Centre
international
pour la
prévention
de la criminalité

International
Centre
for the
Prevention
of Crime

Centro
Internacional
para la
Prevención
de la Criminalidad

EXECUTIVE SUMMARY

6th International Report

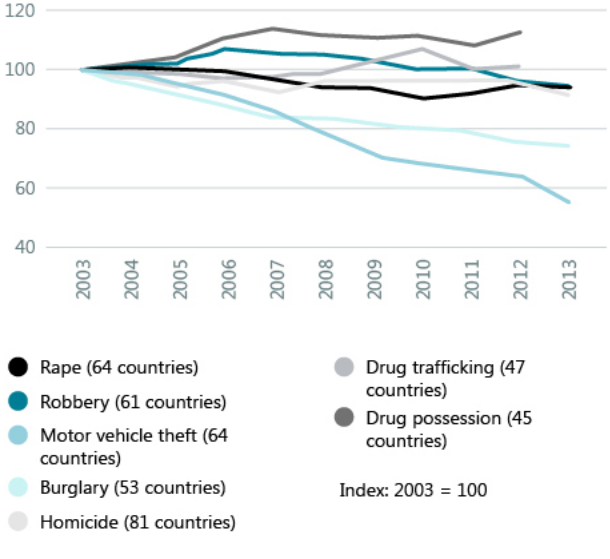
CRIME PREVENTION AND COMMUNITY SAFETY: Preventing Cybercrime

EXECUTIVE SUMMARY

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 cyberspace's growing importance? 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 a difficult hypothesis to prove, it's 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 a pressing need. That said, is it in fact possible to prevent cybercrime? Do the proper 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. In effect, discussion 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 best 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 undeveloped.

These considerations led us to produce an International Report focusing exclusively on the question 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 Chapter 2, the Report's core chapter. In effect, 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 cybervictims. 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.

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 concentrates on the recent crime prevention efforts of international and regional organizations, particularly UN affiliated organizations. Finally, Part III offers a survey of the latest empirical studies. To that end, a review was done of 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 regarding 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 rate 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, indeed, 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 countries 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, etc. Unfortunately, most cooperation initiatives put more emphasis on criminal justice than on prevention.

- A finding of our review of the literature was the importance accorded 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 crime prevention, particularly in police departments in South America. Finally, recent studies have shown that actions based on punitive prevention and rehabilitation policies, 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 focusing in particular on governance issues and inequality factors. 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.) do 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 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 complexified 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, moreover, is subject to rapid and constant evolution. Nevertheless, several key aspects are readily apparent and of particular interest from the perspective 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 very small body 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, which, moreover, is of highly varying quality. Nevertheless, certain preliminary conclusions may be drawn from this data regarding, notably, 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 agenda. Moreover, as they 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 new debates, theoretical as well as practical, 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 to 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 in 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 of the issues encountered in such partnerships. This chapter concludes with a few recommendations.

A number of findings emerged from this chapter:

- As we've 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 which 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.

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

The 6th International report on the Prevention of Crime is available on the ICPC Website
www.cipc-icpc.org