). Kethineni, Cao and Dodge (2017, pp. 13-14) tested the space transition theory in their study and found some support. They mention: "The current study supports some of the theoretical explanations proposed by space transition theory. In particular, identify flexibility, dissociative anonymity, easy online association, and lack of deterrence bring more and more traditional criminals to the Internet.... Also, the notion that when there is a conflict between the norms and values of physical space, and the norms and values of cyberspace offenders choose cyberspace has been supported in this study" (Jaishankar & Chandra, 2017).

In spite of the fact that the space transition theory is tested by few scholars, there are some issues on the difficulty of testing this theory and it has been emphasized by several scholars (Holt, Bossler, & Spellar, 2015; Holt & Bossler, 2016). It is to be noted that getting data of the cyber crime offenders is an onerous task and hence the difficulty of testing the space transition theory



Source: Space Transition Model derived from Jaishankar (2008) by Danquah and Longe (2011)

ensued. Even, Kethineni, Cao and Dodge (2017, pp-13-14) note that: "Although the case studies provide some support for space transition theory, more data is needed to test all of the propositions empirically." Getting a large population of cyber offenders will be difficult at this stage and this issue may be settled in the future. Cyber crimes will grow further in the future and there will be thin line between offline and online offenders in the future and this will enable to get more cyber offender population and the testing of the space transition theory will be much more feasible than the present situation (Jaishankar & Chandra, 2017).

Also, space transition theory does not explain all forms of cyber crimes (Danqua & Longe, 2011; Jaishankar & Chandra, 2017). If a single criminological theory is not able to explain all forms of crime how a single cybercrime theory would explain all forms of cybercrime? I believe that space transition theory is only a starting point of theories on cyber crimes and in the future I expect more theories of cyber crimes to be created by scholars.

Conclusion

The growth of the field of Cyber Criminology is imperative as there is a surge of cyber crimes in the past decade. Bachmann (2008) emphasized that the growth of the field of cyber criminology is seen by two strong indicators. One, the launch of the exclusive journal, the International Journal of Cyber criminology in 2007 and two, the significant growth of scholarly publications in the form of books, journal articles and book reviews in the area of cyber crime/cyber criminology in the past ten years of the establishment of the field of cyber criminology by K. Jaishankar. Further, the Space Transition Theory of Cyber Crimes is "credited by many scholars (Diamond & Bachmann, 2015; Holt & Bossler, 2014, 2016; Holt, Bossler, & Spellar, 2015; Moore, 2012, Wada, Longe, & Danquah, 2012) as a noteworthy contribution to the field of criminology in general and cyber criminology in particular" (Ngo & Jaishankar, 2017, p. 5; Jaishankar, 2017).

Moore (2010) has dedicated a chapter on "Cyber Criminology" in his book titled "Cybercrime Investigating High-Technology Computer Crime". Stalans and Finn (2016, pp. 502-503) values: «The field is young, but has begun to amass scholarship on many forms of cyber crime, including book collections featuring research throughout the globe (e.g., Jaishankar, 2011; Kshetri, 2013; Wall, 2007) and nine (emphasis mine) reviews on the current state of knowledge» (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 and Jaishankar (2017, p. 5) feels that: "Advancing the field of cyber criminology is a salient and pertinent area of inquiry (Jaishankar, 2010) because unlike traditional crime or crime committed in the physical world, cyber crime or crime committed in the virtual world has the potential of causing tremendous damage, both tangible (i.e., economic loss) and intangible (e.g., the unauthorized use of personal data)." Moore (2012, p. 283) feels that: "There is no denying that this area of criminology (cyber criminology) is extremely exciting and certain to become a well-researched area of criminal behavior". Hence, it is envisaged that the field of cyber criminology will grow to a greater extent and there will be no more neglect or marginalization of mainstream criminology (Jaishankar, 2017).

Contribution

Violation by sexual image distribution, "revenge pornography", cyberabuses, and prevention

Matthew Hall
Ph. D, Associate Academic and Researcher
Ulster University, UK

Jeff Hearn
Professor Emeritus
Hanken School of Economics, Finland

Introduction

Violation by way of the distribution of sexual images or image-based sexual abuse or non-consensual "pornography", or more colloquially and simply, "revenge porn", entail the online, at times offline, non-consensual distribution, or sharing, of explicit images of someone else for seeking revenge, entertainment or political motives. Although male ex-partners are reported as the main perpetrators, current partners, (ex-)friends of both victims and perpetrators, people known to the victim, people seeking revenge for friends, internet hackers and trolls, amongst others, may also be involved (Tyler, 2016).

The negative impact it has on victims is significant and profound in terms of physical and psychological health and well-being, as with many other forms of gender and sexual violence and abuse. Victims report a host of negative effects: feelings of humiliation, shame, embarrassment and reputation damage with intimate partners, family, friends, work colleagues and, in public; sexual shame, sexual problems and body image issues with intimate partners; education and employment disruptions; becoming paranoid and hyper-vigilant, and concerned for personal safety. For example, some have reported being stalked, harassed and threatened with gang rape because of their personal information was also made public. Some victims have even taken their own lives (Citron & Franks, 2014).

Technology, image distribution and cyberabuses

The development of smartphones has facilitated an explosion in "sexting" – the sending of explicit sexually images by text message (Hasinoff, 2015). A survey of 5,000 adults (Match.com, 2012) found that 57% of men and 45% of women had received an explicit photo on their phone, and 38% of men and 35% of women had sent one. Once this happens, those seemingly 'private' pictures are potentially available for the world to see if uploaded, and shared, on the Web (Penney, 2013).

The sharing of explicit images of another on the Web without their consent is yet another part of the multifarious possibilities for virtual/online socialities, sexualities and violences, specifically cyberabuses – that is, intentional online behaviour to harm another, often repeatedly, where the victim is typically unable to defend himself or herself (Slonje, Smith & Frisén, 2013). The crux of cyberabuse is the imbalance of power and lack of consent, often facilitated by the perpetrator's ability to remain anonymous. Online abuses can take several forms such as cyberbullying, cyberstalking – the intent to threaten or induce fear in the targeted person by circulating or sending repeated messages and photos (often via hyperlinks to purpose-built revenge porn sites), online aggression, 'flaming[21]' , 'happy slapping[22]' , stalking and trolling (Hearn & Parkin, 2001). "Revenge porn" overlaps with and shares similarities with these forms of cyberabuses, such as posting explicit images or films along with offensive text carries with the intention to violate, harm, abuse or humiliate. These images or films may also be accompanied by abusive emails, 'tag-team-style pile-ons' in internet forums and personal attacks in blog and newspaper article comment sections (Svoboda, 2014, p. 48). "Revenge porn" can also share further features with other forms of cyberabuse, for example, intentional damage of someone's reputation by spreading malicious gossip, rumours or photos (these can also be digitally manipulated, as, for example, with 'deepfakes[23]'); and outing and trickery – the sharing of or tricking someone into revealing aspects of their private life, with the intent to embarrass them (Lacey, 2007).

"Revenge porn" exploits the many characteristics of ICTs and elaborates them in manifold ways, with open-ended and undefined possibilities and effects. ICTs bring a number of distinctive features to everyday life: time/space compression of distance and physical separation, instantaneousness in real time, asynchronicity, reproducibility of images, creation of virtual bodies, blurring of the 'real' and the 'representational'. More specifically, the affordances of computerised communication networks include broader bandwidth; wireless portability; globalised connectivity; personalisation (Wellman, 2001); and blurring, even the abolition, of strict boundaries between, between online and offline, codex and net (Gilbert, 2013). This raises complex issues, for example, how such violations can be simultaneously embodied and virtual. Itis not reducible to just one form or possibility, may be multi-medial, and may only be understandable in the context of a range of social practices beyond the visible and readable revenge porn text. For example, a particular posting may reference, implicitly or explicitly, another earlier topic or social occasion offline and off-screen, positive or negative, for one, both or more parties, which would not be decipherable by an uninvolved party or viewer. Specific instances may be part of a chain of events, occurrences, times and places. Moreover, revenge porn and related violations by sexual images can be seen in terms of the processual nature of the interactive web, in which 'produsers', 'prosumers' and other hybrids create the web interactively, sometimes for the assumed but unknown audiences (Whisnant, 2010), as evidenced in do-it-yourself pornography, selfies, celebrity selfies, naked selfies, reality media, online lives, neknominate (drinking) challenges, and the rest.

Combating violation by image distribution, revenge porn, and cyberabuses

Combating cyberabuses more generally should include matters of politics, policy, law, education, intervention, and support. For example, universal laws for convicting perpetrators of violation by image distribution and revenge porn do not exist. In many countries, the criminal legal frameworks are either non-existent or securing convictions is very difficult (Franks, 2016). Without international and cross-border laws, pursuing perpetrators and those who facilitate these crimes is likely to be very difficult (Topping, 2016). Much needs to be done to stop organisations which are hosting such sexual images and search engines that link to revenge porn and revenge porn sites. Arguably, stronger civil laws should also be in place so that victims can sue perpetrators for damages.

There is also a need to raise public and popular awareness of the potential risks of revenge porn that can follow from sexting, for example (Hasinoff, 2015). One method of doing so is to include this on educational curricula on sex and relationships. Charities and educational groups are reported to be concerned that many teenagers are not being taught about issues like sexting, online pornography, consent and healthy relationships, including the illegality of child sexting and revenge pornography. The primary focus of sex and relationship curricula tends to be on sexuality and health, and what constitutes a healthy relationship; this should include how to communicate online, and also deal with the ending of relationships, problem solving, and training on relationship skills and emotion regulation (Lundgren & Amin, 2015).

Many programmes to support victims of gender and sexuality-based crimes tend to focus on how to reduce the risk of revictimisation, such as social support and safety behaviours. However, most tend to focus on dealing with the legal process of bringing offenders to court, or the removal of the images. Yet, more needs to be done to help victims deal with the fallout. It would help therefore, if protocols of cooperation between relevant authorities and existing support services were strengthened to provide a range of emotional- and practical-based support service, and a web page could be developed for the dissemination of learning and support materials for victims, educators, agencies and the media.

Criminalisation of non-consensual distribution of sexual images and specifically revenge porn is likely to act as a deterrent for some, but not for others. Where legislation does not act as a deterrent, investigators can use software, such as EnCase, to produce an image of the alleged offender's hard drive to see deleted computer files, such as cache files, swap files, temporary files, unallocated space or slack space, and left traces of their browser history, address books, date and time stamps and so on to use as admissible evidence (Widup, 2014). Once convicted, and punished, re-education intervention may be one possible way forward for offenders, who are overwhelmingly male. Having said that, considerable caution is necessary around the likely success of such reforming interventions. This is partly because meta-analyses of evaluations of these kinds of interventions in stopping violence and violation in other contexts, notably 'domestic violence' and intimate partner violence, show mixed effectiveness (Wathen & MacMillan, 2003; Smedslund et al., 2007; Feder et al., 2008; Arias et al., 2013).

In combating these various and relatively newly developed forms of online and sexual image-based violations, key lessons from established offender interventions should be taken up, for example, feminist re-education group treatment focusing on (largely male) power and control (Eckhardt et al., 2013). Such approaches could be applied and modified in relation to preventing revenge pornography. Some fairly well-established methods have been developed in anti-pornography workshops and campaigns, such as various 'Men Against Pornography' groups, and these can be adapted in working with offenders, in the broadest sense of the word, against revenge pornography. Beyond those interventions, there is the array of specific methods and techniques for working with those who have committed crimes of sexual violence.

Concluding remarks

In short, in order to tackle violation by sexual image distribution, and cyberabuses more generally, we recommend four key responses to curb this modern-day phenomenon: First, there should be stronger civil laws in place so that victims can sue perpetrators for damages. Second, we need more international co-operation. That means cooperation between states to help with cross-border prosecutions, and make it easier to take down websites where images are posted; those that profit from this crime. The third response centres on support. Currently the focus is on bringing offenders to court, or the removal of the images, but more needs to be done to support victims, and in particular, how to manage the fallout from these crimes. And finally, educational programmes in schools and elsewhere need to be adapted to highlight the risks and potential consequences of taking and sending images. This problem is not going away. It is only through more action-orientated, multidisciplinary responses that we can help to remove the stigma and trauma this crime causes (Hall & Hearn, 2017).

Notes

16 Synoptic in that it enables one to have a complete vision at a glance and panoptic as it allows one to observe without being seen.

17 Etiology is the study of the causes of delinquency, be they individual, situational or contextual.

18 See the preceding section's discussion of economic theory.

19 A social psychology concept derived from LeBon's Psychology of Crowds (1895) and applied by Zimbardo (1973) in his celebrated Stanford prison experiment.

20 Nigerian scammers were given this nickname due to their abundant use of free email accounts in their commision of cyberfraud activities.

21 A hostile interaction between people on the internet often involving profanity.

22 A group of people film or photograph, and then circulate online, their assault of a person.

23 The use of technology to combine and superimpose an image or video of person onto another person's image or video to give the impression that it is of that person.

References

Chapter 3. Cybercrimes, cyberriminals and cybervictims

Adeniran, A.I, (2008). The internet and emergence of yahooboys 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). Retrieved from 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 delinquen-

cy. 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

Cyber Criminology and Space Transition Theory

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.

Violation by sexual image distribution

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

CHAPTER 4

CYBERCRIME PREVENTION APPROACHES

Today, cyberspace is the subject of theoretical and practical debates in relation to crime prevention. A number of governments use the terms cybersecurity and cybercrime interchangeably and focus their efforts on protecting critical information infrastructure at the expense of much needed preliminary reflection on crime prevention in cyberspace. The object of this chapter is to take a fresh look at the principal developments in traditional approaches to crime prevention – i.e., the developmental, environmental and partnership approaches – in this new context. To that end, it begins by clearly differentiating between cybersecurity and cybercrime, both conceptually and operationally. Finally, in this chapter we analyze the application of these traditional approaches, based on the different measures taken to prevent some of the most frequently cited crimes in international conventions, namely cyberbullying, online sexual exploitation of minors, and cyberfraud.

Introduction

Crime prevention is concerned with the ability to stop crimes before they are committed (Pelser, 2002). In other words, prevention refers to the strategies and measures designed to reduce the risk of crimes occurring (UNODC, 2010). As we saw in the preceding chapter, clearly identifying the risk factors that bear on cybercrime still remains a challenge (Bossler & Holt, 2016). These gaps in our knowledge, accompanied by the virtual absence of the State in the development of prevention measures, give rise to abundant crime opportunities and leave private businesses and citizens largely responsible, by default, for their own security. This situation is effectively transforming cyberspace into a new Far West (Ghernaouti, 2013; Kigler, 2016; Williams & Levi, 2017). Not only are responses lagging, but due to its intrinsic characteristics – i.e., its speed, potential reach and decentralization of interactions – cyberspace simplifies the commission of certain traditional crimes, particularly in light of generalized internet use in the legal economy (Rivière & Didier, 2008) (see chapter 2).

And yet, as the UN's Handbook on the crime prevention guidelines make clear: "it is the responsibility of all levels of government to create, maintain and promote a context within which relevant governmental institutions and all segments of civil society, including the corporate sector, can better play their part in preventing crime" (UNODC, 2010, p. 29). Although cybersecurity strategies do include aspects characteristic of a prevention-based approach, it is our contention that these measures are insufficient given the magnitude of the phenomenon. In effect, today's proliferating cybersecurity strategies largely concentrate on protecting critical information technology infrastructure and/or focus on organized crime (Seger, 2012), to the detriment of preventive measures.

With a view to testing this hypothesis, this chapter will first undertake to clearly distinguish between cybersecurity and cybercrime. The value of this initial discussion lies in its clarification of the issues bearing on the creation of a real cybercrime prevention strategy. Next, we will consider the principal international and regional conventions and strategies to provide an overview of the issues, in terms of the types of crime targeted by said strategies, and the principal recommendations security and prevention in cyberspace put forward by the international and regional organizations concerned. Based on the issues identified in this overview, we will then do a brief review of the prevention measures that have been evaluated and which are the most frequently cited in the literature. Next, based on these measures, we will consider the applicability of traditional crime prevention theories in the context of cyberspace. The objective of this exercise in analysis and synthesis is to produce an accurate picture of the current state of prevention in cyberspace, both in operational and theoretical terms, in order to facilitate and stimulate reflection and recommendations on the development and implementation of a real cybercrime prevention strategy.

Part I - Cybercrime and cybersecurity

As we clearly saw in the preceding two chapters, the democratization of internet use has brought about major changes in traditional behaviours in society, notably in the ways we search for and/or share information, which, in turn, effects our daily activities and interpersonal relations (Lewis & Lewis, 2011). However, this new space has not only transformed customary norms in human interactions, but it has also given rise to its share of new risks, particularly in terms of security.

The notion of cybercrime

The Budapest Convention (Council of Europe, 2001) is one of the sole legally binding international conventions which directly addresses cyberspace security and cybercrime prevention (Jamil, 2014). It defines cybercrime in the following two ways:

1. Offences against the confidentiality, integrity and availability of computer data and systems, that is, offences against computer data and systems, including illegal access, illegal interception, data and system interference, misuse of devices;

2. Offences committed by means of computer systems. This list is limited to those "old" forms of crime that obtain a new quality through the use of computers, that is, computer-related forgery and fraud, child pornography and offences related to infringements of copyright and related rights on a commercial scale.

The preceding chapter also clearly showed that the definition of cybercrime remains a subject of major debate, around which an international consensus is, as of yet, far from forming. However, for the purposes of this chapter, we will use an operational definition of cybercrime, which shall be "understood as offences not only against but also by means of computer systems causes major damage to societies" (Seger, 2012, p. 21).

Notwithstanding the place accorded to traditional crime in the Council of Europe's definition, to a very large extent, current research, national strategies and, as we shall see, international and regional initiatives are rather more interested in the security of information technology infrastructure, citizen self-regulation, legal responses and law enforcement – to the detriment of concrete cybercrime prevention measures (Seger, 2012). This leads us to commence by distinguishing between the approaches focusing on cybersecurity and those addressing the issue of cybercrime.

The 2007 cyberattacks in Estonia represented a historic turning point in terms of cyberspace security issues. They had a global impact in terms of the implementation of cybersecurity-centric strategies. In effect, since 2007, cybersecurity has become increasingly important on political agendas worldwide. The risks associated with multiple cyberattacks and the potential targets thereof are topics of regular discussion. The concepts of cybersecurity, cybercrime and cyberdefence are presently "employed interchangeably without precise definitions based on existing laws or legal concepts" (Pereira, 2016, p. 388). However, as the objectives of these two approaches are fundamentally distinct, they necessarily generate different outcomes.

Box 4.1. **Cyberattacks in Estonia in 2007**

In 2007, Estonia was struck by a wave of cyberattacks affecting many commercial and government servers, which threatened the confidentiality, integrity and availability of the data stored on them. Nearly 11 years later, no state or non-state group has ever claimed responsibility for these attacks. This unprecedented wave of cyberattacks subsequently led to the creation of numerous cybersecurity strategies worldwide (Haataja, 2017).

Approaches to cybersecurity

Les approches visant la cybersécurité, que nous appellerons Approaches that focus on cybersecurity, which in this chapter, we will call **cybersecurity strategies**, have as their objective ensuring the confidentiality, integrity and availability of information technology infrastructures. Such strategies are not concerned with the entire range of crimes committed in cyberspace, but rather focus on issues connected with the protection of personal and private data (Seger, 2012) (see the preceding chapter) and the reduction of risks connected with cyberattacks committed by other states or non-state groups against a given state's critical information technology infrastructure (CITI). As cybersecurity strategies prioritize the security of critical information technology infrastructure, they accord greater importance to public-private partnerships (Seger, 2012) (see chapter 5). Finally, such strategies are usually managed, both at the operational level and in terms of implementation, by public institutions answering to the Ministry of Defence or National Security, in partnership with the Ministry of Justice (Seger, 2012).

Approaches to cybercrime prevention

In contrast, cybercrime strategies focus on crime prevention and criminal justice. In effect, the difference between the two types of strategies replicates the dichotomy between security-oriented approaches vs. prevention-based approaches found elsewhere in criminology[24]. Traditional crime is, therefore, the subject of strategies that we will call **cybercrime prevention strategies[25]**. As we saw in our review of policy initiatives, many of the measures designed to prevent cybercrime consist of public awareness programs, public-private partnerships, international cooperation and deterrence-based approaches entailing the enforcement of increasingly severe punitive measures (ITU, 2014). Although punitive measures do not emphasize prevention, as opposed to punishment (ITU, 2014), and a large proportion of cybercrime incidents do not result in criminal convictions (Broadhurst, 2005), the consensus around the most appropriate preventive measures in the context of cyberspace remains quite weak (Broadhurst, 2005). Such measures may run the gamut from technical solutions, such as antivirus software, to the blocking of access to illegal content (ITU, 2014).

Table 4.1. **Differences between cybersecurity strategies and cybercrime strategies**

Cybersecurity strategies *National interest and national security, trust, resilience, reliability of information technologies*		**Cybercrime strategies** *Rule of law, human rights, crime prevention and criminal justice*	
Unintentional security incidents	Intentional attacks against the confidentiality, integrity and availability of computer systems and data	Infractions committed with the use of a computer and/or affecting content on computer systems	Any infraction involving the use of digital evidence

Source : Seger (2011)

Part II - Trends in cybercrime prevention

In Part II, we will outline the principal measures implemented to prevent cybercrime with a particular emphasis on international and regional initiatives, as well as on specific prevention programs.

International initiatives

At the **12th United Nations Congress on Crime Prevention and Criminal Justice**, two issues were underscored by participants, namely the magnitude of the economic and human damage caused by the commission of criminal acts by means of new technologies and the cross-border nature of these crimes. Two recommendations were formulated in response to these two issues: 1) raise public awareness and reaffirm the role of schools; and 2) improve cooperation among law enforcement and criminal justice authorities at the international level.

1. In effect, educational campaigns in **schools** and **public awareness campaigns** were cited as particularly cost-effective means for addressing prevention and criminal justice issues with youth, particularly regarding **cyberbullying**, and for raising the community's awareness of the risks associated with the utilization of the new technologies (CCPCJ, 2010).
2. Furthermore, many participants also stressed the importance of fostering greater **international cooperation** to combat cybercrime, particularly among **law enforcement and criminal justice authorities**. Other participants raised the importance of developing partnerships with the **private sector**, in conjunction with a global action plan for building technical capacities in terms of prevention, detection, investigation and the criminal prosecution of cybercriminals (CCPCJ, 2010).

In the same vein, the survey conducted by the **Commission on Crime Prevention and Criminal Justice (CCPCJ)** on the issue of cybercrime, and the responses thereto from Member States, the international community and the private sector (2013), identified the following aspects as crucial for cybercrime prevention: a) the promulgation of legislation to regulate the problem and provide a framework for policy measures; b) effective leadership; c) developing and/or building the capacities of the criminal justice and law enforcement authorities; d) public awareness and strengthening the role of education in prevention; e) developing a strong knowledge base on cybercrime-related issues; and f) increased cooperation between government, communities, the private sector and internationally (UNODC, 2013). Furthermore, nearly 70% of this survey's respondents indicated that public awareness, international cooperation and building the capacities of law enforcement agencies were key components of their respective national strategies (UNODC, 2013). Finally, the Commission observed that the **safety of young people, critical information technology infrastructure (CITI)** and **personal data** were often the pivotal concerns of these strategies (UNODC, 2013).

The **Doha Declaration (2015)** also calls for the development of special measures for the prevention of certain crimes committed in cyberspace, such as the **online exploitation of children,** notably by "identifying and protecting victims by, inter alia, removing child pornography, in particular child sexual abuse imagery, from the Internet" (UNODC, 2015). To that end, the declaration recommends the strengthening of **cooperation among law enforcement agencies**, nationally and internationally, as well as **building the technical capacities** of these same actors (UNODC, 2015). As we saw in Chapter 1, the Doha Declaration is a very far-ranging document that goes well beyond the issues specific to cyberspace. Without dwelling on the point, it is worth noting, however, that although not all of the declaration's recommendations concern cyberspace-related issues, this does not mean that they have no bearing on our analysis, as we shall see below.

Recent declarations and reports produced by UN Member States and groups of UN mandated experts (CCPCJ, 2010; UNODC, 2013, 2015) indicate that the international community intends to prevent cybercrime – with the main priorities being cyberbullying, the online sexual exploitation of children, and the protection of CITI and personal data – by means of public awareness campaigns, education, partnerships with the private sector, international cooperation among law enforcement and criminal justice authorities, and capacity-building targeting these same actors. In order to deepen our understanding of the role that states intend to play in cybercrime prevention, our review of these initiatives will now focus on the positions adopted at the regional level. In other words, we will now examine the objectives set by various regional declarations, conventions and strategies on cybercrime prevention.

Regional initiatives

As noted above, the Budapest Convention (Council of Europe, 2001), also known as the Convention on Cybercrime of the Council of Europe, is the sole binding international instrument pertaining to cybercrime. Moreover, the convention has the status of a founding text. As such, it has served as the basis for the national strategies of a number of countries. Its principal objective is to foster the **harmonization of national legal frameworks** around common legal definitions with the object of protecting the population against cybercrime and developing **cooperation between countries** to facilitate investigations and legal proceedings, notably through the sharing of crime evidence/data relevant to investigations (Council of Europe, 2001). Strengthened in 2004, by the "Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems," the Convention's priority concerns are **cyberfraud**, the **online sexual exploitation of children, cyber hate crimes, intellectual property offences** and the s**ecurity of computer networks** (Council of Europe, 2001, 2004).

In 2004, in Buenos Aires, the member states of the Organization of American States jointly recognized, for the first time, the scope of the issues and threats confronting the critical information technology infrastructures of their respective countries and the importance of joint action, based on intersectoral and international cooperation between the region's different governments. This realization led to the adoption of the **2004 Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity**, in which member states agreed to develop:

> "(…) a culture of cybersecurity in the Americas by taking effective preventive measures to anticipate, address, and respond to cyberattacks, whatever their origin, fighting against cyber threats and cybercrime, criminalizing attacks against cyberspace, protecting critical infrastructure and securing networked systems."(OEA, 2004, p. 6)

To that end, the joint declaration (2003) encouraged member states (OEA, 2004) to:

a) foster public-private partnerships with the goal of increasing education and public awareness;

b) identify and evaluate the best technical standards and practices in relation to the security of critical information technology infrastructure (CITI);

c) foster the adoption of policies and laws to protect internet users and deter the criminal misuse of computer networks; and

d) create computer emergency response teams (CERTs) to ensure rapid response in case of incidents.

The **Commonwealth Secretariat** encourages Commonwealth member states to develop policy responses on securing CITI, cybercrime prevention, investigation and criminal prosecution. The Secretariat also recommends the development of partnerships between the public and private sectors, as well as with other Commonwealth governments, particularly for the purposes of capacity-building and sharing best practices on cross-border criminal investigations and prosecutions. The Secretariat also recommends the development of national strategies with specific measures for cybercrime prevention, raising public awareness, inter-agency coordination, the allocation of appropriate resources to the criminal justice system, the creation of national and/or regional CERTs, as well as mechanisms and protocols for cooperation with internet providers and the private sector as a whole. Finally, particular emphasis was placed on cooperation with civil society and the private sector to develop training programs to enhance technical capacities (Commonwealth Secretariat, 2014).

Cognizant of member states' lack of resources (both technical and human) and that their respective national legal frameworks are not harmonized in relation to cybercrime, the Caribbean Community has integrated into its **CARICOM Crime and Security Strategy (CCSS 2013)** a series of cybercrime-related recommendations, including: the creation of CERTs; the development of public awareness campaigns and educational materials on internet use; capacity building for police officers, judges, prosecutors and medical-forensic professionals; the creation

of regional centres of excellence and a CARICOM Cyber Crime Centre; and the development of partnerships and programs with the private sector (CARICOM, 2013).

Box 4.2. **Issues of concern to small States**

In its report, the Commonwealth Secretariat observed that small countries are less likely to dispose of the technical and policy expertise required to develop effective long term responses for combatting cybercrime. In effect, small states often face critical shortages of qualified human resources, be they administrative, academic or entrepreneurial, as well as infrastructure-related deficiencies. These issues pose multiple challenges in terms of developing prevention initiatives, which must therefore be met through greater international and/or regional cooperation with states that possess the necessary technical and scientific capabilities (Commonwealth Secretariat, 2014).

The **African Union Convention on Cyber Security and Personal Data Protection (2014)** calls on member states to develop national strategies which address the following needs: a) raising public awareness; b) building capacities; c) creating public-private and international partnerships; and d) developing measures for curbing cybercrime and promoting cooperation in investigations, prosecution and restorative justice (African Union, 2014). Under the Convention, member states also undertake to promote a culture of security among all stakeholders – be they government agencies, private businesses or civil society entities – by emphasizing the safeguarding of critical information technology infrastructure (CITI), as well as awareness campaigns targeting small businesses, schools and children to encourage safe practices. With regard to information sharing, the Convention urges member states to set up CERTs or Computer Security Incident Response Teams (CSIRTs).

In its report entitled Recommendations on Cybersafety and Combating Cybercrime in the Arab Region (2015), the **Economic and Social Commission for Western Asia (ESCWA),** encourages the region's states to develop measures to raise public awareness, as well as create specialized institutes and offer technical courses to build the capacities of judges, investigators, police officers and other law enforcement professionals. The Commission also recognizes the importance of strengthening regional and international cooperation, and of implementing CERTs to safeguard CITI. Finally, the Commission also recommends the development of partnerships with civil society and the private sector, notably to encourage information sharing, as well as the collective shouldering of the financial and development costs of technical solutions (ESCWA, 2015).

The **2017 ASEAN Declaration to Prevent and Combat Cybercrime** prioritizes the harmonization of legal frameworks and evidence gathering practices. The Declaration also calls on member states to develop their own national action plans and to cooperate in sharing technical expertise, information and good practices, as well as in building the technical capacities of education sector professionals and the civil service. Finally, the Declaration also recommends the development of education and community awareness programs on the risks of cyberspace (ASEAN, 2017).

As we've just seen, **public awareness campaigns** seem to be one of the most widely used prevention tools by governments, and this is the case despite our limited knowledge regarding their effectiveness (Williams & Levi, 2017). In addition, it's clear that much importance is given to the development of **public-private partnerships**, at the national level. Likewise, partnership is also encouraged between **law enforcement agencies**, at the international level. It is also apparent that importance is accorded to the harmonization of legal frameworks and the development of technical capacities, principally to strengthen the detection, investigation and criminal prosecution of cybercrime. In this regard, the International Telecommunication Union (ITU) states that a significant proportion of the measures put forward in national strategies are confined to deterrent-based approaches, consisting of the enforcement of punitive and, indeed, increasingly severe measures, on the one hand (ITU, 2014), and measures aimed at reducing crime opportunities on the other (Reyns, Randa, & Henson, 2016). Finally, the potential role of **CERTs** is touted by most recommendations at the regional level.

Preventing cyberbullying, online sexual exploitation of minors and cyberfraud

In this section, we will address specific measures concerned with preventing cybercrime, particularly offences targeting persons. In the preceding chapter, we specifically referenced three types of cybercrime: computer hacking, cyberfraud and cyberviolence. However, as we've chosen to focus here on cybercrime rather than on cybersecurity, this section will not discuss the subject of hacking, which is only addressed by means of cybersecurity-oriented approaches.

The following discussion will therefore focus on three types of cybercrime: a) cyberbullying; b) the online sexual exploitation of minors; and c) certain economic crimes, in particular cyberfraud. As we've already seen, it is in order to combat these three types of crimes that the international community encourages the adoption of preventive measures (CCPCJ, 2010; UNODC, 2013, 2015).

a. Preventing cyberbullying

As we explained in the introduction, cyberspace provides an impression of relative anonymity, which is conducive to the expression of violent behaviour against others, without fears of immediate retaliation by a third party (Notar, Padgett, & Roden, 2013; Snakenborg, Van Acker, & Gable, 2011). Cyberbullying essentially consists of recourse to a digital communications medium, by an individual or a group, for the purposes of sharing information that

a reasonable person would deem as hurtful, vulgar, threatening, embarrassing, frightening, etc.

In general, international and national responses advocate some form of universal or primary prevention. More specifically, such responses focus on raising the awareness of parents, education sector professionals and students to promote safer internet use. According to Williams and Pearson (2016) many American and British organizations make the following recommendations to young internet users: make use of the available privacy settings, report incidents to adults, save evidence of acts of cyberbullying instead of deleting them, and avoid responding or reacting to cyberbullying. Likewise, the authors encourage adults to report these acts to internet providers, schools and, as the case may be, the social media in question (Williams & Pearson, 2016).

Increasingly, schools everywhere are developing cyberbullying prevention initiatives. However, these mostly consist of organizing awareness raising activities with educational videos or developing a code of conduct intended to foster getting along based on non-conflictual relations (Snakenborg et al., 2011). However, there are other approaches employed in school environments, which are evidence-based and go much further, including a) iSAFE, in the United States; b) KiVa in Finland; c) ConRed (Program for Knowing, Building, and Living Together on the Internet) in Spain; d) No Trap in Italy; and e) ViSC, in Austria. As these programs produce positive outcomes, they are frequently mentioned in the literature (Chisholm, 2014; Espelage & Hong, 2016; Notar et al., 2013; Slonje, Smith, & Frisen, 2013; Snakenborg et al., 2011).

a) The iSAFE program is designed for students in their final year of high school, parents, teachers or community leaders (Snakenborg et al., 2011). The course is comprised of five 60-minute workshops, which address the topics of online security, citizenship in cyberspace, personal safety, intellectual property and law enforcement in the virtual environment (Espelage & Hong, 2016).

b) KiVa is a holistic school program, which combines universal and customized developmental prevention targeting children aged 7 to 15. This program requires the participation of teachers, parents, community leaders and students (Espelage & Hong, 2016). Teachers are provided with an instruction guide, plus a video game designed for primary school pupils and an internet forum for youth at the secondary school level (Espelage & Hong, 2016). One of the objectives of these tools is to make youth aware of the consequences of cyberbullying and encourage them to support young bullying victims (Slonje et al., 2013). The program demonstrated positive outcomes during a large scale study (with a control group) conducted in nearly 90% of the schools in the Finnish school system. One of KiVa's main findings was the importance of the role played by witnesses in the bullying process (Hutchings & Clarkson, 2015).

c) ConRed is an evidence-based intervention program, which focuses on aspects such as the anonymity of bullies, the scope of the bullying problem and the suffering that victims experience (Ortega-Ruiz, Del Rey, & Casas, 2012). The approach followed by Ortega et al (2012) consists of four components: 1) the development of proactive prevention practices, procedures and strategies with the objective of implementing a specific action plan for combating the risks associated with internet use and social media, building the capacities of practitioners and developing self-regulation techniques; 2) developing the knowledge and skills of education sector professionals using tools which facilitate the acquisition of necessary problem identification, prevention and intervention skills; 3) the development of a safe school environment by facilitating communication among students, and promoting a culture of support, mutual respect and empathy with their most vulnerable classmates; and 4) the development of school-family-community partnerships to promote collaboration between education professionals, parents and community organizations, with the goal of reducing problematic behaviours.

d) The No Trap or le Let's not fall into the trap! is a program that seeks to prevent and combat both bullying and cyberbullying. Launched in 2008, the program is composed of two distinct phases. The first phase is managed by researchers in psychology, while the second is run by a group of students acting as positive peer leaders. The latter receive training on how to act as change agents in the virtual world using tools designed to raise awareness, as well as how to play a supportive role with classmates, in a person-to-person context. To be more specific, these leaders organize cooperative activities with classmates, which emphasize empathy, problem resolution and the responsibilities of persons who witness bullying. According to the authors of these programs, the recommended age for participants is 14-15, because, they argue, the risk of dropping out is much greater in that age group (Palladino, B.E., Nocentini, A. and Menesini, E. 2016).

e) e) Finally, ViSC is a program designed to prevent violence and promote the development of social skills in secondary schools. The program envisages three interventions levels: the school, the classroom and the student. In this so-called cascade model, the practitioner applies the program in accordance with the intervention level. The program is targeted at teachers and school psychologists. From 2008 to 2011, thirty-six (36) Austrian practitioners were trained. According to the assessment conducted in 2012 by Strohmeier et al positive effects were observed in the test group, in comparison with a control group (Spiel, C., Wagner, S., et Strohmeier, D., 2012).

Box 4.3. **The role of health sector professionals**

Cyberbullying is often considered a criminal justice and education sector problem (Moreno & Vaillancourt, 2016). However, increasingly, health care professionals are being asked to participate in interventions aimed at preventing cyberbullying (Espelage & Hong, 2016). In effect, by the very nature of their roles, doctors, nurses, psychologists and social workers are in a position to be

more active in identifying and preventing cyberbullying (Dale, Russel, & Wolke, 2014). Some researchers go so far as to affirm that health care professionals should ask youth directly whether they are bullying victims, and if so, since when, where does it happen, and how does it affect the young person's daily life (Espelage & Hong, 2016). Moreover, these kinds of interventions warrant consideration, reflection and analysis within the broader context of public health initiatives (Dale et al., 2014), in partnership with education sector professionals (Moreno & Vaillancourt, 2016).

b. Prevention of online sexual exploitation of children

Child sexual abuse (CSA) is an umbrella term that encompasses all forms of sexual abuse, violence, and exploitation directed toward children and youth through which an individual (usually an adult) can achieve sexual gratification or financial gain (IHE, 2010). Moreover, this social ill is encouraged by stereotypical images propagated in the media, which include the sexualization and domination of children and women, particularly in video games, advertising and television programs, as well as in legal pornography, which also feeds on these same stereotypes (Prevention Institute, 2009).

In its report Child Safety Online (2015), the UK Council for Child Internet Safety recommends better management of the personal content published on social media, the strengthening of internet security and privacy settings, and adjustments to parental controls to protect minors from contact with illegal content. Should a non-consensual dissemination of images occur, the Council offers the victim support from an expert team, envisages recourse to technologies such as PhotoDNA and contacts the relevant actors such as the Internet Watch Foundation to facilitate the elimination of the illegal content in question. Finally, the Council also recommends raising the awareness of both parents and education professionals through public awareness campaigns developed with the support of experts to ensure that different communities are reached (Williams & Pearson, 2016).

Combating these crimes requires a comprehensive approach with the backing of different national and international legal frameworks (ICMEC & UNICEF, 2016). Under a comprehensive approach, it is understood that the strategies developed at each level of government are necessarily multisectoral and multidisciplinary. In other words, the literature recommends that these strategies include the participation of the criminal justice system, child protection services and the IT sector. In addition, such strategies require the implementation of developmental, environmental and partnership-based prevention measures (ICMEC & UNICEF, 2016; IHE, 2010; LIBE, 2015).

In the context of sexual exploitation, developmental measures mainly consist of awareness raising activities, capacity building and support programs for the victims of criminal acts, as well as recidivism prevention programs. Regarding environmental measures, the literature references in particular the shutting down or blocking of sites hosting illegal content and the importance of parental control. Finally, with regard to partnership-based prevention, the emphasis is instead on developing programs designed to address the risk factors associated with sexual exploitation, as well as on imposing accountability on the pornography industry and web hosting providers.

Raising the awareness of youth, parents and other concerned actors

First of all, raising awareness about sexual exploitation among youth, parents and other concerned stakeholders, particularly education professionals, web hosting providers, internet providers and representatives from the media (LIBE, 2015), is a basic recommendation enshrined in the majority of international conventions (ICMEC & UNICEF, 2016). The main object of such awareness raising activities is to foster responsible internet use, in particular by providing information on how to identify clues that indicate exploitative situations (Simantiri, 2017), by helping users to develop self-regulation techniques, and finally, by reminding each user of his or her own responsibilities (LIBE, 2015). For example, the Canadian Centre for Child Protection teaches children and adolescents how to develop safe online behaviour, by reducing their vulnerability and by strengthening their resilience. The program is evidence-based and includes information on dating relationships, and the risks connected with internet use and the uploading of personal content (IHE, 2010).

Development of customized programs for victims and offenders

The Committee on Civil Liberties, Justice and Home Affairs of the European Parliament recommends that victims be identified (2015). In effect, as this committee explains victim identification – or that of potential victims – would enable policymakers and concerned organizations to develop customized support programs (LIBE, 2015). Similarly, looking beyond penal sanctions, the Committee also underscores the need to develop support programs for offenders (Simantiri, 2017), as well as for individuals who have verbalized their intentions before they actually take action, as per the following recommendation of European Union Directive 93 (2011):

> In order to prevent the sexual abuse and sexual exploitation of children, intervention programmes or measures targeting sex offenders should be proposed to them. Those intervention programmes or measures should meet a broad, flexible approach focusing on the medical and psycho-social aspects and have a non-obligatory character. Those intervention programmes or measures are without prejudice to intervention programmes or measures imposed by the competent judicial authorities (Directive 2011/93/UE, no. 37).

Thus, in Austria, for example, there exists a network of monitoring centres for men who fear they are at risk of committing a sex offence against a minor. Other programs, such as LIMES, offer

screening services, individual and group therapies, as well as psychological services for men who have never committed sex crimes against minors, but have expressed the desire to do so. In the same vein, the Sexpo Foundation in Finland provides a prevention program for individuals who have committed sex crimes against minors or are afraid of doing so. This program includes a free hotline and therapeutic monitoring (LIBE, 2015).

Parental control, self-regulation and shutting down of sites hosting illegal content

From the vantage point of environmental prevention, crime opportunity theory encourages us to consider the different mechanisms for making illegal content inaccessible to the general public, at least until such materials can be permanently eliminated (Prevention Institute, 2009). Thus, according to the European Union:

> To combat it, it is necessary to reduce the circulation of child sexual abuse material by making it more difficult for offenders to upload such content onto the publicly accessible web. Action is therefore necessary to remove the content and apprehend those guilty of making, distributing or downloading child sexual abuse images (Directive 2011/93/UE, no. 46)..

Parental control apps, along with age appropriate privacy settings, are technological tools which can enhance child safety in cyberspace (LIBE, 2015).

Role of industry, internet providers and web hosting providers

The pornography industry's role in normalizing sexual violence and sexual exploitation is widely recognized today, as is the media's (MacKinnon, 2005; Prevention Institute, 2009; Sun, Bridges, Johnson, & Ezzell, 2016). In this regard, the Prevention Institute's recommendation to the pornography industry (2009) is that it cease the sexual objectification of adolescents and children. Likewise, its recommendation to the media is that it end advertising which depicts sexualized youth.

Moreover, the International Telecommunication Union recommends that governments broaden the mandate and scope of the regulatory agencies responsible for information and communication technologies (ICT), particularly in relation to consumer protection, cybersecurity and the public's participation in the development and implementation of public policies adapted to the conditions of cyberspace (ITU, 2014).

c. Cyberfraud prevention

As we explained in the preceding chapter, fraud is a protean multifaceted phenomenon, which one might define as "a request made under false pretences to obtain a financial gain" (Prates, Gaudreau, & Dupont, 2013) and/or tangible assets. As we've already noted, research on prevention is largely based on routine activity theory and rational choice models. As a result, most of the prevention measures proposed to date are premised on situational prevention. For example, Gupta and Sherman (2011) have identified three types of situational prevention specific to cyberspace: **active prevention**, which requires users to modify their privacy/security settings and passwords on a regular basis; **prevention by avoidance,** which requires users to use the internet less frequently for banking transactions and purchasing goods; and finally, **passive prevention**, which requires users to reject emails from unknown sources, to install and update antivirus software and to restrict their surfing to trusted websites. According to the authors, applying these three types of prevention would suffice to very significantly reduce the risk of individual victimization (Williams & Levi, 2017, p. 459-460).

It is undoubtedly true that the absence of reliable information on cybercrime, especially in relation to economic offences, is perceived as a major obstacle to the elaboration of cybercrime prevention strategies (Smyth & Carleton, 2011). Consequently, despite the magnitude of the cyberfraud problem today, and although there are millions of dollars at stake every year, prevention efforts remain very much a work in progress.

Box 4.4. **Role of law enforcement agencies in cyberfraud prevention**

Police departments have developed clandestine internet investigation techniques (Chu et al., 2010; Franklin et al., 2007; Hinduja, 2007; Poulsen, 2012; Jenkins, 2001; Wolak, Finkelhor, & Mitchell, 2012; Holt & Lampke, 2010; Peretti, 2009). Many law enforcement agencies have, in effect, infiltrated online forums and chat channels, in order to disrupt markets for example. These approaches are seen as having a deterrent effect because they reduce criminals' potential profits and increase their risks. In such operations, law enforcement agents often take control of these types of sites in order to arrest their members (e.g., Mills, 2009). This type of operation not only facilitates gathering as much evidence as possible against offenders, but it also undermines the confidence of various actors in the illicit market in question. However, certain studies indicate that cybercriminals tend to receive insufficiently harsh sentences in comparison with their offences, thereby raising strong doubts about their deterrent effect (Holt, 2013; Wall, 2007).

Part III - The difficulties in applying traditional prevention theories to cybercrime

For over thirty years, crime prevention theories have developed around efforts to comprehend the behaviour of victims and the potential motivations for crime (Lewis & Lewis, 2011). Over time, the notion of crime prevention has become an important component of national, regional and local public safety strategies (see chapter 1). A basic postulate of crime prevention is that crime is associated with a series of underlying risk factors and that, consequently, it is by identifying these factors that effective prevention strategies may be successfully developed. As we saw in the preceding chapter, the identification of said factors largely depends on the criminological approach applied to a given crime-related issue. As regards the identification of risk factors, cyberspace raises a number of issues, due to a host of reasons (already mentioned above) such as users' impression of relative anonymity, the weak social control exercised over social media, spatio-temporal characteristics specific to the virtual world, the easy multiplication of interactions, the potential scope of online actions, etc. In this context, we therefore propose to identify the principal findings of the literature regarding the applicability of the most frequently employed crime prevention approaches, namely developmental prevention and environmental prevention.

Developmental prevention

First of all, it's important to remember that crimes against the integrity of the person represent important public health issues, associated with highly negative consequences in terms of mental health, social development and harms such as social and economic marginalization, depression or even suicide (Chisholm, 2014; Espelage & Hong, 2016; Kowalski, Limber, & Agoston, 2008; Notar et al., 2013). According to Patchin & Hinduja (2012), Espelage & Hong (2017), the rapid democratization of internet use and new information technologies has weakened the borders between the private and public spheres, thereby turning the internet into an extension of the real world, rather than a complement to it, with its own specific characteristics (Berguer, 2015). According to Collier (2010), this finding is crucial to the understanding violence in cyberspace, as it suggests that technology is "neither the problem nor the solution" (Collier & Nigam, 2010, p. 10). Consequently, the prevention of cyberviolence should be understood, above all, as a social question rather than a technological one, otherwise any prevention strategy will be doomed to failure. Hence the continuing pertinence of developmental prevention in the context of cybercrimes against the integrity of the person.

Box 4.5. **The developmental approach**

The developmental approach to crime prevention is rooted in the idea that delinquency is to a great extent connected with the social and environmental risk factors affecting an individual's development (Tilley, 2005; Tremblay & Craig, 1995). It is mainly founded on behavioural and sociological theories of the 1960s and 1970s, which analyzed different criminal behaviours to both propose specific categories of crimes as well as identify criminal life paths (Tremblay & Craig, 1995). According to the UN's guidelines for the prevention of crime, developmental prevention seeks to "promote the well-being of people and encourage pro-social behaviour through social, economic, health and educational measures, with a particular emphasis on children and youth, and focus on the risk and protective factors associated with crime and victimization" (UNODC, 2010, p. 13).

Although frontline practitioners and researchers are becoming increasingly interested in developmental prevention in their respective activities, this approach still occupies a very marginal place in the literature on cybercrime, as well as in the different national prevention strategies implemented in recent decades (Bossler & Holt, 2016; EUCPN, 2017; Seger, 2012; Williams & Levi, 2017). In effect, beyond awareness campaigns on online bullying, protection of personal data, as recommended by the UN guidelines (UNODC, 2013), or the provision of educational workshops in school environments, such as iSAFE, very few customized programs have been developed to reduce or mitigate the risk factors specific to cybercrime (KiVa and ConRed are notable exceptions). This deficiency is perhaps due to the relatively small body of studies on the risk factors specific to cybercrime, except in relation to cyberbullying and online sexual exploitation (Lewis & Lewis, 2011). Furthermore, in the wake of the cyberattacks of 2007, policymakers prioritized the protection of critical information technology infrastructure.

As the two preceding chapters made clear, the current state of research on cybercrime does not presently enable the establishing of direct correlations between "macro" type risk factors (e.g., social and economic inequalities) and criminal or victimization processes.

Notwithstanding the evident difficulties in applying this prevention model, we can nonetheless envisage at least two factors which can serve to problematize this issue: social norms and social control. In effect, **values** and **social norms** seem to be a factor concerning whether or not illegal activities develop in cyberspace. On this point, certain aspects are worth stressing from a situational perspective. More specifically, social norms are constructed in accordance with a number of dynamics in cyberspace, including two which are of particular interest from the vantage point

of cybercrime prevention. First of all, the social values that exist in the so-called "real" world undergo modification in cyberspace. This is the case regarding the perceived gravity of the actions of cybercriminals: in a word, there tends to be greater acceptance of illegal activities in cyberspace than in the real world. This has been demonstrated by many studies, particularly studies on the phenomena of cyberstalking and cyberviolence against women (Herring, 2002; Dunn, Lalonde, & Bailey, 2017; West, 2014). Moreover, the same holds for studies on the perception of infractions such as online piracy (Chaudhry, Chaudhry, Stumpf, & Sudler, 2011; Krawczyk, Kukla-Gryz, & Tyrowicz, 2015). Secondly, social norms also undergo (re)construction in accordance with conditions intrinsic to cyberspace, including, notably, its characteristic anonymity and the depersonalization of interactions that it engenders (Koops, 2010). Consequently, one cannot solely count on public awareness campaigns and repression if we really wish to curb the problems of cyberbullying and online sexual exploitation. If, as the OAS' Cyber Security Strategy prescribes, we must develop a culture of cybersecurity, then it is important to first develop a culture of preventing reprehensible acts against the integrity of the person, and thereby change the social norms which enable the trivialization of this type of crime, among others.

Likewise, **social control,** which acts as a powerful protective factor in the "real" world, is to, a very considerable extent, a diminished force in cyberspace – albeit not always, as we shall see forthwith. In effect, the redefinition of social norms, as well as environmental characteristics such as anonymity or depersonalization, have come to modify how the collectivity acts as a factor of regulation in the behaviour of individuals: on the one hand, physical disconnection and anonymity tend to weaken the possibility of social control; on the other, the capacity for mobilization on a vast scale, notably through social media, contribute to strengthening this same social control. A counter-trend attested to by #Me too movement.

Finally, there is a consideration that is too often disregarded in the literature on crime prevention: the **principle of differentiation**. To be more specific, according to the principle of differentiation stakeholders must consider issues of cyberviolence in a differentiated manner as a function of gender, sexual orientation, religion, etc. The adaptation of prevention strategies to different target groups is an absolutely core principle in traditional prevention. Of course, cybercrime occurs by definition in a differentiated context (for both offenders and victims). That said, the differentiation of prevention strategies will depend on the type of offence: as not every type of crime committed on the internet lends itself to a differentiated approach. Ang and Goh (2010) advocate a differentiated approach in relation to cyberbullying. In their view, although all prevention programs should include trainings on empathy, the specific emphasis should be gender informed: thus, whereas with boys the focus should be on cognitive empathy, with girls it should be on affective empathy (Chisholm, 2014).

Environmental prevention

Environmental prevention includes both situational prevention and prevention through environmental design. Mainly developed during the 1970s by the British Home Office (Tilley, 2005), environmental prevention seeks to limit crime opportunities, increase the risks associated with the commission of a crime and reduce the potential benefits accruing to an offender (UNODC, 2010). This approach is mainly based on rational choice theory (Clarke & Cornish, 1985), routine activity theory (Cohen & Felson, 1979) and crime pattern theory (Brantingham & Brantingham, 2008), also known as opportunity theory (Sutton, Cherney, & White, 2008; Tilley, 2005). Newman et Clarke (2003) posit that "crime follows opportunity when the presence of motivated offenders, and attractive and tempting targets in the absence of effective guardians combine in time and place" (Broadhurst, 2005, p. 7). In the present day, situational prevention has become, in a manner of speaking, synonymous with the reduction of crime opportunities. In practice, this type of approach often takes the form of targeted police patrolling, social mediation activities in parks and public transportation, or the installation of closed circuit cameras (Sutton et al., 2008).

The preventive measures most often discussed in the literature on cybercrime consist of so-called situational prevention approaches, generally based on routine activities theory (Cobb, 2014; Dashora, 2011; Leukfeldt & Majid, 2016; Williams & Levi, 2017; Poonia, Bhardwaj, & Dangayach, 2011). These approaches emphasize the reduction of crime opportunities through changes in users' behaviour and by modifying environmental characteristics conducive to the generation of crime opportunities (Cornish & Clarke, 2003; EUCPN, 2017; Sutton et al., 2008).

More specifically, Bossler and Holt (2016) envisage four categories of situational intervention in the context of cybercrime prevention: (1) increasing the difficulty of offending; (2) increasing the risks of offending; (3) mechanisms to reduce rewards of involvement in cybercrime; and finally (4) removing the excuses for offenders and victims, which enable them to justify their actions based on external factors (Bossler & Holt, 2016, p. 137). Examples might include the use of antivirus and/or ad-blocking programs to protect against malicious software (Ngo & Paternoster, 2011) and identity theft (Bossler & Holt, 2016). That said, the effectiveness of such measures is not always guaranteed (Ngo & Paternoster, 2011). As for parental control software, these types of programs apparently have a minimal impact in terms of reducing the risks of bullying, stalking and sexual advances, to which youth may be subject in cyberspace (Jones et al., 2006; Marcum, 2013).

Further to the question of limiting crime opportunities, Ngo and Paternoster (2011) propose a new vision of police patrolling in the context of cyberspace. Cognizant that police patrols can't operate in the same manner in the virtual world, the authors nevertheless drew on this traditional practice to develop their concept of distributed policing strategy. Instead of relying first on the police, then on citizens, this strategy is based on the

premise that cyberspace requires an inversion of these roles. In effect, in cyberspace when an individual fails to take charge of his or her own security this may lead to the victimization of another person (Ngo & Paternoster, 2011). Similarly, Garland (2001) argues that law enforcement in the virtual world also requires accountability (and empowerment) on the part of the business community and civil society (Williams & Levi, 2017).

Although the notion of opportunity enables environmental prevention to identify propitious locations for the commission of criminal acts, this approach does not explain the causes of crime (Cobb, 2014; Tilley, 2005). In addition, as it does not directly address the causes of crime, situational cybercrime prevention only very rarely drives long term changes. Moreover, according to rational choice theory, the effect of environmental prevention may simply be to displace crime problems to other locations (Cobb, 2014). Consequently, the presence of measures based on the environmental prevention approach could even have a detrimental effect on the public's feeling of insecurity to the extent citizens are aware of this displacement effect (Cobb, 2014).

Towards partnership-based prevention in cyberspace

Cybercrime prevention requires radically different governance structures in comparison with those of the real world, namely governance structures organized in the form of networks. The operationalization of such networks requires the formation of partnerships and certain collaborative processes, including, notably: 1) the harmonization of legal frameworks and international cooperation between justice systems and law enforcement agencies; and 2) cooperation between different types of actors under a system characterized by nodal governance.

As was underscored in the two preceding chapters, one of the major difficulties which arises in the fight against cybercrime lies in the very nature of cyberspace and the activities taking place in it. Of particular importance is cyberspace's (relative) disconnection from physical locations. This disconnection is a central issue with important implications inasmuch as the study of traditional crime supposes a certain unity in the localization of the offender, victim and crime. However, this unity is shattered with cybercrime, as the victim and the perpetrator may be located in different countries. Furthermore, the act as such may involve other physical locations, such as, for example, the location of the hacked servers where the stolen data was stored.

One implication of this reality is the now familiar physically fragmented governance structure. Another is that traditional ways of addressing crime are ill-adapted for responding effectively to cybercrime, as policing and justice system institutions (and legal and legislative frameworks) only operate within geographically limited jurisdictions. Consequently, close collaboration among actors at the international level is essential in the fight against cybercrime. As is the harmonization of regulatory frameworks. In this regard, Dupont (2016) observes that existing cooperative practices augur the emergence of a new model of governance, which he terms polycentric, and which is characterized by the functioning of multi-actor networks in the form of partnerships. Moreover, according to this author, these networks demonstrate greater adaptability than is generally thought, notably as regards governmental institutions, most particularly those from the justice system and law enforcement sectors.

Box 4.6. **Informal police networks**

Comprehensive prevention of cybercrime requires specialized resources capable of tackling complex issues. However, many law enforcement agencies are unable to adequately respond to cybercrime issues due, among other reasons, to a lack of sufficient knowledge or qualified personnel. In this context, networking with other police departments may prove an inexpensive and effective alternative. In the same vein, Bayer (2010), in a major review of the literature, enriched with a number of interviews with different police departments and intelligence agencies, observes that the traditional policing networks are generally criticized as ineffective and costly, due to the size of the bureaucracies involved in such networking processes. This is why certain authors, such as Eskola (2012), recommend the formation of informal networks for sharing practices, knowledge and technical expertise as a means of avoiding unnecessary bureaucratization of procedures, to the benefit of the law enforcement agencies concerned (Eskola, 2012).

Nhan and Huey (2008) identify four nodal clusters, i.e., poles of essential actors that form networks: governments (including all governmental or multi-governmental institutions, both national and international, which are not part of criminal justice systems); law enforcement (the entire range of law enforcement and justice system actors); private industry; and, finally, the general public (which also includes online and real world civil society organizations). Quéro and Dupont (2017) distinguish five types of capital, which shape the specific characteristics of nodes in relations with other types of actors: 1) social capital refers to a node's ability to create and maintain mutually beneficial social relations with other nodes; 2) cultural capital concerns a node's knowledge in terms of cybercrime and cybersecurity, which could potentially constitute a resource for others; 3) political capital denotes a node's capacity to comprehend the dynamics bearing on political and governmental structures and public institutions at all levels; 4) economic capital denotes a node's grasp of market dynamics and economic structures, both locally and at all other levels, as well as its own economic power; and 5) symbolic capital encompasses all factors contributing to a node's organizational legitimacy.

For these networks to form, and for their different nodal clusters to cooperate in an effective manner, a number of supporting pro-

cesses must be in place, including: 1) the harmonization of regulatory frameworks; 2) cooperation between different law enforcement and justice system actors from distinct jurisdictions; and 3) partnership development, which include all categories of actors.

Given the multitude of risk factors, weak social control and abundance of crime opportunities, Williams and Levi (2017) argue that it is essential to envisage all cybercrime prevention initiatives in terms of partnerships. Community or partnership-based prevention is founded on the notion that it is possible to exercise positive influence on criminal behaviour by modifying the physical and social organization of a given environment (Tonry & Farrington, 1995). Prevention initiatives based on this type of approach are evidence-based and informed by the expertise of practitioners (Tilley, 2005). "Scholars of crime prevention argue that programs and policies will achieve maximum effectiveness if they are built on scientific knowledge regarding the nature and causes of crime and delinquency and on the knowledge of what works, or best practices" (Rosenbaum & Schuck, 2012, p. 1). To ensure that these initiatives are well informed, as well as effectively and sustainably implemented, it's important to ensure the participation of the health sector, social development and urban planning, job search assistance services, parks and rec, the education sector, the justice system, social services and the private sector (Crawford, 1999), as well as internet providers and online content hosting services. In effect, the latter two are particularly well situated in terms of informing and elaborating cybercrime prevention measures, as they dispose of the technical capacities required to observe problematic user behaviour, ban access to illegal content, ensure that laws are applied, facilitate criminal investigations and intervene when individuals are victimized by criminal acts (UNODC, 2013).

The governance of cyberspace is multipolar, with the central roles played by the private sector actors that manage its infrastructure, provide access and host content on the internet, as we saw in detail in Chapter 2. As a consequence, the conventional model, in which leadership is primarily ensured by the public authorities, is inapplicable to crime prevention in cyberspace. The governance of cyberspace demands an adapted model, founded on partnership and cooperation rather than on leadership ensured by a single category of actors.

From the vantage point of the state, concern over criminal activities in cyberspace really commenced in the post 9-11 world when it adopted a primarily security-oriented approach to deal with the threat of terrorism (Fratianni & Savona, 2005). Thus began an evolution away from the libertarian model, which underlay the internet's creation and development, as well as from a resolutely multi-actor and private sector-centred governance structure, as many States, both democratic and authoritarian, moved to strengthen their control over cyberspace through stricter regulations and oversight (Deibert & Crete-Nishihata, 2002).

In this regard, as Tilley and Sidebottom (2017) point out, security-related responsibilities in cyberspace have weakened among actors and users organized in the form of networks (Tilley & Sidebottom, 2017). As a consequence, Wall advocates a model in which the leadership exercised by public authorities is that of a facilitator, which encourages new relations amongst the different nodes of the networks responsible for cybersecurity (Wall, 2007).

In fact, the issue of the security and cybercrime prevention responsibilities incumbent on different actors is at the heart of the (re)definition of cyberspace governance. Just as the public authorities cannot constitute the sole regulator and responsible entity, the private sector, despite its absolutely core role in cybergovernance, is unable to assume these responsibilities in their entirety. This lack of clarity around the responsibilities of different stakeholders impacts first and foremost the victims of cybercrime; in effect, victims of cyberfraud or identity theft generally have few remedies at their disposal, and many such crimes are de facto treated as (and considered) the negative but inevitable consequences of the digital age.

It follows from the foregoing that there is a need to redefine cyberspace governance in a manner that integrates a more victim-centred approach to cybercrime prevention. Thus, in addition to posing the question of defining the responsibilities of the different actors, it is also necessary to address the regulations, norms and standards governing cyberspace access, activities and usages. This question constitutes an essential priority in the fight against cybercrime and has implications for core issues such as the collection of personal data and the privacy, protection and permitted uses thereof. Another core issue concerns the extent to which law enforcement agencies and justice systems are adapted to the new constraints imposed by cyberspace. From the point of view of victims, the matter of cyberspace governance raises the issue of who are (or should be) the competent authorities responsible for their security and that of their personal data.

Finally, there is another aspect of partnership-based prevention, which concerns issues of interdependence and coordination across different levels of government. In traditional crime prevention, coordination issues may arise due, notably, to differences in scale in the interlocking activities of different levels of government. Hence the importance of identifying the appropriate scale or level of government in the different aspects of prevention strategies. In short, it's important to ensure that the national strategy and local initiatives contribute to common objectives and, to that end, are articulated in a complementary manner.

Having said that, issues of interdependence and scale are radically transformed in the context of prevention in cyberspace. First of all, notions such as the scale of action or policy do not have the same meaning in cyberspace. In effect, although different levels of governance may be involved in cybercrime prevention, they are all dealing with an object that is global and transcends issues of scale. Interdependence, therefore, applies exclusively to governance actors. To this interdependence of levels of governance, one may also associate, in the case of multipolar and multi-actor governance structures, the interdependence of nodal clusters: in effect, the actions and initiatives conducted by a given group of actors must, likewise, contribute to achieving common objectives, in a complementary manne.

Conclusion: Recommendations

By definition, prevention activities are developed and implemented over the medium and long term. In contrast, cyberspace is characterized by high paced change and extremely rapid evolution. Consequently, for those endeavouring to encourage reflection on how to prevent the various forms of violence and crime in cyberspace, the challenge is to integrate the reality of rapid evolution into an approach that is sustainable over the long term. The question, then, is how to construct highly adaptable prevention models capable of retaining their pertinence and effectiveness in changing conditions.

First of all, as we've just suggested, the partnership-based approach is central to cybercrime prevention. In partnerships, it is essential to construct transparent prevention initiatives, which clearly define the roles and responsibilities of the different stakeholders and which, moreover, are subject to rigorous evaluation. After all, as we've already seen, the multi-actor and multipolar governance of cyberspace further complexifies the development and implementation of prevention initiatives as:

1) Leadership, which traditionally falls to public authorities, becomes more problematic and is subject to power struggles and jockeying for influence; and
2) With respect to issues of implementation, administration and funding, a greater capacity for consensus-building and collaboration amongst the different core actors is required to ensure that a balance of interests is found, notably in cases where initiatives involve co-financing and co-management by groups of very different actors..

Of course, the dispersal of leadership, in conjunction with the sharing of responsibilities and roles among groups composed of different types of actors, only complexifies the identification of transparent processes, based on greater accountability. This issue has been widely documented in the literature (notably in the areas of environmental management and public-private partnerships), particularly in discussions of the complexities of constructing effective multi-actor governance and the associated benefits in terms of transparency and accountability (Brinkerhoff & Brinkerhoff, 2011) (see preceding chapter). In a word, responsibility for crime prevention cannot fall to a single actor or, for that matter, to a small group of actors. At all levels, cybercrime prevention initiatives must be envisaged in terms of a comprehensive or holistic process, which assembles the actors of the criminal justice system, youth protection services, the IT sector, the education sector, the health sector and law enforcement agencies, with a view to ensuring developmental and environmental prevention. Moreover, such cybercrime prevention initiatives must be consistent with the principle of interdependence, clearly defined roles, human rights and respect for the rule of law.

Furthermore, given our current state of knowledge on cybercrime, which is embryonic, the founding of a preventive approach based on a solid scientific foundation remains a challenge, as is the case, moreover, with traditional crime (see chapters 2 and 3). For decision-makers, then, it's important to reflect on new policies and approaches to prevention. Secondly, the assessment of cybercrime prevention programs is affected by two major constraints. First of all, measuring prevention outcomes constitutes a challenge per se, particularly in the case of social prevention, which is concerned with macro-level risk factors. In effect, such interventions are designed to produce systemic effects which are intrinsically difficult to measure. In addition, such prevention efforts are handicapped by our still inadequate knowledge of crime processes and victimization in the context of cyberspace and their corresponding causes and risk factors (see preceding chapter).

For institutions like the International Centre for the Prevention of Crime this situation represents a major challenge, namely: how might we develop tools that enable informed decision-making, based on complementary approaches intended to remedy the lack of sufficient scientific knowledge?

Contribution

Confronting the issues of digital crime

Jérôme BARLATIER,
Ph. D, Squadron Commander
Central Criminal Intelligence Unit (SCRC), France

The reality of the digital era is now an unavoidable fact of life for law enforcement in virtually every area of its activities. It creates new opportunities for criminals by providing conditions, which they can exploit to adapt their methods or devise new ones. On the other hand, it also holds new and unprecedented potential for investigators at home in a world where criminals may be tracking by the digital footprints they leave. The Internet is neither a new lawless Far West nor the realm of the surveillance state merely, as it merely recreates the normal issues of the police-criminal relationship.

The present article will describe the strategy of the Centre to Combat Digital Crime (C3N), an office of the National Police's Criminal Intelligence Service (SCRC).

An organization based on complementarity and subsidiarity

La gendarmerie nationale française a accompagné dès l'origine The National Police has monitored the internet's development from its very outset. It is now preparing to confront the impending issues, arising with the digitization of society.

Its identity firmly rooted in local action and the versatility of its agents, it is now turning its efforts to address the intangible character of cyberspace by means of increasingly specialized methods.

The reconciliation of this apparent paradox is premised on a two-fold principle:

- The subsidiarity between, on the one hand, the democratization of knowledge and tools which enables addressing the pervasive digital considerations in modern investigations, and specialization, on the other hand, which makes it possible to take on the most complex cases of cybercrime;
- The principle of complementarity is used to guide a criminal police service with a dual structure: an investigative structure (combining generalist units and specialized services) and a support structure (drawing, in particular, on expertise in forensics and crime intelligence).

The National Police integrates these two elements under Cybergend, a network of 4,400 national police officers working in three areas of competence (enforcement, monitoring and expertise). It is thus equipped to handle a broad range of investigations adapted to the sui generis characteristics of internet crime. The composition of cybercrime is as follows:

- 70 % cases concern fraud;
- 10 % concern attacks on automated data processing systems;
- 10 % consist of cases of reputational harm;
- et 10 % concern other offences.

The C3N sits at the apex of this operational structure for combating cybercrime. As such, it is at one and the same time:

- a high-level investigations unit;
- a leadership division for Cybergend;
- a national crime pattern database and digital monitoring service;
- a contributor of strategic, operational and tactical intelligence; and
- a research laboratory.

The diversity of these missions is an obvious asset when it comes to developing a judicial police agency that is both strategic and exploratory.

A strategic cutting edge judicial police agency

In a competitive criminal investigation environment, an investigative service must seek out a niche which highlights the advantages it offers.

C3N has therefore opted to focus its efforts on a strategic problematic, which cannot be effectively addressed at any other level. Internet crime is unconstrained by the normal rules of territoriality. Cyberspace is a borderless expanse. Given the possibilities of reaching vast numbers of potential victims in the privacy of their homes, cyberspace constitutes eminently fertile ground for criminals. The conditions of the internet allow criminals to maintain their anonymity and depersonalize victims. It encourages criminals to act, as direct confrontations may be averted. With a few clicks, a single cunning individual or group can reach a sizable population and cause considerable damage. Under these circumstances, C3N works to neutralize prolific offenders by seeking out recurring criminal patterns. The launching of targeted investigations allows investigators to identify similarities based on the collection of the critical mass of forensic information needed to identify offenders and build cases.

Criminal prosecutions are not the only outcomes of these activities. In effect, the forging of strong, trust-based partnerships between public and private stakeholders can also lead to other non-justice system measures for containing certain phenomena.

C3N also is also focusing on cutting edge forms of prevention. In effect, it is endeavouring to exploit its strategic intelligence capabilities to anticipate threats and understand future challenges in cyberspace. With their advanced technical skills and legal knowledge, its agents must be adept at employing innovative investigative methods in new cutting edge areas. In past years, investigations focusing on cryptocurrencies and the dark web were the issue of the day. Having established the feasibility of

such investigations, the C3N research units have assimilated and capitalized on this expertise. The challenges of the coming years will probably include developing comprehensive knowledge in relation to the internet of things (IoT), addressing the challenges of Big Data and harnessing the potential of artificial intelligence.

The ambitions of this strategic and innovative judicial police agency would not have been possible without the elucidation provided by intelligence work and research.

Operational action guided by intelligence and research

Criminologists have traditionally described the work of investigators as bureaucratic, events driven and routine (see, in particular, Greenwood Chaiken and Petersilia 1976, as confirmed by a growing body of literature reviewed by Barlatier, 2017). Two movements in policing policy aim to change this traditional approach to investigation.

First of all, intelligence-led policing (ILP) posits a model where operational activity is determined upstream, based on a knowledge of criminal phenomena and actors (Ratcliffe 2016). Under such conditions, raw intelligence is transformed into insight. It allows the investigator to strategically monitor both crime hot spots and prolific offenders. According to ILP, the intelligence accumulated by the police is only useful to the extent that it guides policing.

The fight against cybercrime lends itself quite well to the practices of ILP. The status quo is characterized by a systematic and legally sterile complaint recording process, under which local units are overwhelmed by a deluge of complaints for which they lack the means to address in any effective manner. Happily, with ILP, we are seeing the progressive emergence of dedicated reporting platforms, i.e., a system that provides a web-based mechanism where victims can describe the incidents which affected them. That said, this process does not necessarily mean that no criminal investigation will opened. On the other hand, it provides a means to collect, organize and analyze large quantities of intelligence, which may potentially support criminal investigations or other remedies. This system intelligence enables federal officers to act with informed judgement, thereby increasing the chances of effective action.

In 2018, the SCRC will implement its PERCEVAL system for reporting online bank card fraud, a type of crime whose annual incidence is less than 10,000 when measured by complaints filed, although the banking and e-commerce sectors estimate the real number of incidents to be 1.9 million. Enriched with additional sources of information prior to advanced data processing, the information provided by private individuals may then be analyzed and compared in order to detect criminal patterns. In a sense, this process reverses the usual pattern. In effect, rather than investigators reacting to information from the public, generated in a passive fashion, citizens enrich the knowledge of investigators to equip the latter to act in a proactive, cogent and effective manner.

Secondly, evidence-based policing (EBP) is an approach to law enforcement that relies on solid research (Sherman 1998). EBP endeavours to overcome the mutual indifference with which police and researchers often regard each other, on the basis of a two-fold observation:

- police activities represent a fertile ground for empirical research;
- the knowledge generated by researchers may in turn prove particularly useful to investigators.

The SCRC oversees a research and development policy consisting of two components:

- Short to medium term initiatives, linked closely with operational concerns, run by in-house SCRC researchers;
- Medium to long-term initiatives for studying concepts and tools of value in investigations or intelligence activities, which are spearheaded through partnerships with public and private research institutes.

In this framework, C3N's research and development unit has been particularly dynamic with its direct support for investigators (e.g., development of scripts to facilitate the collection and management of large quantities of data from the internet) and the development of tools likely to be useful to a broader population (e.g., online monitoring or search applications, methods of collecting and analyzing digital traces, image recognition and processing using AI).

The SCRC/C3N in no way holds itself up as a model. Rather, it demonstrates a pragmatic willingness to address the issues raised by criminal investigations in cyberspace. While its strategy respects the National Police's traditional methods of operation, SCRC/C3N's methods and tools are nevertheless premised on a necessary paradigm shift and a useful opening up and reconfiguration of approaches.

Contribution

Réponses des États pour prévenir la cybercriminalité ?

Cécile Doutriaux
Lawyer
Member of the Cyberdefence Chair, Saint Cyr School Board, France

> "Cyberattacks are sometimes more dangerous for the stability of democracies and economies than rifles and tanks."[26]

These words indicate the concern shown by states in relation to cybercrime[27], as for over twenty years, cybercriminals have been committing numerous computer attacks worldwide.[28]

Computer threats can take many different forms (phishing[29], ransomware[30], computer sabotage[31], denial of service attacks[32], website defacement[33], digital identity theft…) and target a vast range of victims, including states, communities, companies, individuals.

Cybercriminals take advantage of modern technology's speed and anonymity to commit crimes without regard for international borders, as digital networks are available worldwide.

As a consequence, they can commit attacks in countries where laws are less strict or, indeed, nonexistent, thereby rendering investigations and criminal prosecution more difficult and complex.

Thus, to insure that offences committed in cyberspace do not go unpunished, it is not enough for states to act on an individual basis. Rather, all countries must cooperate fully.

Yet, although considerable means and resources have been deployed at the European and international levels, some have proven less effective than others, which calls into question their deterrent effect and capacity to prevent cybercrime.

At the International Level

International organizations have taken several initiatives to prevent cyberattacks.

a) The UN

The United Nations[34] has thus instructed the ITU[35] to prepare an international framework for the regulation of cyberspace.

A Group of Governmental Experts (GGE), named by the secretary general of the UN, proposed a series of standards later adopted by the G20, which led to the recognition of the applicability of international law to cyberspace, particularly the United Nations Charter, the Universal Declaration of Human Rights, the Law of Armed Conflicts and law on the international responsibility of states.

In 2010, at the Davos World Economic Forum, the ITU suggested the adoption of an international treaty on cybersecurity, based on three principles: the establishing of a state cyberdefence policy, prohibiting the sheltering of cybercriminals and the renouncing of any offensive action against other states.

The multiplication of WSIS[36] meetings and forums on Internet governance initiated by the UN, has strengthened dialogue between countries.

However, although states recognized the principle of prevention, cooperation and non-proliferation in cyberspace in 2013 and adopted voluntary commitments of "good conduct" in cyberspace in 2015, they have yet to reach a real consensus on the regulation of cyberspace.

Indeed, several states, including the United States, are reluctant when it is a matter of ceding their power to regulate the Internet to the United Nations.

As a consequence, the UN remains powerless in relation to global cyberspace security due to the numerous policy differences in the international community which limit cooperation.

b) NATO

As early as 2002, NATO sought to reinforce its defences against cyberattacks by establishing a dedicated structure: the NATO Computer Incident Response Capability (NCIRC) Technical Center.[37] This agency manages all of NATO's information systems and responses to the cyberattacks perpetrated against them.

In 2008, NATO also created a cyberdefence excellence center in Tallinn, Estonia, to conduct research on computer attack issues and perspectives, as well as organize trainings, vulnerability tests and joint exercises to reinforce the response capabilities of member states.

At the Warsaw Summit in 2016, the NATO allies undertook to strengthen and improve the securitization of their infrastructure and national networks.

Furthermore, NATO is working in partnership with the European Union (EU), the United Nations (UN) and the Organization for Security and Cooperation in Europe (OSCE) in a spirit of complementarity, in the interests of achieving an enhanced securitization of cyberspace.

However, despite the efforts deployed by NATO, it was the target of several attacks attributed to the Anonymous group in April 2010, which had the effect of discrediting it and, moreover, demonstrated that the security of its computer systems left much to be desired.

As international organizations have shown their limits in preventing cyberattacks, national governments tend to prefer cooperation efforts which mobilize a smaller number of partners with the express intent of ensuring greater effectiveness.

At the European level

a) ENISA

Created in 2004, the European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cybersecurity in Europe. It helps member states prevent, detect and respond to information security issues.

In September 2017, the European Commission decided to strengthen its powers. Henceforth, this agency would be known as the "EU's Cybersecurity Agency" with a permanent mandate to help EU member states, institutions and businesses counter cyberattacks.

A permanent Computer Emergency Response Team for EU Institutions, bodies and agencies (CERT-EU) was also created in order to ensure coordinated responses to cyberattacks against EU member states.

This agency is also tasked with implementing the directive on the security of network and information systems (NIS) adopted in 2016 to strengthen cooperation between member states. It directs every EU country to designate a national cybersecurity authority and adopt a strategy for combating cyber threats.

Finally, in addition to working closely with the computer security teams of EU institutions and member states, it will also cooperate with NATO.

b) The Council of Europe

In fact, cooperation between states is largely in keeping with the Budapest Convention on Cybercrime[38] of November 23, 2001, which seeks to harmonize signatories' criminal code provisions bearing on cybercrime and institute a rapid and effective regime for international cooperation in this area.[39]

This convention is also intended to "make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence."[40]

Thus, based on this convention, a signatory state can secure the rapid safeguarding of computed data stored in the territory of another state in order to identify cybercriminals and establish proof of their actions.

Cross-border cooperation between member states' law enforcement agencies is achieved with the assistance of the European Police office (Europol)[41] and the European Union's judicial cooperation unit (Eurojust),[42] which harmonize their practices and share information on cybercrime.

Operationally, EU governments collaborate closely with the European Cybercrime Centre (EC3), created in 2013 under the auspices of Europol, and Eurojust to harmonize member states' policy approaches and practices in the fight against cybercrime.

This cooperation between EU member states is effective, as attests an investigation carried out with the support of Europol and Eurojust, which led to the arrest of a group of 20 hackers that had falsified the emails of tax authorities in order to defraud bank customers in Italy and Rumania to the tune of one million euro, on 28 March 2018.

Furthermore, on March 28, 2018, Europol revealed that it had successfully apprehended a group of criminals in Spain who had infiltrated 100 financial institutions in 40 countries using the Carbanak and Cobalt malicious software,[43] following an investigation by the Spanish national police with the support of Europol, the FBI, the Romanian, Moldovan, Byelorussian and Taiwanese authorities, as well as private cybersecurity companies.

Conclusion

The control of information technologies represents a major issue and many states are reluctant to cede part of their sovereignty in favour of full and comprehensive cooperation in the fight against cybercrime.

In a global context of international tensions and a return to a certain protectionism, it is difficult to envisage enhanced international cooperation, even if national governments everywhere stand to benefit.

Therefore, the way ahead for more effective cybercrime prevention is clearly that of favouring occasional cooperation involving small numbers of states, and this from an exclusively criminal and economic vantage point, bereft of any political considerations whatsoever.

Another solution would also consist of developing technical solutions at the national level, such as delisting networks and rendering them unavailable – an already widely implemented measure.

Contribution

The role of cybersecurity strategy development in supporting a framework for combatting cybercrime[44]

Belisario Contreras
Cybersecurity Program Manager, OAS
USA

Kerry-Ann Barrett
Cybersecurity Policy Specialist, OAS
USA

Introduction

With increased connectivity to the Internet, the world has never been smaller. The Internet of everything has changed the way people, businesses and governments interface with each other. With more than 3 billion Internet users, representing just over half of the world´s population and in Latin America and the Caribbean alone approximately 417,940,160 internet users,[45] more and more people are now experiencing both the benefits and risks of being online.

Latin America and the Caribbean currently represents one of the fastest-growing Internet populations in the world, giving rise to a number of significant cybersecurity challenges, including those surrounding critical infrastructure protection and increased malicious activities using the Internet. With this increase in Internet usage, the difference between the real world and the digital world is rapidly disappearing. Criminally motivated cyber incidents as a result, have become an extensive and damaging threat that requires governments, international organizations, the private sector and civil society, to work together recognizing that cybersecurity threats concerns everyone.

Cybersecurity and Cybercrime

The nexus between cybersecurity and cybercrime is sometimes blurred and there are instances where cybersecurity practitioners and those that work within the criminal justice system with a focus on cybercrime, deliberate on where the role of one ends and the other begin. This paper takes the perspective that, cybersecurity and cybercrime, while interrelated, are distinct disciplines. Further, it is proposed that cybersecurity measures can provide a framework that contributes to the mitigation of the occurrences of cybercrime and/or provide mechanisms for the resolution of its effect.

Cybercrime can be described as the malicious use of the Internet or computer systems to commit a crime or the commission of a crime targeting a computer system. Cybersecurity, on the other hand, refers to those practical measures that are taken to ensure that information communication systems are able to remain operational without interference. From a broader perspective, this includes not only the technical measures taken to ensure that the systems remain available and without interference, but includes a wider ecosystem that impacts the application of technical measures, such as laws, regulations, policies and practices. This wider eco-system provides the framework for national, regional and international players to be able to identify and respond to a cyber incident and to take further action if it is identified as a crime. As such, cybersecurity also involves a multi-stakeholder approach to develop and implement these measures to protect networks.

To address cybercrime, many contingent pieces must be in place as it would require investigation, prosecution and evidence sharing which often involves other states and state actors. Some of the questions one must consider include: is there legislation in place that identifies the elements of the crime? Does the legislation require that there is a victim or to prove that damage has been caused? Does the court have jurisdiction over the accused? (especially when the crime is committed in one jurisdiction but the alleged perpetrator resides in another) and also, do the investigators and prosecutors possess the necessary capabilities to investigate and prosecute the case?

The differences between cybercrime and cybersecurity are also apparent in the people who work in these areas. Investigation, and prosecution of cybercrime is best left to the criminal justice sector—law enforcement, analysts, prosecutors, magistrates and judges. On the other hand, cybersecurity is largely accomplished by information and communications technology (ICT) specialists—such as software developers, networks and systems engineers and cyber risk analysts—and educated computer users.

When formulating cybersecurity strategy, policy-makers must recognize these distinctions, i.e. between addressing cybercrimes and managing cybersecurity. They must also understand how cybercrime fits into the wider ecosystem of cybersecurity.

The wider ecosystem of cybersecurity

Taking into account the distinction between cybersecurity and cybercrime, one must consider the other areas that impact cybercrime and its investigation. These include efforts at the national and international level to implement measures that ultimately, can only lead to the improvement of state-to-state cooperation during investigations. This is what we describe as the wider ecosystem (see Fig 1) which facilitates the investigation and prosecution of cybercrime, and include:

1. **National Legislation** once in effect provides the basis in which cybercrimes can be investigated and prosecuted. This also provides, among other things, investigative powers and tools for law enforcement authorities;
2. **Incident Response** facilitates recovery and continuity of networks. However, if in place, the evidence collected can be further used for the investigation and prosecution of cybercrimes within well-established guidelines and procedures;

3. **Investigation and prosecution of malicious incidents** contributes to ensuring public safety by deterring, identifying and minimizing malicious actors online and also builds confidence and trust in end-users to utilize online services;
4. **End-User awareness** provides tools needed for citizens to not fall victim to a cybercrime and if they do, what action they could take and to whom and where to report it;
5. **International cooperation** includes not only the international cybersecurity mechanisms, but also anti-cybercrime mechanisms, such as the UNODC IEG on cybercrime[46] and the Budapest Convention,[47] aimed at addressing cybercrime. These, too contribute in establishing reciprocity and cross-border investigation;
6. **Regional and International norms**[48] contribute to the wider discussion on state-to-state co-operation and can provide guidance to states on state behavior on a whole in the treatment of cybersecurity and cybercrime related issues.

It is in this context that we would like to highlight the very practical ways that the development of a national cybersecurity strategy can support the development of a robust framework to combat cybercrime. A national cybersecurity strategy (NCS) is a plan of action designed to improve the security and resilience of national infrastructures and services. It is a high-level top-down approach to cybersecurity that establishes a range of national objectives and priorities that should be achieved in a specific timeframe.[49] In order to approach the issue holistically, it is recommended that countries think about their national cybersecurity strategy as a framework that can support a nation's efforts to protect the computers, networks, and data of its government, businesses, and people. A component of any strategy should address the prevention, investigation, and prosecution of cybercrime. Areas to consider are:

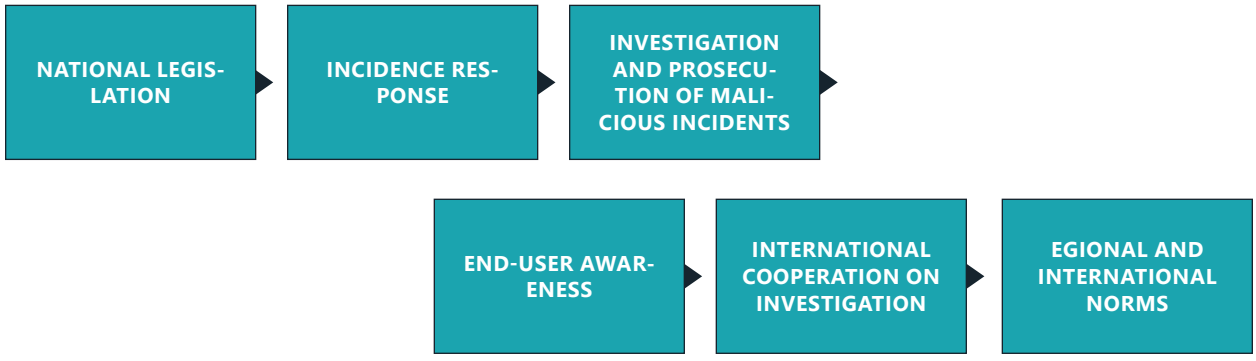
1) National Coordination reduces ad hoc responses to cyber incidents and duplication of efforts of responsible agencies within a country and should include:
   a. Definition of the roles and responsibilities of responsible agencies and national stakeholders, to include the national coordination authority, cybersecurity authorities (such as CSIRTs, ICT ministries, etc.) and criminal justice sector authorities (such as law enforcement, prosecutors, magistrates, judges);
   b. Identification of points of contact for coordination;
   c. Coordination of national stakeholders for the development of policy and for response to incidents.

2) Allocation of strategic and adequate resources ensures that there is the technical capacity available to respond adequately to cyber threats and should include:
   a. Budget allocation for cybersecurity efforts;
   b. Adequate personnel allocation;
   c. Continuous training of cybersecurity officials;
   d. Experts available 24 hours a day for incident response coordination;
   e. Experts dedicated to the investigation of cybercrime.

3) A legislative framework that addresses cyber-related crimes and provides the necessary tools for law enforcement and includes:
   a. Legislation that criminalizes cybercrimes;
   b. Measures that support the ability to collect, preserve and share evidence.

4) International cooperation and collaboration which takes into account the borderless nature of cyber-related crimes and includes:
   a. Participation in the international dialogue on cyber issues (such as cybercrime);
   b. Provision of "dual criminality" in domestic law;
   c. Entering into bilateral and multilateral mutual legal assistance (MLA) agreements (e.g. OAS MLA Treaty[50]).

Illustration 4.1. **Cybersecurity Wider Ecosystem**



Source: Authors

Development of National Cybersecurity Strategies

Taking into account the above and the ever-evolving threats that impact cyberspace, each country can consider the areas identified in the previous section and find a strategic approach that suits its needs. The best strategies are those that promote an adequate assessment of the risks and threats, take into account risk mitigation measures, are tailored to individual national needs, and engage all relevant stakeholders in the decision-making and implementation process. In this regard, there is a recognized need for a high level national policy directive for cybersecurity that has an associated strategic plan of action to achieve that directive and the goals of the strategy. The process for its development should always involve all relevant stakeholders (government (including law enforcement), private sector, civil society, academia, et al.) and culminate in a document that is clear in its scope, addresses specific national threats, and articulates clear goals, objectives, as well as the steps needed to achieve those goals in light of identified priorities. In relation to its implementation, once approved, the associated costs and available resources must be identified and included in the budgets of implementing agencies or entities.

It is worth noting that the Secretariat of the Inter-American Committee against Terrorism (CICTE) of the OAS General Secretariat (OAS/GS), through its Cybersecurity Program, has been working for more than a decade with member states to build national cybersecurity capabilities as part of efforts to implement the Comprehensive Inter-American Cybersecurity Strategy, adopted by OAS member states in 2004. In Latin America and Caribbean, the importance of having a national cybersecurity has become evident in recent times with several countries publishing strategies in recent times: Colombia (2011 and 2016)[51], Panama (2013)[52], Trinidad and Tobago (2013)[53], Jamaica (2015)[54], Chile (2017), Paraguay (2017) and Costa Rica (2017)[55].

Conclusion

The inter-play between cybersecurity and cybercrime can only gain benefit with the development of a national cybersecurity strategy. National cybersecurity strategies establish a framework within which all players can work together, including on the definition of roles and responsibilities. The development and implementation process requires commitment from senior officials and cooperation and participation of various national stakeholders. The implementation of the objectives identified in this paper will assist a nation in improving its cybersecurity capabilities and in the end be more agile in addressing cybercrimes when they occur.

Notes

24 See for example the difference between the security approaches employed in counter-terrorism vs those in radicalization prevention discussed in the introduction to our study "How to prevent radicalization: a systematic review" (ICPC, 2015).

25 In light of the lack of consensus on the definition of cybercrime, the term "cybercrime" in the present text will encompass the concepts of computer crime as well as crime in cyberspace.

26 Jean-Claude Juncker, president of the European Commission (state of the Union speech, September 2017).

27 Cybercrime refers to "any illegal behavior committed by means of, or in relation to, a computer system or network."

28 Worldwide, the economic losses from attacks have been estimated at 400 billion euros per year and in 2016, 80% of European companies experienced computer incidents, according to the European Commission.

29 Phishing is a technique whose objective is to obtain personal information and bank account identifiers for criminal purposes.

30 Ransomware is malicious software (e.g.: Locky, TeslaCrypt, Cryptolocker, WannaCry. etc.) that encrypts data in order to render it unavailable.

31 Computer sabotage consists of making an information system wholly or partially inoperable by means of a computer attack.

32 Denial of service makes a website or online service unavailable by overwhelming it with traffic from multiple sources.

33 Website defacement changes the appearance or content of an Internet site and compromises data integrity.

34 The United Nations Organization (UN) is an international organization created on October 24, 1945, that includes 193 member states, whose objectives are to facilitate cooperation in international law, international security, economic development, and social progress in order to foster world peace.

35 The International Telecommunication Union (ITU) is the United Nations agency responsible for developing information and communication technologies among states and the private sector.

36 The World Summit on the Information Society (WSIS) is a world forum organized by the International Telecommunication Union, a UN agency.

37 "NATO computer incident response capability" or NCIRC.

38 Adopted on November 23, 2001, at the International Conference on Cybercrime, the Budapest Convention came into effect on July 1, 2004, and represents the first international treaty on crimes committed via the internet and other computer networks.

39 Source: Council of Europe, Explanatory Report to the Convention on Cybercrime, [2001], STE n°185, p. 4. As of 25 March 2018, 56 states had joined the Budapest Convention. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

40 Council of Europe, "Convention on cybercrime," op. cit., Ch. II, Title 4, art. 10.

41 Europol (European Agency for Law Enforcement Cooperation) is a European police agency created in 1995 to facilitate operations against major international crime. It has 28 member states and works with several partner states that are not members of the European Union. It facilitates information sharing on cybercrime between national police forces.

42 Eurojust is a body of the European Union created in 2002 to improve the coordination of judicial investigations and prosecutions among EU member states in relation to cross-border organized crime.

43 The criminals sent bank employees phishing emails with a malicious attachment mimicking a legitimate company. Once downloaded, the malicious software allowed the criminals to remotely control the victims' infected computers, thereby giving them access to the internal bank network, which in turn enabled them to infect the servers controlling ATMs.

44 DISCLAIMER: The opinions expressed in this paper do not necessarily reflect the views of the General Secretariat of the Organization of American States or the governments of its member states, but represents that of the authors.

45 World internet usage and population statistics- December, 2017 – Update, accessed at: https://www.internetworldstats.com/stats10.htm.

46 Open-ended intergovernmental expert group meeting on cybercrime- https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-meeting-on-cybercrime.html.

47 Convention on Cybercrime- https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

48 For example, at the regional level, the Organization of American States adopted Á Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, in which member states agreed to coordinate their efforts to enhance cybersecurity (http://www.oas.org/en/sms/cicte/Documents/OAS_AG/AG-RES_2004_(XXXIV-O-04)_EN.pdf). At the international level, the consensus report of the United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, adopted in July 2015, recommended that states consider the following norm of responsible behavior: "States should consider how to best cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats." Report, paragraph 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

References

Chapter 4. Crime Prevention Approaches

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. Retrieved from 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. Retrieved from 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-seguri-

dad-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 Pre-

vention. 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.

Contributions

Confronting the issues of digital crime

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

CHAPTER 5

PUBLIC-PRIVATE PARTNERSHIPS IN CYBERCRIME PREVENTION

The fifth and final chapter tackles the question of public-private partnerships in cybersecurity, particularly in relation to cybercrime prevention. The chapter begins by defining the concept of the public-private partnership before examining its emergence into crime prevention. The second part of the chapter provides an overview of public-private partnerships in cybercrime prevention, followed by a description of the stakeholders in these types of partnerships and of their partnership implementation and development approaches, including the specific components thereof. Third, comes a brief survey of international public-private partnerships and national strategies focusing on cybercrime prevention. Fourth, comes a discussion on the issues encountered in such partnerships. This chapter concludes with a few recommendations.

Introduction

Since the end of the 20th century, the private sector has taken on an increasingly prominent role in a number of national security-related sectors, in particular, critical infrastructure protection, cybersecurity, port security and energy management (Busch & Givens, 2012). One reason for this increasing importance of the private sector in these areas is technological change, which has reinforced two trends: globalization and privatization. These two processes decrease the importance of the state and also have implications for security (Dunn Cavelty & Brunner, 2007). Moreover, the growing importance of the private sector has encouraged the proliferation of public-private partnerships (PPPs), thereby increasing collaboration between the public and private sectors (Busch & Givens, 2012).

It should be noted, on the other hand, that one of a government's fundamental roles is to ensure the security of its citizens. Indeed, the state, in our modern perception, is widely considered to be responsible for the provision of security services. In fact, security is considered to be its most important responsibility (Etzioni, 2017). Consequently, any delegation of responsibility in this area to the private sector is likely to prove a very sensitive matter (Dunn Cavelty & Suter, 2009).

At the same time, as we shall see below, the private sector has become increasingly involved in crime prevention since the 1980s. For many, including the UN (ICPC, World Bank Sustainable Development Department for Latin America and the Caribbean, Bogota Chamber of Commerce, & Instituto Sou da Paz, 2011), crime prevention requires partnerships among a multitude of actors, from both the private and public sectors. The same observation is often made in relation to cybercrime. In that light, the object of this chapter is to discuss PPPs, particularly in the area of cybersecurity, in order to identify their characteristics and the attendant issues, as well as consider some concrete examples. The previous chapter identified different cybersecurity approaches to digital infrastructure protection and cybercrime. However, the lack of available information makes it difficult to study models of PPPs focusing exclusively on cybercrime. It will therefore be instructive to focus on the PPPs in general, while providing examples of cybersecurity PPPs where possible.

What is a public-private partnership?

The recourse to PPPs has been growing in popularity since the 1990's. This trend is due to the increasing privatization of critical infrastructure, which governments see as economically advantageous (Carr, 2016; Forrer, Kee, Newcomer, & Boyer, 2010; Manley, 2015). It is apparent that PPPs are not unique to cybersecurity and cybercrime prevention; such arrangements are employed in a range of contexts to manage various issues, including in the areas of security and crime prevention. While they are increasingly employed around the globe as solutions to an array of government-related issues, some ambiguity remains as to their exact definition (Weihe, 2005). Indeed, there are a number of varied definitions of PPPs..

For example, the European Union Agency for Network and Information Security (ENISA), described in greater detail later in the chapter, defines a PPP as "an organised relationship between public and private organisations which establishes common scope and objectives, and uses defined roles and work methodology to achieve shared goals" (ENISA, 2011a, p. 10).

The Canadian Council for Public-Private Partnerships (CCPPP), for its part, offers the following definition of the PPP: "a cooperative venture between the public and private sectors, built on the expertise of each partner, that best meets clearly defined public needs through the appropriate allocation of resources, risks and rewards" (The Canadian Council for Public-Private Partnerships, 2016). The US's National Council for Public-Private Partnerships offers a similar definition:

> "a contractual arrangement between a public agency (federal, state or local) and a private sector entity. Through this agreement, the skills and assets of each sector (public and private) are shared in delivering a service or facility for the use of the general public. In addition to the sharing of resources, each party shares in the risks and rewards potential in the delivery of the service and/or facility" (Bechkoum, Thomas, Campbell, & Brown, 2017, p.8)

What these definitions make clear is that PPPs differ from contractual agreements, wherein the public sector, that is, the government, subcontracts to a private company to carry out a specific project (for example, construction of a bridge or building). The difference lies in what is shared between the partners: resources (property, skills, expertise, and financing), risks and benefits (Bechkoum et al., 2017).

Although the definitions of PPPs are varied, they generally share some characteristics. Li and Akintoye (2003) and Forrer et al (2010) state that, in the first place, the relationship between the partners must be stable, long term and continuing: PPPs differ from sporadic, one-off transactions. Secondly, a critical aspect of PPPs is the sharing of responsibilities regarding outcomes and activities. This type of relationship differs from endeavours in which the government consults the private sector for advice and recommendations on policies while maintaining control over said policies. The sharing of responsibilities, however, gives rise to some important considerations regarding accountability, which we will address later in this chapter. Li and Akintoye (2003) also indicate that this partnership must include at least one participant from each sector. Each participant must also be in a position to negotiate on its own behalf, without having to defer to other sources of authority. Finally, Forrer et al. (2010) state that the private sector must participate in the decision-making processes, not only regarding the development of goods and services, but also in deciding the best way to offer them to the public.

Manley (2015), moreover, lists two desirable outcomes of a PPP. The first is that the collaboration and the sharing of resources give rise to a synergy between the participants. The second is that one or more of the organizations in the partnership is transformed by the process.

The public and private sectors are often seen as two separate and fundamentally distinct entities. This dichotomy is further accentuated by the fact that the values attributed to each are apparently in contradiction. One of the sectors is seen as virtuous by some and the other is seen as corrupt by others; one appears to value community and solidarity, while the other seems to put the individuals and their interests first. (Etzioni, 2017). This vision of the public and private spheres may obviously vary from one country to another based on institutional differences. For example, a very clear distinction exists between the public and private sectors in the US in particular, and is presumed to underlie American legal thought (Etzioni, 2017). This dichotomous view of the two sectors is not, however, universal. In the social sciences, a number of experts hold that the distinction between public and private is more nebulous than public discourse would have us believe, and that public and private organizations should be represented as falling along a continuum, rather than as a dichotomy (Etzioni, 2017).

Public-private partnerships in crime prevention

The goal of this section is to briefly discuss the emergence of public-private partnerships in crime prevention.

As emphasized in the UN guidelines on crime prevention, effective prevention should rely on partnerships between a multitude of actors: government ministries and institutions, associations, NGOs, civil society and business (UNODC, 2011). In practice, however, although civil society has long been active in crime prevention and in the promotion of public safety, the involvement of the private sector is a more recent, but growing, phenomenon (ICPC, 2011).

Throughout the 1980's and 1990's, public-private crime-prevention partnerships were essentially limited to protecting commercial properties, gated communities, and private residences (ICPC, 2011). These measures used a situational crime prevention approach, the objective being to maximize the risks and minimize the benefits of a criminal act without addressing the root causes of crime. The private sector, for that matter, is generally less interested in activities targeting the social causes of crime. As Capobianco writes: "Corporate cultures, which are grounded in firm targets and visible solutions, may not be easily reconcilable with social development projects whose benefits may be unclear, difficult to measure, or long term" (2005, p. 17). It follows that crime-prevention PPPs tended to favour initiatives using a situational prevention approach over other crime prevention approaches.

There is, however, a gradually emerging trend of second-generation PPPs that are adopting a more social and community-oriented approach. Initiatives carried out under these partnerships include, for example, support for prevention pilot projects or research to develop crime-prevention measures (ICPC, 2011).

Mobilizing the private sector to participate in crime prevention is, however, no simple task. First of all, in matters of security, prevention (as opposed to repression) is rarely a government priority; a weak commitment by the public sector is not conducive to strong mobilization of the private sector which, as a matter of course, does not see crime prevention as a priority. (Avina, 2011; ICPC, 2011). Moreover, fearing the potential repercussions on their reputations, companies may be hesitant about being associated with crime-prevention initiatives. They may, for example, be apprehensive that their involvement in crime prevention could be perceived as an attempt to correct past mistakes or that such involvement will publicly link their government with an issue that tarnishes the country's reputation (Gardiner, 2009).

Mobilizing the private sector to invest in a crime-prevention partnership is even more problematic when it does not appreciate the potential benefits of such an action. On the other hand, the issue of cybercrime changes this outlook considerably: this type of crime can not only directly undermine a company's security, but the commission of such crimes necessarily involves the use of privately owned networks and systems. It follows that the role of the private sector in crime prevention is invariably transformed by a type of crime that involves the private sector itself.

Public-private partnerships in cybersecurity

In recent years, approaches to cybersecurity have been largely based on the idea that it's necessary to recognize the role of the private sector in the security of information networks and that partnerships between the public and private sectors must therefore be established (Tropina, 2015). As Germano (2014) states, the multifaceted nature of cybersecurity issues has considerably influenced the modes of interaction between governments and the private sector. The general consensus is that governments are not equipped to fight cybercrime without the involvement of the private sector. That said, a number of questions remain to be answered: What should be the respective role of each entity? What form should the cooperation between the two sectors take? Should government intervention be kept a minimum, or would this likely lead to excesses by the private sector? What approaches should be favoured when developing and implementing prevention PPPs in cybersecurity? This section will discuss these questions and examine current PPPs in cybersecurity.

What is a public-private partnership in cybersecurity?

For the purposes of this chapter, we will adopt the definition of a PPP in cybersecurity as presented by Bechkoum et. al., which is:

> "a collaborative agreement whereby government or public organisations engage in cooperative ventures with industry or academia to mitigate cybersecurity risks through enhancing cyber defence capabilities, cooperation and information sharing." (2017, p. 8)

Actors in cybersecurity public-private partnerships

a) Description of actors

A simple public-private dichotomy does not adequately reflect the complexity and diversity of the actors participating in a PPP, particularly when it comes to cybersecurity. As Carr points out:

> "It should be noted also that the public-private partnership in national cybersecurity is multifaceted. Governments have diverse relations with internet service providers (ISPs), multinational information corporations (Google, Facebook, etc.), private cyber-security firms, promoters of human and civil rights, law enforcement agencies and civil society." (2016, p. 45)

ENISA, mentioned earlier in the chapter, is a European Union (EU) agency created in 2004 with the mandate to provide a high level of security for networks and information. It acts as a centre of expertise for the EU, its member states, its citizens, and the private sector. ENISA works with these different actors to develop advice and recommendations on sound information security practices. In particular, the agency helps EUmember-states comply with relevant EU legislation, and works to improve the resilience of Europe's critical infrastructure and information networks (ENISA, 2017b).

In keeping with its mandate, in 2017, ENISA conducted a study of the cybersecurity PPPs currently operating in Europe, in order to identify issues common to member states, as well as pinpoint best practices (ENISA, 2017b). Based on a review of the literature and interviews with private and public sector stakeholders from 12 EU member states, the report's authors identified the types of participants typically involved in cybersecurity PPPs:

- private sector service providers;
- cybersecurity agencies;
- research agencies;
- the relevant national authorities;
- law enforcement agencies;
- public sector service providers;
- other types of organizations;
- national intelligence agencies.

According to the ENISA study, private providers of services were the stakeholders most frequently involved in partnerships, followed by cybersecurity agencies, research agencies and relevant national authorities. The types of stakeholders invited to participate naturally depends largely on the objectives of the partnerships and the projected areas of action. For example, the European Financial Coalition against Commercial Sexual Exploitation of Children Online (EFC), one of the few examples of a cybercrime-related PPP, assembles European law enforcement bodies, in particular, the Italian, Swedish, Swiss and Danish police.[56] The involvement of non-governmental organizations (NGOs) is also a noteworthy trend that Dupont (2016) identified in his study of initiatives in international cooperation to fight cybercrime. Indeed, NGOs spearheaded 33 percent of the initiatives analyzed, and among the main groups of stakeholders represented in the category of NGOs were associations that defend children's rights (2016).

In short, it is important to consider the multiplicity of stakeholders' apt to fall under the more generic terms "public sector" and "private sector." Nevertheless, for the sake of simplicity, these terms will be used throughout this chapter.

b) Motivations for forming or joining a public-private partnership

The private and public sectors each have their own reasons for either participating in or developing cybersecurity PPPs. That said, certain motivations are common to both sectors.

We will first examine public sector motivations for creating or joining a PPP, then the motivations typically found in the private sector, and finally, the motivations common to both sectors.

Public sector motivations

A primary motivation of the public sector for creating or par-

ticipating in a PPP is to **facilitate the implementation of a national cybersecurity strategy (**ENISA, 2011b). The national strategy may, for example, require the implementation of a mechanism for sharing information with the private sector. Such a mechanism can take the form of a PPP. The government may also find itself with insufficient wherewithal to implement the national strategy by itself; a partnership with the private sector would facilitate the implementation of such a strategy and provide the government with access to a range of private sector resources.

Beyond the national cybersecurity strategy as such, the public sector may also envisage a PPP as a means of **obtaining the private sector's participation in cybersecurity** more generally. It is the government's responsibility to ensure the protection of critical infrastructure (see Box 5.1). That said, in a number of industrialized countries, the private sector is the principal owner-operator of these critical infrastructure systems (Carr, 2016). It is, therefore, essential for the government to establish a mechanism that ensures the private sector's involvement in the protection of critical infrastructure. A PPP can and will facilitate such involvement.

Box 5.1. **Protection of critical infrastructure: an essential element of cybersecurity**

Public Safety Canada defines critical or essential infrastructure as:

> "…processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence." (Public Safety Canada, 2017)

The US and the United Kingdom (UK) have similar definitions, to the effect that compromising, damaging or destroying critical infrastructure systems would have a severe impact on national security, national economic security, public health, or any combination of the above (Carr, 2016).

For this reason, critical infrastructure protection has for years been at the forefront of debates about cybersecurity. It is, therefore, alongside the economy, one of the key areas targeted by the national cybersecurity strategies of the US and the UK (Carr, 2016).

As Carr (2016) explains, the government is seen as responsible for ensuring security, specifically national security. The protection of critical infrastructure is, therefore, seen as an integral part of a government's national security mandate. Indeed, a large-scale cyberattack on a country's critical infrastructures could have such devastating consequences that the government must acknowledge its responsibility in this matter. It follows, as Carr points out, that national cybersecurity strategies make critical infrastructure protection a central concern. Whereas many aspects of cybersecurity are linked with a nation's interests, the protection of critical infrastructure is fundamental to the safeguarding of national security (2016).

However, critical infrastructure systems in many industrialized countries—water supply, wastewater treatment, electricity, financial systems, communications, and transportation—have been privatized in recent years. It follows that, in order to ensure the security of these systems, the government must establish relations with their owner-operators, that is, the private sector. Dunn-Cavelty and Suter, moreover, hold that cooperation between government and the private sector in protecting critical infrastructure is not only useful, but henceforth inevitable (2009).

Accordingly, protecting critical infrastructure has become a key cybersecurity issue for many governments, and PPPs have become the preferred vehicle to facilitate this protection. Carr, moreover, in her study of national cybersecurity strategies (2016), explains that in countries where critical infrastructure systems have been privatized, PPPs occupy an important place in national cybersecurity strategies as a mechanism for limiting attacks.

The public sector may also consider it advisable to develop or join a PPP to **coordinate different initiatives** designed to combat cybercrime. In particular, a PPP offers the possibility of creating synergies between different private sector initiatives which would otherwise operate independently of one another (ENISA, 2017b).

Finally, the public sector may decide to develop a PPP in order to **assist the private sector in applying new statutory regulations**. For example, in the framework of the ENISA study on European PPPs in cybersecurity (2017b), some of the European experts interviewed mentioned the fact that new European regulations—for example, the Directive on security of network and information systems (NIS Directive), adopted on July 6th 2016 by the European Parliament and the Council of the European Union (ANSSI, 2016), or the General Data Protection Regulation (GDPR), adopted by the European Parliament on April 14th 2016—imposed particular obligations on the private sector. As a consequence, governments decided to form partnerships aimed at helping the private sector comply with these new regulations.

Private sector motivations

One characteristic private sector motivation for developing or participating in PPPs is to **exercise influence over the regulatory framework** in terms of public policy and/or legislation on cybersecurity. A partnership with the public sector can give the

private sector a voice in future national strategies and other cybersecurity-related policies and legislation. A PPP can also serve as a feedback mechanism, enabling the private sector to communicate with governments regarding the obligations it sees as too restrictive, inappropriate or unrealistic (ENISA, 2011b). The private sector's economic interests, i.e., protecting its commercial interests and avoiding costly obligations imposed through legislation, are often central to its motivation for participating in a PPP (ENISA, 2017b).

A private organization may also be confronted with a cybersecurity problem requiring solutions which are beyond its organizational capacities (ENISA, 2011b). The organization may therefore view a partnership with other actors as the only means of **overcoming its limitations.**

The private sector may also view joining a partnership as a way of **advancing its private interests**. Dupont, for example, notes that in the area of international police cooperation against cybercrime, companies such as Microsoft, Symantec and Telefonica:

> "[...] do not hesitate to deploy their technical and legal capacities in a more or less coordinated manner with certain national and international law enforcement institutions to advance their private interests, whether it be to maintain the confidence of consumers in their products or to convince the latter that their solutions are superior to the ones offered by their competitors" (2016, p. 117)

Motivations common to both sectors

Access to resources is a typical motivation for both the private sector and the public sector alike (ENISA, 2011b). For the private sector, a PPP is a means of gaining access to public funds or to privileged public-sector resources such as confidential information. Although the private sector is typically seen as a stakeholder with the potential to contribute substantially to a cybersecurity partnership, particularly in terms of resources (both technical and financial) and expertise. Germano (2014) reminds us that the public sector also has many strengths that should not be overlooked. Public authorities can investigate, arrest and prosecute cybercriminals; collect foreign intelligence on cyberthreats; offer statutory protections to companies that share information with the government; analyze information from domestic and foreign sources before it is available to the private sector; and gather and disseminate information to different industries and companies. Through the aforementioned capabilities, the government is able to enhance the understanding of a threat, thereby facilitating the development of risk mitigation and protection measures that benefit potential victims (Germano, 2014). The public sector, through a PPP, can access resources such as expertise to help develop standards and good practices, and information that provides it with a more detailed understanding of the critical information infrastructure protection (CIIP) measures implemented by the private sector (ENISA, 2011b). These partnerships also give each sector access to direct and credible contacts with other organizations and, thereby, to sources of experience and knowledge. The public sector may not, for that matter, have sufficient resources to mobilize or motivate many smaller actors, which are nonetheless relevant in creating a cybersecure environment, for instance small and medium-sized businesses. The private sector, on the other hand, may dispose of the wherewithal (i.e., the financial and other resources) to reach a broader spectrum of actors.

In addition to the sharing of resources, the **sharing of the risks and costs** associated with providing a service to the public is a major motivation for both the public and private sectors (Kaijankoski, 2015).

The forming of PPPs may, in some cases, be mandated by **new regulatory requirements**. In certain instances, the public authorities may deem that the best way to ensure that a law is effectively applied would be through a PPP. Such laws might, among other things, deal with emergency or crisis management. A particular law may also specifically cover PPPs, stipulating the terms of cooperation and joint action. These laws typically cover PPPs in general, rather than specifically focusing on cybersecurity-related laws. Finally, under certain laws, the participation of a given private sector organization in a PPP may be stipulated as a statutory requirement (ENISA, 2011b).

A PPP may also be formed with the goal of **improving coordination** between different sectors. Public and private organizations may recognize that information-sharing is inadequate, or that there exists an unnecessary duplication of activities which can be remedied through a partnership. Coordination between sectors such as communications and information technology is also essential, as the boundaries between these two sectors become increasingly vague (ENISA, 2011b). Moreover, a climate of distrust may sometimes exist among competitors in a particular region or sector. A PPP facilitates recourse to an external mediator to ensure coordination between parties, who would otherwise be less inclined to cooperate.

Another reason to form a PPP might be to **ensure that cybersecurity is regarded as an important item on the collective agenda** by both the government and private sector in order to generate and promote mobilization among stakeholders (ENISA, 2017b).

PPPs also constitute a means of **adapting to the changing nature of threats**, which are either assuming new forms (cyberterrorism, for example) or becoming increasingly international in scope (ENISA, 2011b). As Germano states, "the private sector often needs the government's help to reach across borders and develop comprehensive international solutions to tracking, identifying, and mitigating cyberthreats" (2014, p. 2).

Finally, PPPs help the public and private sectors **reduce their vulnerabilities** in the wake of attacks, should they occur (ENISA, 2011b).

ENISA (2017b) emphasizes that PPPs are typically formed in response to a range of considerations, and not for one single reason.

Implementation and development of a public-private partnership in cybersecurity

Various approaches can be used to implement and develop a PPP. Regarding cybersecurity, ENISA (2017b) has identified different possible combinations in terms of both implementation and development.

a) Public-private partnership implementation approaches

With respect to implementation, the two main approaches are top-down and bottom-up. When a PPP is implemented using a **top-down approach**, it is generally formed as the result of a government directive or action plan calling for its formation. On the other hand, a partnership stemming from a **bottom-up approach** is generally the result of a need identified by a community which then mobilizes through a partnership to address this need. According to stakeholders interviewed for an ENISA study (2017b), a PPP in cybersecurity that is formed in response to needs identified by the private sector—in other words, through a bottom-up approach—is much more likely to be dynamic and successful.

b) Public-private partnership development approaches

Following its implementation, a PPP can be developed in a number of ways. In a partnership implemented using a top-down approach, the government may go about member recruitment on its own. On the other hand, in some cases, the development of the partnership is bottom-up; therefore,, despite the partnership's formation being government-mandated, decisions regarding the parties in charge and partnership members are not made exclusively by the public sector – the private sector is actively involved in partnership decisions and development. In fact, this **combination of top-down implementation and bottom-up development** is the model used by more than two-thirds of the PPPs in cybersecurity analyzed by ENISA in its study (2017b). The reverse is also possible: a group of actors might identify a need and form a partnership to respond to the need, and then subsequently approach a government authority to obtain support for the initiative. The government may make financial contributions or confer upon it a degree of authority to develop the partnership. In this case, the **combination is one of a bottom-up implementation and a top-down developmen**t.

A public-private partnership may also be developed independently of the structure used to create it. As ENISA states:

> "A central body, often government led, creates a defining structure for a partnership, promotes its use but once the partnerships are created they are autonomous. A start-up kit may be supplied which may include tools and the ability to buy or register for services such as warnings or alarms (in case of a cyber attack)" (2017b, p. 17)

Finally, as the PPP develops, restructuring might be required to optimize its effectiveness. To this end, it might split into sub-groups, each with its own specialization or specific objective. The information gathered by these sub-groups is generally more specific, and the smaller group size builds trust among members—a key determinant of PPP success. This will be examined in greater detail later in the chapter. Conversely, it may be advisable for a number of PPPs to merge, particularly when they share common issues, competencies or objectives.

Components of a public-private partnership in cybersecurity

In 2011, ENISA published its first report and good practices guide on effective models of cooperation for public-private partnerships in cybersecurity. Based on the PPPs studied, ENISA developed a taxonomy of public-private partnerships based on seven components:

- **Governance Structure.** This component covers how the PPP is organized, how partners cooperate, its rules, and financing.
- **Scope.** This component refers to the aspects of security and resilience addressed by the PPP. The partnership's scope shall determine the services it offers and orient its activities in accordance with the stages of a life-cycle model of security (described below). In other words, the scope determines whether the partnership will seek to prevent cyberattacks, to respond to them, or both.
- **Services.** This component lists the types of services the PPP offers in addressing its scope, which includes, for example, information sharing and running exercises to simulate attacks on partners.
- **Threat.** This component covers the types of security threats that the PPP considers within its scope.
- **Coverage.** First of all, this component concerns the geographical extent of the partnership; that is, the geographic location of the partners, i.e., is it a regional, national or international partnership? It also refers to the partnership's sectoral dimension: does the partnership deal with a particular issue, an entire sector (e.g., financial), or is it cross-sectoral?
- **Development.** This component describes how the PPP was establised, how it evolved and grew, as well as the incentives used to encourage and maintain partner participation.
- **Links.** The final component describes what links the PPP has with other PPPs and organizations outside its immediate membership.

In the following discussion, we will focus in particular on the second and third components, i.e., the partnership's scope and its

services. As we will see, these two components, and more particularly the scope, determine whether the partnership adopts a preventive approach to cybersecurity.

a) The scope or objectives of a cybersecurity public-private partnership

As previously noted, the security objectives of a partnership will correspond to one of the stages of the cybersecurity life cycle, as indicated in Figure 5.1.

- **Deterrence.** A PPP with a deterrence-oriented scope will focus on discouraging attacks by cybercriminals. Its services might therefore include raising awareness about law enforcement measures or about cybersecurity and the consequences of an attack for cybercriminals.
- **Protection.** To strengthen the protection of systems, PPPs with this objective work to develop new industry standards and foster information-sharing communities. To this end, they compile information on the latest security threats and protection mechanisms.
- **Detection.** PPPs with a detection-oriented scope study new cybersecurity threats to understand and better address them. They rely on information sharing and early warning systems to achieve this objective.
- **Response.** A response-oriented PPP will develop partners' capacity to cope with and respond to the initial impact of an attack or emergency. For example, this might include services such as simulations where partners practice their response to attacks, emergency planning and crisis management.
- **Recovery.** A PPP with a recovery-oriented scope will develop the capabilities of its members to resume operations and make necessary repairs in the aftermath of an attack. In other words, it will work to return systems to business as usual.

b) Services offered by a public-private partnership in cybersecurity

PPPs in cybersecurity may offer a wide range of services to members. ENISA (2017b) identifies, among others, the following services: crisis management and incident handling; research/analysis (to develop more secure technologies, for example); development of good practices guides and avenues of action; information sharing; early threat alerts; exercises and simulations that allow partnership members to practice their response to an attack; sensitization to threats; technical assessments; benchmarking; strategic, emergency and resilience planning; risk analysis. The specific services offered will of course vary in accordance with the partnership's scope.

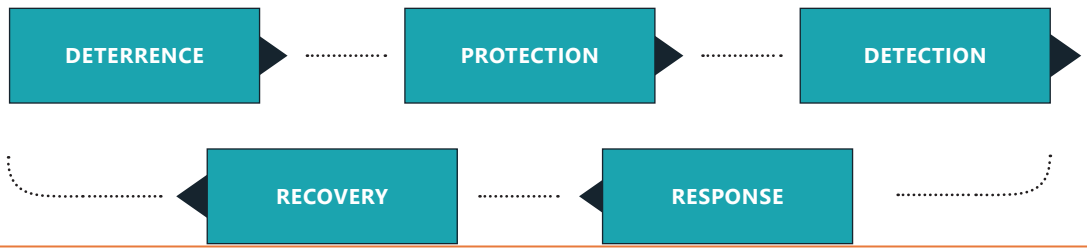
c) The main types of public-private partnerships in cybersecurity

ENISA has identified a typology of PPPs based on the stage of the cybersecurity life cycle the partnership aims to address. In other words, the scope or objectives of the partnership is central to this typology. The three main types of PPPs are: partnerships focusing on prevention, partnerships focusing on response, and partnerships focusing on the entire cybersecurity life cycle. As ENISA (2011b) explains, all of the PPPs identified in its study correspond to one of these three types, demonstrating that, despite the wide range of countries, legal frameworks, cultures and organizations extant, there obtains a similarity and simplicity in terms of the approaches followed.

Prevention-focused public-private partnerships

These PPPs focus on deterrence, protection and detection (insofar as the partnership seeks information on new cyberthreats to better understand them). It is clear then that the prevention approach is circumscribed, with a focus limited to imminent threats and reducing opportunities for the commission of crimes. Rather than focusing on immediate threats, these partnerships instead adopt a long term view of cooperation. Partnership members endeavour to learn from one another and apply this knowledge for the duration of their collaboration. It follows that the benefits of participating in this type of partnership may not be immediate, meaning that the partnership will require private sector stakeholders in a position to invest in its activities without the promise of immediate returns. These PPPs are generally spearheaded by the stakeholders from the private sector that are responsible for longer term national interests (ENISA, 2011b).

FIGURE 5.1. **The cybersecurity life cycle**



Services offered by a prevention-focused partnership would include, for example, good practices guides, information sharing, early reporting of system vulnerabilities, exercises and simulations, awareness raising, technical assessments and standards setting.

Response-focused public-private partnerships

The aim of response-focused partnerships is to ensure the appropriate response during an attack and during the post-attack recovery phase. These partnerships may, therefore, have short term objectives, i.e., responding immediately during an attack, or long term objectives aimed at implementing or improving the mechanisms that enable a rapid response. The value of these partnerships would therefore appear to be clearer to private organizations, which are in a better position to lead such initiatives. On the other hand, the public sector may also initiate this type of partnership, for instance in the wake of a major attack such as 9/11. These partnerships generally mobilize members with strong technical capabilities in order to ensure rapid response during cyberattacks (ENISA, 2011b).

The services offered by these partnerships would include, among others, crisis management, and emergency and resilience planning.

Umbrella public-private partnerships

Umbrella partnerships have the capacity to develop and implement actions at every stage of the cybersecurity life cycle. These partnerships can take various forms. They may, for example, encompass a range of stakeholders with numerous roles, competencies and responsibilities. To coordinate such a large number of partners, sub-groups focusing on specific subjects or sectors are typically formed. Another type of umbrella partnership is a small organization assembling the senior representatives of various response or prevention-oriented partnerships (ENISA, 2011b).

International initiatives and national strategies

This section will discuss a number of cybersecurity PPPs, and more particularly, those adopting the prevention-oriented approach discussed above. International initiatives will be presented first, after which, we will examine national cybersecurity strategies including a PPP component.

International initiatives

Given the international nature of cyberspace, it is logical for countries to enter into international agreements—whether bilateral or multilateral—to regulate it and, potentially, to coordinate cybersecurity initiatives. This section will discuss two such initiatives. The first, the Forum of Incident Response and Security Teams (FIRST), is particularly prominent at the global level due to the large number of stakeholders it mobilizes. The second, the European Public-Private Partnership for Resilience (EP3R), an initiative that ended in 2013, illustrates certain aspects of cybersecurity PPPs at the pan-European level.

a) The Forum of Incident Response and Security Teams

Dupont (2016) rejects the hypothesis that policing and judicial institutions have difficulty adapting to a constantly evolving digital environment. His review of 51 international multilateral initiatives to combat cybercrime shows that since the 1990s, a multitude of "hybrid networks of national police agencies, international organizations, non-governmental stakeholders, professional associations and businesses" (Dupont, 2016, p. 96) has developed for that purpose.

Dupont observed the decisive role played by the private sector in these international initiatives. Of the 657 stakeholders involved, 47 percent (a total of 312) are private businesses, and at least 12 percent of the initiatives analyzed were spearheaded by the private sector (Dupont, 2016). Among these is the Forum of Incident Response and Security Teams (FIRST), developed by the private sector to coordinate the international response to cyber-related incidents.

This initiative is worthy of particular attention. As Dupont (2016) explains, FIRST includes the largest number of stakeholders, for the most part companies of all the initiatives analyzed. At present, FIRST appears to have more than 400 members representing 85 countries (FIRST, 2014). Its membership mainly consists of Computer Emergency Response Teams (CERTs), also known as Computer Security Incident Response Teams (CSIRTs). These official bodies are tasked with providing risk-prevention services and assistance in handling cyber incidents. They may be spearheaded by a range of stakeholders: governments, business, universities, law enforcement, etc. (Global Forum on Cyber Expertise, 2017). FIRST functions as a global umbrella organization representing these response teams. In addition to FIRST's large number of CSIRT members, it is also open to individuals and representatives of organizations. The majority of stakeholders involved in FIRST "have no other channel of communication and exchange with the initiatives or other stakeholders making up the global network" (Dupont, 2016, p. 116). In other words, FIRST controls the flow of communication between a large number of stakeholders involved in international initiatives to combat cybercrime.

Based on ENISA's typology, FIRST corresponds to a PPP model focused largely on the prevention of cyber incidents. Indeed, the forum's objectives are to encourage cooperation and coordination in the prevention of cyber-related incidents and promote information sharing between CSIRTs worldwide. In the furtherance of these objectives, FIRST not only maintains an international network of intervention teams, but also offers services such as the creation and sharing of tools, technical information,

methodologies and good practices, in addition to organizing and coordinating conferences to promote sound cybersecurity practices.[57]

b) The European Public-Private Partnership for Resilience

With respect to European PPPs, the case of the European Public-Private Partnership for Resilience (EP3R) was illustrative of many of the major issues encountered by regional or pan-European PPPs. This initial attempt to establish a Pan-European PPP to promote security and resilience in telecommunications was implemented in 2009 and ceased operations in 2013. It was intended to serve as a platform for sharing information on policies and practices to enhance the security and resilience of critical information infrastructure, define a framework to improve the coherence and coordination of security and resilience policies in Europe and identify and promote good practices (Irion 2013).

Dupré (2014) interviewed EP3R participants to gather information about the initiative, the issues encountered, and the lessons and recommendations learned. Although generally well received, a number of criticisms were voiced.

Firstly, more than half the interviewees reported a central issue that hindered their full participation in the partnership was that their organization was not adequately informed of the initiative's objectives and intended outcomes.

Moreover, the participants did not see tangible benefits deriving from their participation in EP3R. This spurred the departure of a number of members and significant turnover among participants. In turn, the resulting instability in personal networks hindered the development of trust among the partnership's members.

Another problem identified was that participation in EP3R activities, particularly travel to meetings, was at the participants' expense. In other words, participation largely depended on each member's resources. Some interviewees noted that there would have been positive outcomes such as increased participation and commitment to EP3R had funds been provided to participants.

Another issue raised by interviewees is that a number of major private sector actors were not participants. Such a limitation diminished the initiative's general appeal, particularly among small and medium-sized enterprises.

Finally, all interviewees mentioned that EP3R had failed to identify specific measures to achieve the intended outcomes. Moreover, many noted that a lack of knowledge on national legal standards and restrictions meant that the obstacles that certain participants might face were not considered and, as a consequence, the recommendations offered were not necessarily adapted to national contexts.

EP3R is obviously not the only major Pan-European PPP to address cybersecurity needs. For example, the European Commission reached a PPP agreement with the European Cybersecurity Organisation (ECSO)[58] in July 2016 under the auspices of the European cybersecurity strategy (ECSO, 2018). This PPP, which includes a 450 million euro financial commitment from the European Commission and three times that sum from the private sector, is intended to facilitate cooperation between public and private stakeholders, as well as build a competitive European cybersecurity market.

These new pan-European PPPs can capitalize on the experiences of EP3R to anticipate issues likely to hinder the participation of different stakeholders, as well as learn lessons apt to promote more successful outcomes.

National cybersecurity strategies

The following section will present a brief overview of national cybersecurity strategies which address public-private partnerships.[59]

A number of countries have recently created national cybersecurity strategies that emphasize some form of public-private partnership. Carr (2016) notes that this is true of Australia, Austria, Canada, the Czech Republic, Estonia, Finland, France, Hungary, India, Japan, Lithuania, the Netherlands, New Zealand, Slovakia, South Africa, the United Kingdom and the US. As noted above, many countries with privatized critical infrastructure systems (for example, in the transportation and financial sectors) have created national cybersecurity strategies that are of great value to PPPs, which are seen as key risk-mitigation mechanisms (Carr 2016).

In the US and the US, PPPs are frequently described as the cornerstones of their respective cybersecurity strategies (Carr, 2016). In both cases, the private sector owns and operates the bulk of the critical infrastructure. For this reason, the governments could hardly ensure the security of the national infrastructure without private sector collaboration (Etzioni, 2017). As it happens, the US is the first country to have created cybersecurity strategies that rely on PPPs, thereby influencing the development of similar strategies elsewhere. Such strategies first appeared in the early 2000s under the Clinton administration. Although in the years that followed, PPPs remained the centerpiece of the national strategy. The parameters and nature of the relationship between the two parties has never been explicitly defined (Carr, 2016).

In Europe, in keeping with ENISA requirements, one of the objectives common to all national cybersecurity strategies is collaboration (2017a, 2017b). This collaboration typically occurs through one of two structures: public-private partnerships and information sharing and analysis centres (ISACs). The latter are described in greater detail in Box 5.2 below.

Box 5.2. **Information Sharing and Analysis Centres**

ISACs are typically non-profit organizations that serve

as resource centres for gathering information on cyberthreats (generally those targeting critical infrastructure) as well as mechanisms for bilateral information sharing between the public and private sectors (ENISA, 2017a).

Dunn-Cavelty and Suter (2009) indicate that the first ISACs emerged in the US in 1999, following the recommendations of the Commission on Critical Infrastructure Protection, established by President Clinton in 1996. The Commission's report identified information-sharing among stakeholders in the field of critical infrastructure as the most pressing security need. The report recommended that the different sectors create public-private partnerships, organized as ISACs, with the purpose of sharing information regarding security, threats detected, and best practices (Dunn Cavelty & Suter, 2009).

As described by the US' National Council of ISACs:

> "Information Sharing and Analysis Centers (ISACs) help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency […] Most ISACs have 24/7 threat warning and incident reporting capabilities, and may also set the threat level for their sectors. And many ISACs have a track record of responding to and sharing actionable and relevant information more quickly than government partners." (National Council of ISACs, 2018)

There are many ISACs operating worldwide, frequently in specific sectors (World Economic Forum, 2017). In the US, for example, ISACs have been formed in the automobile, aviation, electrical and health sectors. Information exchange also occurs between different sectors concerned with critical infrastructure; ISACs collaborate and share knowledge about threats and mitigation measures through the National Council of ISACs (National Council of ISACs, 2018).

Certain European strategies stipulate specific actions under the auspices of PPPs. This is true, for instance, of the Czech Republic and Spain (Luiijf, Besseling, & Graag, 2013). The Czech national cybersecurity strategy (National Security Authority, 2015) prescribes, among other things, cooperation between the private and public sectors in the development of uniform security standards and the setting of a mandatory level of security for all stakeholders playing roles in critical information infrastructure. Likewise, Spain's national strategy stipulates the development of cybersecurity standards by means of public-private partnerships (Gobierno de España, 2013).

In addition to concrete measures regarding collaboration between the private and public sectors, certain strategies clearly define the roles delegated to each sector under the partnership. For example, Japan's national cybersecurity strategy indicates that companies must name a chief information security officer (CISO) tasked with ensuring the security, availability and integrity of information and data systems.

According to ENISA (2017b), a country's culture is one of the key factors influencing the implementation and operation of a PPP. As a result, a country's distinctive cultural traits, along with the character of the relationship between its public and private sectors, have considerable bearing on the approach most likely to ensure a successful partnership.

For example, in countries with a tradition of strong public administrations, there is a certain remoteness between the private and public sectors, which are disinclined to work together. In the event that a partnership is formed, the rules and objectives must be specified, often following the hierarchical model characterizing public administration (ENISA, 2017b). On the other hand, countries where the public authorities have less power tend to adopt a more pragmatic approach in creating such partnerships; thus, a legal framework is not necessarily required and, instead, confidentiality agreements may suffice (ENISA, 2017b).

This cursory overview examined the different ways PPPs may be envisaged in the context of a national cybersecurity strategy. As previously stated, ENISA offers a more in-depth discussion of the subject.

Issues

Partnerships formed between public and private actors with the objective of preventing and combating cybercrime often give rise to certain issues. Some of these issues derive from the nature of the stakeholders, others are inherent to the very structure of such partnerships.

Issues arising from the nature of the stakeholders: differences that are hard to reconcile

PPPs consist of stakeholders with different identities, as well as different interests.

a) Different institutional identities

Private and public stakeholders are characterized by institutional cultures and values, which are not only different, but conflicting. As Gal (2002) indicates, the public sector focuses on the community and sees its role as based on solidarity-based values; the private sector, on the other hand, puts individuals and its own specific interests front and centre. In this light, it seems a definite challenge to establish dialogue between these two spheres,

which may find it difficult to understand one another and speak the same language (ENISA, 2017).

In addition to these ideological obstacles, temporal issues also arise when the private and public spheres collaborate on cybersecurity. Private sector stakeholders must act quickly once an incident is detected. They are likely to be apprehensive that news of the event will spread and will want to allay the fears of their clients. It follows that private stakeholders are extremely responsive regarding the sanctioning of those involved, the dissemination of information regarding the event and the improvement of protection and prevention measures. In contrast, constraints stemming from the nature of government bureaucracies will cause public stakeholders to act much more slowly. This difference in the culture of the private and public spheres engenders issues when it comes to responding to incidents (Germano, 2014).

Moreover, when an incident occurs, public authorities, unlike private organizations, are bound by a duty to inform, which in this context means making the incident known and apprising the parties concerned. In contrast, the functioning and culture of the private sector dictate that it avoids divulging attacks or incidents to avoid undermining users' trust and tarnishing the company's reputation (Germano, 2014). This difference is exacerbated by the very concepts of incident and threat, which do not necessarily hold the same meaning for governments as they do for private stakeholders. Given this difference, the challenges and issues of cybercrime are bound to be viewed differently by these two groups (Germano, 2014).

b) Differing visions of public-private partnerships: divergent interests and expectations

As Carr (2016) writes, "successful public–private partnerships are either characterized by shared interests or, if the interests of the partners are not well aligned, governed by rules." However, in cybersecurity PPPs, interests are dissimilar and insufficient rules exist to structure such partnerships. In other words, one of the key problems encountered in PPPs is the discrepancy between the expectations and interests of one party to the agreement with respect to those of the other.

Interests dictated by divergent values

As stated above, the private and public sectors are informed by different values. Whereas the latter places a strong emphasis on the community as a whole and is committed to the public interest, the private sector is motivated by individual economic interests. Unlike public stakeholders, companies make decisions based on a business model that prioritizes profit margins and shareholder interests. Society's interests and the interests of private companies do not necessarily coincide; in fact, they often diverge. In effect, it is often difficult to assess the profitability – if any – of actions taken in the public interest (Carr, 2016). Fundamentally, the private sector makes its cybersecurity decisions based on a cost-benefit analysis of its investments, and not with an eye to the public interest and national security concerns which guide decision-making by public sector stakeholders (Carr, 2016).

The issue of privacy protection

One area where public and private interests are rarely in alignment is the question of protecting individuals' privacy and personal information. Here, clearly, the two sectors do not pursue the same objectives. The public sector gathers certain information with the declared aim of protecting the public, in particular by preventing terrorism. The private sector, by contrast, is motivated by marketing or business objectives. Moreover, since Edward Snowden's revelations about the mass surveillance of citizens by the US Government with the assistance of the private sector, companies are increasingly reticent to share their clients' data. In effect, they are endeavouring to avoid being associated with a system that is negatively perceived and the repercussions that this could have for their image and appeal to consumers and clients (Germano, 2014). Consequently, in a climate where more and more companies are using encryption to protect client and consumer information, the question arises regarding whether government authorities, which are mandated to protect the public, should be given access to the decryption keys. In such cases, the private sector is apparently putting its own interests first by refusing to provide this information when requested to do so by the authorities. This was, for example, the case in 2014 when Microsoft refused to provide certain information to the FBI (Dupont, 2016), and for that matter, continues to be the case with Apple, which is now using powerful encryption techniques that cannot be decrypted, not even by Apple, even when a warrant is presented (Etzioni, 2017). While this represents a step forward for cybersecurity and the protection of personal information from governments and law enforcement, some observers point out that it could however affect the work of national security agencies (Comey, 2014).

The public sector, for its part, seems increasingly intent on preventing companies from distributing the private information of users for purposes not authorized by the latter. We need only look at the American and Canadian governments' reactions to the revelations that Facebook shared details of 87 million users' accounts with the strategic communications firm Cambridge Analytica in March, 2018. Facebook CEO Mark Zuckerberg appeared before the US Congress in mid April 2018 to testify in response to Cambridge Analyrica's use of Facebook data for political purposes (Wong, 2018). Likewise, Kevin Chan, Facebook's head of public policy for Canada, was called to account before a House of Commons privacy committee in Ottawa in April, 2018 (Baillargeon, 2018).

A lack of private sector interest to enter into partnerships with the public sector

A number of authors have observed that many private sector companies often fail to see the value of entering into partnerships with public stakeholders (Dupont, 2016; Germano, 2014). Companies control their operations and infrastructure and often have financial, technical and human resources that surpass those of the public sector. Moreover, they are unconstrained by the bureaucratic, institutional and constitutional considerations that limit public actors (Dupont, 2016; Germano, 2014). Thus, over and

above the private sector's reticence to collaborate with the public sector owing to its distinct interests, as discussed above, it also sees itself as endowed with sufficient resources and capabilities to effectively deal with the challenges and issues of cybercrime. In that light, temporary collaborations, based on a company's needs in response to a real and tangible threat, would be preferable to a partnership based on a proactive approach (Germano, 2014).

c) Limited citizen participation

One observation emerging from the study of cybersecurity strategies is the relative lack of consideration given to citizens' potential to proactively help in fighting and preventing cybercrime. And yet, as Luiijf et al note, "most NCSS recognise the need for a society-wide approach: citizens, businesses, the public sector, and the government" (2013, p. 27). Nevertheless, most strategies do not include measures that give citizens an active role in developing and implementing cybersecurity and crime-prevention initiatives.

It is worth noting the generally limited role citizens play in PPPs focused on preventing cybercrime. In most cases, they are considered passive actors; some information is shared with citizens, often through public awareness campaigns urging citizens to secure their own systems. One example of this is Luxemburg's SECURITYMADEIN.LU platform, which offers applications and services intended to improve the cybersecurity of individuals and organizations.[60] In this perspective, citizens' contributions in fighting cybercrime are limited to individual preparedness, with no mutual exchange or collaboration with public or private entities.

Some initiatives, on the other hand, do call for input from the citizens when it comes to reporting incidents, particularly when they are the victims of such incidents. Signal Spam, a PPP in France, provides a national spam-reporting platform.[61] Internet users are asked to report what they consider to be email spam. Signal Spam then passes the information along to the competent authorities so appropriate action may be taken.

On the other hand, citizens are not invited to collaborate in creating solutions to prevent and combat cybercrime. Clearly, investigating such crimes requires a comprehensive, up-to-date knowledge of information and communications technologies, something which is not readily available to the average citizen. Such expertise is not only highly specialized, but access to it is also quite limited (Jakobi 2015).

Issues stemming from the structure of public-private partnerships

a) Stakeholder responsibility: a missing element in partnerships

Some observers (Paquet-Clouston, Décary-Hétu & Bilodeau, 2017) have observed that both the private sector, notably services providers or companies, and the public sector, notably legislators and law enforcement, seem to be evading their responsibilities in the field of cybersecurity. In effect, these stakeholders, each for its own reasons, tend to avoid taking adequate and appropriate measures to prevent and combat cybercrime. In the public sector, governments and lawmakers are reticent to introduce more and stricter legislative measures (Carr, 2016). As for law enforcement agencies, their measures to fight cybercrime, rather than integral parts of coherent cybersecurity strategies, seem instead to consist of disparate and isolated actions (Paquet-Clouston, Décary-Hétu & Bilodeau, 2017). For their part, private stakeholders refuse to accept or assume responsibilities stemming from a cyberattack, which either targets their clients and consumers or threatens national security (Carr, 2016). One can find clear evidence in recent scandals like the one involving Equifax, the US credit reporting agency whose clients had their personal information stolen (a case discussed in Chapter 2), or Facebook, whose clients' confidential information was used to achieve political goals by a third party. In the latter case, the actors in question, Facebook and Cambridge Analytica, point the finger at each other, with Facebook claiming that the communications company used the data for unauthorized purposes and Cambridge Analytica maintaining it received Facebook's approval.

This avoidance of responsibility at the individual stakeholder level can also be observed in PPP governance, where the issue of accountability often remains ill-defined, if not entirely absent (Carr, 2016). In other words, public-private partnerships, which are mechanisms of cooperation intended to make cyberspace secure and prevent or deter incidents, fail to set down clear rules of accountability (Carr, 2016).

b) Collaboration

Maintaining trust between the parties

One of the main obstacles to effective collaboration by the parties in a joint initiative, particularly a PPP, is the question of trust (Germano, 2014). The divergent values and interests discussed above may give rise to mutual mistrust and suspicion regarding the other party's capacity to take constructive and appropriate actions. In the event of an incident, given the public and private sector's divergent approaches to problem solving in terms of both reactivity and transparency, how can the private sector be sure that the public partner will not interfere with its operations (Germano, 2014)? As for public sector interlocutors, can they be confident the private sector will take the appropriate measures and be forthcoming about the incident? A case in point, is the Equifax affair. In effect, Equifax only disclosed the facts of the case more than a month after it discovered them and more than four months after the initial incidents. Similarly, in the name of national security, governments may enact laws and policies giving them greater control and supervision over online content. Such actions could force information and technology companies to limit or remove certain content, thereby exposing them to public censure in the name of protecting society and fighting terrorism. On the other hand, the public sector must be able to trust that online services will fulfil their role of monitoring and reporting illegal and/or dangerous content.

Beyond the difficulty of trust building between partners, there

exists the additional issue of maintaining such trust over the long term (ENISA, 2017). The majority of European PPPs identified in ENISA's study (2017) described maintaining the bond of trust between partners as an ongoing effort requiring both personal relationships and considerable time commitment. As a PPP evolves, the relationship of trust is vulnerable to weakening, for example, when new members join the partnership, existing members are not sufficiently active, or certain members take advantage of the partnership's services without contributing to carrying out the required pre-defined tasks (ENISA, 2017).

Information sharing

Information sharing is seen as a critical component in the fight against cybercrime (World Economic Forum, 2017). This function frequently forms the cornerstone of a PPP's activities. In the United Kingdom, for example, the Cybersecurity Information Sharing Partnership (CiSP) is an initiative of the government and the private sector to facilitate information sharing about cyberthreats (National Cyber Security Centre, 2018). In the US, the National Cybersecurity and Communications Integration Center (NCCIC) also serves as a central information-sharing platform, which enables a range of partners involved in cybersecurity and the protection of communications to coordinate and synchronize their activities (US-CERT, 2018).

Both the public and private sectors recognize the need to share certain information in order to better prevent and combat cybercrime. As has been made clear a number of times, no stakeholder can accomplish this objective acting alone. Moreover, as criminals are themselves sharing information in order to adapt to continual changes in technology, victims and the authorities charged with prevention and law enforcement must do the same (World Economic Forum, 2017; Germano, 2014). In short, the sharing of information is not only a tool for limiting the harmful effects of a cyberattack and assisting law enforcement, but it also serves to prevent incidents from occurring in the first place (World Economic Forum, 2017).

Nevertheless, as Carr (2016) observes, the sharing of information under a PPP raises three related issues. First of all, it can be difficult for a company to readily distinguish between a technical problem, a small-scale cyberattack and a large-scale attack with the potential for causing lasting damage. Moreover, for reasons previously identified, a company may view it as more prudent to attempt to apprehend and solve a problem before its competitors become aware of it. Sharing information regarding the company's vulnerabilities with public actors, particularly the police or the justice system, may conflict with its business interests; in effect, choosing to act unassisted may give it an edge over its competitors. Finally, a private security firm may be reluctant to share information with the government, knowing it could be disclosed to its competitors. The business model of private security firms is to obtain information with the object of reselling it, not disclosing it for free. The public partner, for its part, might be limited to only sharing certain classified information with stakeholders with the required security clearance (Carr, 2016).

Much reflection has been devoted to the question of how to overcome these difficulties and coordinate information sharing between public and private stakeholders. For example, in 2017, the World Economic Forum (WEF), an international organization of multinational companies, published a guide on public-private information sharing against cybercrime (World Economic Forum, 2017). This guide first discusses the importance of information sharing, as well as the difficulties it presents, before turning to three key questions: what type of data should be shared?; with whom?; and how? Regarding the **type of data to be shared**, the private and public sectors share the expectation that alerts and information about cyberthreats should be timely so as to enable prompt corrective action. However, collaboration between the public and private sectors is typically beset by a lack of clarity on the precise nature of this data and the required depth of detail (Germano, 2014). The WEF addresses this problem by listing five types of information that the public and private sectors should exchange: data related to the attack, such as indicators of compromise; criminals' modus operandi; causal or attributing factors; data on stakeholders' practices, including best practices and lessons learned; and prevention, detection and protection measures. Moreover, the WEF (2017) highlights certain issues bearing on the ensuring of effective information sharing. For instance, stakeholders should not only share information that they are legally obligated to divulge, but also data subject to no such obligation, provided its disclosure is not prohibited. Stakeholders, particularly companies, hold a wealth of information, potentially invaluable to cybercrime investigations which, in the absence of the legal obligation to do so, they choose not to share, largely out of concern that it could be disclosed to competitors. Conversely, the parties must ensure that information they wish to share does not constitute information which may not be legally disclosed; in effect, without respect for such protections it would be impossible to protect personal information and guarantee the right to privacy. Public and private stakeholders are therefore advised to verify the legislative framework in force to avoid disclosing protected information. In addition, the Forum recommends sharing only processed data, and not raw data, as this facilitates its analysis and, moreover, reduces the risk of divulging personal or sensitive information. Finally, the Forum (2017) notes that information sharing should be reciprocal, otherwise many stakeholders would likely see little interest in the exercise.

The second issue in relation to public-private information sharing concerns the **methods of sharing**. For public-private information sharing to take place, the stakeholders must get to know one another. Good relations between the sectors should be cultivated, and each must be confident that the other is trustworthy and the information being shared will only be used for the purposes established under the partnership; in other words, as mentioned above, trust is a fundamental issue (World Economic Forum, 2017). It is also advisable to enlist the appropriate people, senior managers in particular, as well as mobilize sufficient necessary resources (United States General Accounting Office, 2001). The use of secure data transmission methods, including encryption, is essential for the secure exchange of

potentially sensitive information (United States General Accounting Office, 2001). Finally, for certain information, particularly incident reports, real-time, 24/7 data sharing is preferable to facilitate prompt and effective action (World Economic Forum, 2017).

c) Lack of diversity among private sector participants

One issue mentioned previously is private stakeholders' lack of interest in participating in a PPP. There is, however,another issue surrounding private sector involvement, specifically relating to small and medium-sized enterprises (ENISA, 2017). In addition to their lack of interest, these businesses do not feel they have any stake either in the issue of cybersecurity or that of PPPs (Germano, 2014). Indeed, it has been observed that some small businesses, owing to their size, do not feel threatened and do not envision themselves as potential victims of cyberattacks. Therefore, they are less inclined to participate in cybercrime-prevention initiatives, particularly as participation in a PPP means committing time and human resources, which, very often, represent costs beyond the means of small businesses (ENISA, 2017; Germano, 2014).

Nevertheless, as Germano (2014) indicates, a dialogue has begun around the issues and dangers of cybercrime, which could help to sensitize small businesses and mobilize them to join these partnerships. Likewise, changes in regulatory frameworks and civil liability are increasingly illuminating the risks run by businesses that do not take the appropriate steps to prevent or respond to cyberattacks. When sensitized in this way, these businesses come to appreciate the necessity of proactive cybersecurity measures (Germano, 2017).

Recommendations

This section proposes recommendations regarding the development and implementation of public-private partnerships in cybersecurity.

Develop a common terminology and classifications

As seen throughout this report, stakeholders participating in cybersecurity initiatives are confronted by a lack of common terminology and harmonized system of classification. These shortcomings give rise to particular issues, as partners may fail to share a common understanding of threats. In addition to information sharing, it is also important to use a common terminology about cybercrime.

Build a relationship of trust between partners

The bond of trust between partners is, obviously, not present from the outset, but must be cultivated over time. Partnership members must demonstrate transparency and communicate directly and openly, both with the other partners and within their own organizations. This level of trust creates a mutual sense of confidence that members will benefit from their involvement. As in any partnership, and in particular one involving information sharing, it is essential to create a framework that specifically defines (1) the roles of the public and private partners; (2) the relationships between these partners; and (3) the areas in which they are to cooperate (ENISA, 2011a).

Create a framework for partner accountability

As previously mentioned in this chapter, PPPs (whether in cybersecurity or other fields) imply a major inherent issue: unlike government-only actions, the responsibilities that go along with these initiatives do not fall on a single partner, but rather on a range of actors from both the private and public sectors. This shared responsibility complicates the question of accountability in the event of errors which, in cyberspace, may be prejudicial to a critical mass of individuals.

To avoid this situation, mechanisms must be created to ensure that the private and public sectors may mutually hold each other to account. Mechanisms must be implemented that provide a means for each partner to demonstrate its commitment to the partnership (Forrer, Kee, Newcomer, & Boyer, 2010).

Forrer et al. (2010) put forward six key dimensions that may be useful in developing a framework for evaluating accountability under a PPP:

- **The risks** associated with the partnership's actions should be clearly identified and understood by all the partners. On that basis, an agreement must then be reached concerning which partner is capable of assuming the responsibilities associated with said risks.
- A **cost-benefit analysis** should be performed to identify the projects most appropriate for the partnership.
- An analysis of the partnership's **social and political impacts** should also be performed.
- It is important to ensure that the **expertise** of each partner, the private sector stakeholders in particular, has been identified, is optimally leveraged, and subject to proper monitoring.
- Regarding **activities where partners work in collaboration,** a number of elements should be considered. Each partner organization must be able to count on representatives who demonstrate leadership and, when mistakes are made, are able to hold those responsible to account for their actions. Ongoing and clear communication between the partners is also essential, as is effective project management. Finally, as previously mentioned, a strategy should be put in place to build and maintain trust between partners.
- **Performance measures** should also be used to monitor the implementation of the partnership and determine whether the expected outcomes are realized.

Beyond a situational approach to cybercrime prevention

As our entire discussion makes apparent, the prevention approach favoured by PPPs is almost exclusively situational. Cyberattack prevention is ensured by enhancing the security of information systems and sharing expertise to facilitate threat detection. The intended objective is to reduce the opportunities for committing cyberattacks. However, as Kavanagh points out, regarding terrorists' use of the internet and ITC to advance their designs, preventive online cybersecurity measures does nothing to deter the offline activities underlying these criminal acts (2016). As a consequence, it will fail to prevent such problems upstream. On the contrary, such measures focus on interdicting actions when, in fact, the conditions leading to the crime already exist. This "reactive" approach to prevention is by its very nature defensive. It is vital to develop other types of preventive actions, for example, initiatives relying on social or proactive prevention, which can play a fundamental role in combating cybercriminal actions.

Conclusion

This chapter sought to present today's main trends in relation to cybersecurity public-private partnerships. As this overview has shown, managing horizontal relationships, such as those in PPPs, is not without its share of challenges. Regarding partnerships specifically developed for cybersecurity and cybercrime prevention, these challenges are further complicated by the difficulties intrinsic to managing an entity as vast – and constantly – evolving as cyberspace. An additional issue to be underscored is the problem of obtaining data from the public sector. More specifically, most of the available data is from the private sector or from sources that it helps to fund. This gives rise to two problems: the issues a PPP chooses to address will be of greater import to private interests, to the potential detriment of issues or concerns that might be in the public interest. The second problem is that only the private sector's voice is heard, which tends to foreclose debate regarding its role as a critical and essential actor in cybersecurity. Moreover, the issues raised will mainly concern improvements in processes and modalities of participation beneficial to the private sector. As we've seen throughout this report, it's important to consider the possibility that other governance models, which include other stakeholders, may be adapted to address cybercrime prevention and other types of prevention.

Contribution

PPPs as a strategic objective in NCSS

By ENISA

Introduction

As society becomes more and more dependent on IT, the protection and availability of critical assets are increasingly becoming a topic of national interest. Incidents causing disruption of critical infrastructures and IT services could cause major negative effects in the functioning of society and economy. As such, cyber security is increasingly regarded as a horizontal and strategic national issue affecting all levels of society.

On the 6th of July 2016 the Directive on security of network and information systems (the NIS Directive) was adopted and entered into force in August 2016. The NIS Directive requires EU Member States to develop and adopt a national cyber security strategy (NCSS). If needed, Member States can call upon ENISA to assist them in drafting a NCSS. Within three months after the adoption of their NCSS, EU Member States need to forward the strategy to the European Commission.

National cyber security strategies are the main documents of nation states to set strategic principles, guidelines, and objectives in order to mitigate risk associated with cyber security. Cyber security is shared responsibility thus relies heavily on collaboration.

ENISA - the EU Cyber Security Agency - works in the area of National Cyber Security Strategies (NCSS) since 2012. The goal of ENISA is to support EU Member States in their efforts to develop, implement and evaluate their NCSS by providing online tools1 and guidelines2.

European legislation like the Cybersecurity Strategy3 of the European Union: 'An Open, Safe and Secure Cyberspace and Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', encourages the need for private-public cooperation in the field of cybersecurity as well as the importance of trust building through public-private partnerships.

Establishing Private Public Partnerships

A common strategic objective of every European national cyber security strategy is collaboration to enhance cyber security across all levels. From threat information sharing to awareness raising, collaboration is often achieved through Public Private Partnerships (PPPs).

In the majority of countries, private companies own critical infrastructure and critical services are provided by the private sector. Therefore, a high degree of communication and cooperation can be an effective way for governments to understand the needs and challenges of private companies, but also to ensure that the necessary measures are implemented to achieve a sufficient degree of security.

Public-private partnership can be an effective tool in two ways:
- by pooling expertise and resources of the private and public sector;
- by establishing a common scope, objectives, and work methodology to achieve shared goals.

An example is the private sector cooperation in Bulgaria:

> Public-Private Partnership - Improving Cyber-security requires a combined, multi-sector, comprehensive approach that focuses on building a "whole-of-government" cyber organisation that includes cooperation with private enterprises and places an emphasis on educating the citizen. Opportunities to enhance the involvement of the private sector and to ensure that we capitalize on their expertise should include jointly exploring best practices and procedures to ensure that no part of the critical infrastructure, whether in public or private hands, would become a weak link and vulnerability.

In 2011, ENISA published a **Good Practice Guide on Cooperative models effective PPPs**. The study reveals the main five components associated with creating and maintaining PPPs by answering the following questions:

- **Why,** referring to **scope and threat**. The idea here is to identify the real problem and try to solve it by covering all possible aspects. It is important for potential members to clearly understand the relevance of the PPP to their own organisation. This will help support them in justifying their involvement to their own management. This is also true where membership is mandated, as it will determine the level of involvement.
- **Who,** referring to **coverage and link.** Having people that are passionate about what they are doing is key in this step. A PPP can involve partners at a national, pan- European or International level and its focus may be thematic, sectorial or cross-sectorial.
- **How, r**eferring to **governance.** How to organise and run a PPP requires careful consideration. How a PPP is organised, how partners work together, and its rules and financing can have a key impact on the success of a partnership. The governance of a PPP was defined as critical by all the PPPs surveyed.
- **What, r**eferring to **services and incentives.** Having something concrete to offer, listening to the members and delivering what they ask for is crucial for a successful PPP.
- **When,** referring to **start up and sustainability.** It is very

important to understand how the PPPs grow and evolve. Public sector organisations should consider the successful strategy used by many PPPs, by starting with a top down approach and over time growing the PPP from the bottom up.

Finally, the study collects data from both public and private sector stakeholders and provides guidance on how to create a partnership and help stakeholders to easily choose those aspects that will add value to their endeavours in setting up and running PPPs.

In 2017, ENISA conducted a study on **Cooperative Models for Public Private Partnership (PPP)** collating information on best practices and common approaches. This research analyses

- the **status of PPPs in the EU**,
- identifies the main **models of collaboration**,
- the **current challenges** that both private and public sector face while setting up and developing PPPs, and
- provides **recommendations for the development of PPPs** in Europe.

Today more than 15 MS have established an official PPP, an increase compared to 2012. In many cases, partnerships are created to conduct a specific project i.e. a national cyber security exercise or a cybersecurity awareness campaign (European Cybersecurity Month). It is very important to notice that since the first Good Practice Guide, sectorial PPPs have been created in the EU following the approach of the US. This again is an indication of maturity and sophistication on the approach towards cybersecurity.

While analysing PPPs in Europe, it is evident that culture is one of the most important determinants of the way private-public partnership are being established, developed and worked. There is no universal scenario of how to create a successful PPP; what works perfectly in one country can be tricky and challenging in another. That is mainly because of the cultural differences and the fact that the general relation between public and private sector differs amongst member states. In some countries, formality is the most important part of PPP, while in the others pragmatism is more important.

Based on the ENISA study – Cooperative Models for Public – Private Partnerships, the types of PPPs developed in Europe are the following:

- **Institutional PPP**. In this type, the whole institution works under a PPP framework. Usually, there are many services that this type of institution delivers, such as research, analysis, development of good practices and guidelines, help desk, security audits and some more focused services. This type of PPP is linked with the critical infrastructure protection. This is because the institution is in charge of critical infrastructure protection by a legal act (e.g. emergency/ crisis management act). A proper solution is the cooperation in the PPP framework with the critical sectors. Common means of cooperation are working groups, rapid-response groups and long-term communities. The goal is to secure critical infrastructure in general, and cyber threats are considered important elements in the threat landscape.
- **Goal-oriented PPP.** PPPs of this type are created for the purpose of building a cybersecurity culture in the MS. There is usually a platform or a council established which brings private and public sector together to exchange knowledge and good practices. The objective for the members is to focus around one subject or a specific goal.
- **Service outsourcing PPP.** PPPs of this type are initiatives created by the government and the private sector. Their main task is to raise the cybersecurity awareness and cybersecurity level amongst stakeholders. These PPPs can actually be considered as a third party for outsourcing services which address the need of industry and support the government in policy making process (e.g. NIS implementation, drafting of national cybersecurity strategies).
- **Hybrid PPP.** This type of PPP includes the CSIRTs operating under a PPP framework. In this case, governments decide to assign to an experienced entity – with already proven experience in operating CSIRT to deliver CSIRT services to the public administration or to the whole country.

Finally, a few recommendations based on main challenges are analysed in the 2017 ENISA study to help PPPs in the EU be more efficient and evolve.

Trust building in PPPs

Building and maintaining trust between public-private, private-private and public-public entities has been recognised as the one of the biggest challenges of PPPs; Most PPPs define trust as an ongoing process that involves personal relations and consumes a lot of time.

There are several mechanisms that support trust building and are used by PPPs, such as regular meetings, face-to-face meetings, social events, thematic conferences, joint exercises,

Face-to-face meetings, regular meetings and social events are considered as the most effective tools of trust building as they contribute to build long term partnerships. Personal qualitative interaction between the members of the PPP is considered as a key point for successful PPP.

In the process of building trust, the need for a "manager" would be considered catalytic as he/she would be someone who believes in the cause of, who is devoted to the presence and maintenance of it and by this attitude inspires others to get involved and to collaborate.

PPPs with a high level of trust are obviously more efficient – they recognise the needs of both public and private sector and they are able to address them through cooperation.

Motivation for the private sector to participate is a priority when establishing a PPP

What is clearly visible in every analysed model of PPP is the fact that to create successful and efficient PPP, resources are needed. These kind of collaborations need a driving force to stimulate them, so that it could be really vital. It is not enough to provide incentives and money. PPPs will not grow if there is lack of people who will work on them. A PPP really needs someone who interacts with every member of the partnership; drives the agenda, sets up the meeting and keeps strategic perspective. PPPs need a whole group of people who prepare the action plans and work closely with both public administration and the industry. The most sophisticated PPPs are usually NGOs or institutions created only to build and strengthen cooperation and collaboration between public and private sector.

Promotion of the concept of PPPs amongst Small and Medium Enterprises (SMEs)

It is common that big companies are mostly involved in the PPPs. SMEs do not have the resources to get involved and most of the time they do not realise that participating in a PPP could be beneficial for them. It would be useful also from a societal perspective to involve other types of stakeholders like SMEs and start-ups in the PPP to gain experience from larger players in the field.

Public institutions to lead the PPP or the national action plan for PPP

Since cybersecurity is highly interdisciplinary, there are usually many public bodies involved in PPP – Ministry of Internal Affairs, Ministry of Defence, Ministry of Economy or Development to name only a few. It is very important for public administration to communicate clearly and honestly their needs and limitations to the private sector.

The point of contact is perhaps just the most visible aspect, the tip of the iceberg. But what is much more important is the fact that government entities involved in a PPP should know in advance - ie, before inviting private sector partners to join - what they want to achieve, what their contribution is going to entail, and what the private sector should contribute. Or to put it shortly: get the strategy right before you join the PPP.

It is very frustrating for the private sector representatives to witness disagreement between key public institutions. Private sector expects government to act. If the public sector could agree for the one contact point for PPP, that could be enormously beneficial for the overall PPP.

PPP is about private-private, public-public and private-public cooperation. Focusing only on the relationships between public and private sector could be very short-sighted for the PPP policy. The right level of dialog and understanding between public agencies is often the key to successful PPP.

The same applies to the private sector. The successful PPP integrates not only private administration and the industry, but also different entities among the industry (e.g. energy companies, banks, telecoms).

For this reason, the PPPs all over the EU should focus also on private-private and public-public cooperation and collaboration.

Conclusion

It is evident that partnerships require a clear framework specifying the roles of the public and private sectors, their relationships and the areas for co-operation. If organisations are to face coherent, straightforward and effective regulatory and/or non-regulatory requirements, public-private co-ordination needs to be optimised.

ENISA is supporting EU MS on how to develop PPPs by providing recommendations, good practices, guidelines and by bringing stakeholder together to collaborate, exchange views and information. **Cybersecurity is a shared responsibility** and ENISA, together with the community, is stepping forward and working towards making collaboration and information and knowledge sharing stronger and more reliable. The multi-faceted efforts of ENISA across the cybersecurity spectrum are supporting and empowering a more cyber secure and safe Europe.

Notes

56 http://www.europeanfinancialcoalition.eu/

57 https://www.first.org/

58 Founded in June 2016, ECSO is a non-profit association whose mission is to support initiatives to develop and promote cybersecurity in Europe. It assembles over fifty public and private organizations and represents the industry-led contractual counerpart to the European Commission for the implementation of this public-private partnership (https://ecs-org.eu/about).

59 The question of public-private partnerships in national cybersecurity strategies will be explored in greater depth by ENISA in its contribution to this chapter.

60 https://securitymadein.lu/tools/

61 https://www.signal-spam.fr/

References

Chapter 5. Public-private partnerships in cybercrime prevention

ANSSI. (2016). Adoption de la directive network and information security (NIS) : l'ANSSI, pilote de la transposition en France. Retrieved from 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. Retrieved from 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 Cybersecurity 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). Retrieved from 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.

Retrieved from http://www.fbi.gov

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. Heraklion, Greece: European Union Agency for Network and Information Security.

ECSO. (2018). About the cPPP. Retrieved from https://ecs-org.eu/cppp

ECSO. (2018). About ECSO. Retrieved from https://ecs-org.eu/about

ENISA. (2011a). Cooperative Models for Effective Public Private Partnerships: Desktop Research Report. Heraklion, Greece: European Union Agency for Network and Information Security.

ENISA. (2011b). Cooperative Models for Effective Public Private Partnerships: Good Practice Guide. Heraklion, Greece: European Union Agency for Network and Information Security.

ENISA. (2017a). Cooperative Models for Information Sharing and Analysis Centers (ISACs). Heraklion, Greece: European Union Agency for Network and Information Security. Retrieved from https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

ENISA. (2017b). Cooperative Models for Public Private Partnership (PPP). Heraklion, Greece: European Union Agency for Network and Information Security. Retrieved from 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. Retrieved from 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

Gal,S (2002). A semiotics of the public/private distinction. Difference: A Journal of Feminist CulturalStudies, 13(1), 77-95.

Gardiner, L. (2009). The foundation for corporate citizenship and sustainable businesses. Retrieved from 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.

ICPC, World Bank Sustainable Development Department for Latin America and the Caribbean, Chambre de commerce de Bo-

gotá, & Instituto Sou da Paz. (2011). Public-Private Partnerships and Community Safety: Guide to Action.

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, California.

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.

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. Retrieved from http://www.nationalisacs.org/about-isacs

National Cybersecurity Centre. (2018). Cybersecurity Information Sharing Partnership (CiSP). Retrieved from https://www.ncsc.gov.uk/cisp

National Security Authority. (2015). National cybersecurity strategy of the Czech Repubic for the period from 2015 to 2020. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.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

Public Safety Canada. (2017, July 4). Critical Infrastructure. Retrieved from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

SECURITYMADEIN.LU. (2018). Tools and services from the Luxembourg cybersecurity ecosystem. Retrieved from https://securitymadein.lu/tools/

The Canadian Council for Public-Private Partnerships. (2016). Definitions and models of public-private partnerships. Retrieved from 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

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. Retrieved from 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.

UNODC. (2011). Handbook on the Crime Prevention Guidelines. Making them Work. Retrieved from : https://www.unodc.org/pdf/criminal_justice/Handbook_on_Crime_Prevention_Guidelines_-_Making_them_work.pdf

US-CERT. (2018). National Cybersecurity and Communications Integration Center. Retrieved from https://www.us-cert.gov/nccic

Weihe, G. (2005). Public-Private Partnerships: Addressing a Nebulous Concept. Presented to the 10th International Research Symposium on Public Management, Glasgow Caledonian University, Scotland.

Wong, J.C. (2018). Congress grills Facebook CEO over data misuse – as it happened. The Guardian. Retrieved from https://www.theguardian.com/technology/live/2018/apr/10/mark-zuckerberg-testimony-live-congress-facebook-cambridge-analytica

World Economic Forum. (2017). Guidance on Public-Private Information Sharing against Cybercrime (No. 040117-00026464). Geneva, Switzerland: World Economic Forum

INTERNATIONAL CENTRE FOR THE PREVENTION OF CRIME

465 rue Saint-Jean, bureau 803
Montréal (Québec) H2Y 2R6
Canada

+1 514 288-6731

cipc@cipc-icpc.org
www.cipc-icpc.org