INFORMATION SYSTEMS, WEB AND PERVASIVE COMPUTING SERIES

CYBERSECURITY SET

Volume 3

Cybercrime during the SARS-CoV-2 Pandemic (2019-2022)

Evolutions, Adaptations, Consequences

Edited by
Daniel Ventre and Hugo Loiseau

ISTE
WILEY

Cybercrime During the SARS-CoV-2 Pandemic (2019-2022)

Cybersecurity Set

coordinated by
Daniel Ventre

Volume 3

Cybercrime During the SARS-CoV-2 Pandemic (2019-2022)

Evolutions, Adaptations, Consequences

Edited by

Daniel Ventre
Hugo Loiseau

ISTE

WILEY

First published 2023 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

Library of Congress Control Number: 2022950071

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-78630-801-6

Contents

Introduction ix
Daniel VENTRE and Hugo LOISEAU

Chapter 1. The Evolution of Cybercrime During the Covid-19 Crisis 1
Daniel VENTRE

1.1. Introduction. 1
1.2. Observing the evolution of cybercrime 4
1.2.1. Leveraging annual data: the case of India 8
1.2.2. Leveraging monthly data 11
1.2.3. Leveraging weekly data: the case of China. 21
1.3. Has the global geography of cyberattacks changed?. 29
1.4. Conclusion 34
1.5. Appendix 39
1.5.1. Cybercrime tools: malware 39
1.5.2. CVSS as indicators of vulnerability levels 40
1.5.3. Heterogeneity and complexity of cybercrime typologies. 41
1.5.4. Attitude of companies toward cyber risks: the case of the United Kingdom 46
1.6. References 47

Chapter 2. The SARS-CoV-2 Pandemic Crisis and the Evolution of Cybercrime in the United States and Canada 49
Hugo LOISEAU

2.1. Introduction. 49
2.2. The impacts of the SARS-CoV-2 pandemic. 50

2.3. Cybercrime and SARS-CoV-2 52
2.3.1. Targets and victims 53
2.3.2. Malicious actors 57
2.3.3. Cyberspace: a propitious environment for cybercrime 58
2.4. The evolution of cybercrime in North America during the pandemic . . 61
2.4.1. The United States 62
2.4.2. Canada 67
2.5. Discussion 69
2.6. Conclusion 72
2.7. Acknowledgments 74
2.8. References 74

Chapter 3. Online Radicalization as Cybercrime: American Militancy During Covid-19 81
Joseph FITSANAKIS and Alexa MCMICHAEL

3.1. Introduction 81
3.2. A new typology of cybercrime 83
3.3. Internet connectivity and violent militancy 85
3.4. The pre-pandemic domestic threat landscape 87
3.5. The domestic threat landscape of the pandemic 88
3.6. Pandemic accelerationism 91
3.7. From virtual to real-life criminality 93
3.8. Online radicalization during Covid-19 94
3.9. A new methodological paradigm for online radicalization? 98
3.10. Conclusion: meta-radicalization as cybercrime 100
3.11. References 102

Chapter 4. Cybercrime in Brazil After the Covid-19 Global Crisis: An Assessment of the Policies Concerning International Cooperation for Investigations and Prosecutions 109
Alexandre VERONESE and Bruno CALABRICH

4.1. Introduction: Brazilian cybercrime and the Covid crisis impact 109
4.2. Cybercrime in the literature and the Brazilian case 112
4.3. A theoretical model for international cooperation 115
4.4. The evolution of cybercrime in Brazil 119
4.5. The evolution of the Brazilian legal system concerning cybercrime and its connection to the international regime 126
4.6. Managing international cooperation without having the best tools . . . 133
4.7. Difficulties with cooperation: joints, mortises, and notches 137

4.8. Conclusion: what to expect from the future? 140
4.9. References 142
4.10. Appendix: List of interviews and questions 147

Chapter 5. Has Covid-19 Changed Fear and Victimization of Online Identity Theft in Portugal? 149
Inês GUEDES, Joana MARTINS, Samuel MOREIRA and Carla CARDOSO

5.1. Introduction. 149
5.2. The impact of the Covid-19 pandemic on cybercrime. 150
5.3. Evolution of cybercrime in Portugal 153
5.4. Online identity theft (OIT). 155
5.4.1. Definition and modus operandi. 155
5.4.2. RAT applied to cyberspace 156
5.4.3. Individual variables and OIT victimization. 159
5.5. Fear of (online) crime. 160
5.5.1. Determinants of fear of (online) crime 160
5.6. The present study 162
5.6.1. Measures 163
5.6.2. Results 165
5.6.3. Variables associated with online victimization and fear of identity theft. 169
5.7. Conclusion 170
5.8. References 171

Chapter 6. A South African Perspective on Cybercrime During the Pandemic. 177
Brett VAN NIEKERK, Trishana RAMLUCKAN and Anna COLLARD

6.1. Introduction. 177
6.1.1. Background to South Africa and the pandemic 178
6.1.2. Methodology 179
6.2. International rankings. 180
6.3. Cybercrime and related legislation 183
6.4. Cybersecurity incidents. 186
6.4.1. Ransomware. 186
6.4.2. Scams and fraud. 188
6.4.3. System intrusions and data breaches. 190
6.4.4. Disinformation and malicious communications 192
6.4.5. Other 196
6.5. Discussion 197

6.6. Conclusion 199
6.7. References 199

List of Authors 211

Index 213

Introduction

Cyberspace is composed of several different layers that are essential to the functioning of an interconnected and functional network. The physical, software and informational layers, although forming the functional body, are of little interest to the political field. It is, on the contrary, the social stratum that concerns and interests politicians and political scientists in particular. This layer includes the set of individual behaviors interacting with cyberspace and a collective component that affects the policies, institutions, laws, norms, regulating and framing the interactions and use of cyberspace. Despite the fact that cybercriminals may be interested in flaws in software or physical systems to commit their crimes, the social character is also fraught with vulnerabilities that can be identified and exploited by cybercriminals. Considering that each user is responsible for his or her actions in the cyberspace and that cybersecurity practices are not always appropriate or sufficient, the user is simultaneously a potential victim and a system gateway. In that sense, systems are vulnerable from the very moment a user behaves unsafely.

By virtue of its supranational character, the cyberspace is particularly difficult to govern and secure. Based on the amount of information that passes through the networks at all times, supervising and controlling information and transactions, verifying content legitimacy and legality and processing complaints or incident reports within a reasonable amount of

Introduction written by Daniel VENTRE and Hugo LOISEAU.

time, constitute major challenges for supervisory, governmental, industrial, public or private bodies. The detection and recovery phases can be affected by those capacity limits, making systems non-operational, or exposing them to multiple risks.

Network security and protection are considered a shared responsibility between security and law enforcement agencies, government bodies, businesses, organizations and individuals. Several social changes have therefore taken place in recent years with the increasing dependence on and use of cyberspace. Policies and surveillance do not always keep pace with the advances in this space. This is especially true in the event of a crisis such as the one experienced by all the States during the SARS-CoV-2 (or Covid-19) pandemic in 2020.

During this health crisis, cyber risks and cyberthreats seem to have increased. Cyber risk is the product of the level of threat with the level of vulnerability. While cyber risk determines the likelihood of a successful cyber attack [SAN 22], cyberthreat represents a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm [SAN 22]. These two notions are fundamental, because the cyberization that societies have experienced over the past 20 years has contributed greatly to the complexity of cybersecurity issues. In 2001, U. Beck already heralded that the social production of wealth is accompanied by the social production of risks [BEC 92]. The SARS-CoV-2 pandemic in 2020 and its following multidimensional crisis (social, economic, political, etc.) represent a contextual window, which perfectly illustrates the risk society that Beck referred to, featuring the multiplication and diffusion of systemic and cross-sectoral risks resulting from technological and industrial developments. Globalization and the expansion of the cyberspace increase such risks [BEC 92]. During this period, cybercrime evolved in a context of globalization and cyberization.

Cybercrime research primarily focuses on two broad categories of crime:

– Organized cybercrime, large-scale cyber attacks, which could be part of the more general framework in the study of major crime. Jean-François Gayraud proposes four main characteristics for appraising “major crimes”:

- i) major crime is chiefly manifest by polycriminality; major criminal groups are opportunistic and pragmatic in criminal markets, meaning that they do not necessarily develop a specialization of their criminal practices;

- ii) these groups are territorialized, rooted in a space that allows them to create their own biotope, setting up hermetic enclaves inaccessible to the public authorities; this favors the territorialized and immaterial expansion into the cyberspace;

- iii) these groups and organizations are considered unsinkable; this is because they are highly adaptable to socioeconomic changes and resistant to repression by the public authorities or to the competition from other criminal groups;

- iv) finally, these groups a have major macroeconomic impact since they manage massive, globalized and interconnected financial flows, which facilitate and stimulate corruption, as well as the laundering of illicit income [GAY 21].

– The scope of cybercrime and its study is not limited to organized crime, but includes everyday life, ordinary criminal acts, such as online defamation, violent extremism and hate speech on the Internet and social media [BEN 22], radicalization [ALA 21], disinformation [PAR 20], etc., which are all common forms of cybercrime.

Major criminal groups and ordinary cybercrime play a crucial role in what might be termed a "criminological diffuse background", whose omnipresence and pervasion in the cyberspace act as the basis for many illicit practices of interest to cybersecurity [BRE 10]. As a result, cybercrime benefits from an immense market bringing together the supply (of software, services and available techniques in the cyberspace) and the demand from criminal or non-criminal organizations, states and individuals whose goal is to exchange a good (data) by means of an increasingly dematerialized and fungible currency: the cryptocurrency [BAD 20]. While the aggregation of these characteristics has facilitated cybercrime, what can be said about the crisis context in 2020?

I.1. The context

I.1.1. *The pandemic, its management, its effects*

The SARS-CoV-2 epidemic emerged at the end of 2019, its first cases being recorded in China, and then in Thailand. China quickly implemented measures trying to contain the epidemic: massive population lockdown in

Wuhan, as well as the construction of field hospitals whose progress the whole world could follow live via webcams connected to the site on a permanent basis. Soon enough many cases and victims were identified in various parts of the world. The WHO officially announced the outbreak of this new disease on January 30, 2020 and declared it a global pandemic on March 11, 2020. As a result, several states in the world decided to implement emergency health safety policies. These policies were not implemented everywhere at the same time, or in the same way, given the fact that the epidemic did not evolve at the same pace around the world. In addition, governments often had conflicting approaches as to what should be done (to close the borders or not, to confine the whole population or only certain age brackets or professional categories, etc.). Measures took several forms:

1) Those aimed at fighting the epidemic itself:

– measures prohibiting or restricting movement within the states and/or internationally, the lockdown of national or local populations (districts, cities, regions), isolation of individuals and social distancing;

– measures restricting social, economic and professional activities: store closures, the reduction of international trading volumes and the closure of schools and businesses.

These measures were applied to varying degrees across the different countries – not in all states – at different times, and sometimes disparately even within the same country, following specific schedules for each region (as was the case in France, and is still the case in China in 2022, where the population of Shanghai, for example, has been forced into strict lockdown, while other regions have not been confined).

2) Some states also decided to implement measures to mitigate the negative effects produced by health constraints on society, in particular, the impact on the economy. It is worth recalling:

– economic security measures: state funding in order to help the economic activity of companies, business loans, emergency social benefits, etc.;

– measures to ensure the continuity of activities: not only remote working, distance learning, but also hybrid work formulas alternating teleworking and regular attendance to the office.

Due to its lethality and morbidity, and to the disruption of societies' working mechanisms, the Covid-19 pandemic is considered "a public health crisis without precedent in living memory […] which brings with it the third and greatest economic, financial and social shock of the 21st century, after 9/11 and the Global Financial Crisis of 2008" [OEC 20]. According to the OECD report, the "shock" occurred at several levels:

– a halt or slowing down in production in countries affected by the pandemic and the lockdown phases;

– a disruption of supply chains across the world;

– a steep drop in consumption;

– a collapse in "confidence" (which is reflected in the fluctuations of financial markets confronted with a scenario of extraordinary uncertainty);

– the significant loss of human life;

– proof of the stark weaknesses of healthcare systems around the world, including in the richest countries.

Other elements could be added to this list, such as the emergence of conspiratorial and anti-vaccine movements.

This reveals the presence of *at least* two types of crisis whose effects are combined: a health crisis together with an economic and financial crisis.

I.1.2. *The concept of "crisis"*

The term "Covid-19" was quickly associated with that of "crisis".

Crises are particular moments of tension, during which certain phenomena or processes are exacerbated. The definitions of "crisis" highlight some of these characteristics: "the emphasis is on the idea of a sudden and intense manifestation of certain phenomena, signaling a rupture"; "a sudden and intense manifestation, whose duration (of a state or behavior) is limited, potentially leading to harmful consequences"; "a disturbing situation, due to a disruption of balance and whose outcome is decisive for the individual or society"; "a situation of deep unrest in which society or a social group is immersed, giving rise to fear or hope for a

profound change"[1]. Briefly stated, a crisis is a temporary situation, a turning point, a moment of instability and stress. However, the aforementioned approach assumes the pre-existence of a state of normality – albeit temporarily interrupted – which must be regained. The return to the previous state will be considered to be the crisis resolution. Although the crisis represents a moment of exception, it is a condition one may still cope with.

For Fearn-Banks [FEA 09], a crisis is "a major occurrence with a potentially negative outcome affecting the organization, company, or industry, as well as its publics, products, services or good name. It interrupts normal business transactions and can sometimes threaten the existence of the organization" [FEA 09, p. 2].

But normality can also be considered to be the crisis: from that perspective, the history of the world would be a series of successive, superimposed, nested crises [CAR 18], constituting the normalcy of the world, its structural signature [KOS 72].

Crises are moments of tension, of disorganization having reached a threshold that an individual, a group of individuals, or a society can no longer find acceptable or tolerable. The peak of intensity cannot last. But it should also be noted that crises are maintained over time, which may seem incompatible with its very definition (economic, security, climatic, political, social crisis, etc.). Still, the notion of duration is highly subjective. Furthermore, it is perhaps not so much the duration that characterizes the crisis, but the level of disorganization or even destruction it engenders, as well as the acceptability threshold of such an exceptional state by an individual or society. The crisis signals a moment of unbearable tension. What is called the end of crisis, the after crisis, the exit or crisis resolution is a return to a level of acceptability, even if the disturbance persists. But it is simply less intense or perceived as such. What is called the crisis exit may not always refer to the end of the event itself, but denote the ability to coexist with it, or to partially accept it. Therefore, *risk tolerance* is an essential component in the definition of a crisis. As such, it may differ from one society to another. Tolerance acts as a threshold defining the presence of a crisis or its absence.

Finally, with the resolution or exit from the crisis, one cannot consider that it is possible to return to the normality prior to it because the crisis has

1. Available at: https://www.cnrtl.fr/definition/crise.

necessarily left a mark on society. One may observe there is a pre-crisis period (A), a crisis period (B) and a post-crisis period (C), where C differs from A, because C = A + the effects of B.

The notion may be manifest as an economic, financial, debt, social, demographic, systemic, political (a state crisis, a crisis of power, a crisis in confidence, a crisis of democracy, etc.), humanitarian, migratory, health, climate, environmental, national, international or global crime crisis [ALT 07]. Cybercrises refer to crises resulting from one or more cyberattacks. These are rare events with a strong impact, situations when one or more malicious action(s) on an information system cause(s) a major disruption of the entity, having various and significant impacts, and sometimes causing irreversible damage [ANS 21].

Crisis indicators have been designed to try to keep track of the many crises occurring worldwide. The "crises" identified[2] have their origin in armed conflicts, insurrection movements, civil wars, proxy wars, intra-state conflicts, conflicts for the control of territories and resources, leading to humanitarian (due to the scarcity of resources and massive displacement of populations), health, economic crises. Other indicators[3] propose a quantitative measurement of the degree of severity of humanitarian crises, in view of adapting the responses to be provided. The INFORM Severity Index, produced by ACAPS[4], identified 136 global crisis situations in 2022[5].

Crises are moments of destabilization experienced by societies, having a varying impact on social groups. Crime can exploit such moments to establish its influence, its presence and develop its activities. For example, Mexican drug cartels took advantage of the Covid-19 crisis to expand their influence into realms or areas of activity where the state was weakened or absent (protection theory) [JAS 19, KLE 14]: "With a health care system inaccessible to large portions of the population, as well as welfare programs put under extreme strain, criminal organizations have been observed

2. Available at: https://theowp.org/our-work/crisis-index/.

3. Available at: https://drmkc.jrc.ec.europa.eu/inform-index/Portals/0/InfoRM/GCSI/GCSI%20Beta%20Brochure%20Single.pdf.

4. ACAPS is a non-governmental initiative, supported by three NGOs: the Norwegian Refugee Council (NRC), Save the Children and Mercy Corps. Available at: https://data.humdata.org/organization/acaps.

5. Available at: https://www.acaps.org/sites/acaps/files/crisis/gcsi-download/2022-06/20220606_inform_severity_-_may_2022.xlsx.

distributing resources to some local communities. Though anti-drug efforts continue at the state and federal level, officials within the government have largely side-lined security in favor of prioritizing pandemic response"[6]. Facing the mask crisis [WAN 20], mask shortages and the inability to ensure sufficient industrial production, criminal actors rushed into the breach, hoping to take advantage of the expectations of populations. Criminal cyber-operations on the theme of Covid, masks and drugs have been carried out all over the world [EUR 20a].

The link between crime and crises has been the subject of numerous studies, particularly borrowing from the economic theory of crime [DEF 11], but also focusing on other categories of crisis such as wars, political crises and disasters. For example, Kontula [KON 97] considers that crime occurring in exceptional circumstances is marked by predatory behavior, the erosion of moral values and the reduction of fear of punishment, as well as by the loss of control of the situation by security actors. UNODC [UNO 12] argues that economic factors are important in the evolution of crime. But the analyses diverge: when addressing the effects of the 2008 international financial crisis, Kurtz [KUR 15] concluded there was no close relationship between the two phenomena. In Russia, on the contrary, periods of economic turbulence coincided with an upsurge in criminal activity in 1998, and later in 2008–2010 (economic crimes and crimes against property seem to have been highly reactive to changes in economic conditions) [IVA 12]. "Peaks" in criminal activity may occur during periods of economic crises or "economic stress".

I.1.3. *The role of cyber in crises*

Digital was quickly considered as one of the responses to certain aspects of the Covid-19 crisis: teleworking was supposed to partly guarantee the continuity of activities in several sectors; e-commerce was expected to support market activities; and the various online applications proposed by governments and/or private sector initiatives were to maintain the efficiency of the health system, organize the logistics of large-scale vaccination phases, manage the lockdown and traveling restrictions (through the use of tracing applications) and ensure the respect for social distancing (by checking the possession of a health pass to access the places requiring it). Furthermore,

6. Available at: https://theowp.org/crisis_index/mexican-drug-war-2/.

digital technology had to be a tool for creating social ties at a time when individuals were forbidden from the slightest face-to-face relationship, it had to take citizens out of their isolation and help them cope with situations which had only existed in works of fiction until then (the all-pervading images of deserted cities and millions of individuals at their windows, cloistered by force, awaiting liberation).

But while digital technology has contributed, in its own way, to the global effort to fight the spread of the virus, it has also exacerbated the already high degree of dependence of societies on communication technologies, in particular the Internet and cyberspace.

Did cybercrime feed on that particular context, taking advantage of such dependence, those vulnerabilities and the increase in the use of digital technology? As the above-mentioned indicators have shown, the crises in the world are multiple at a time t, simultaneous, distributed within the entire international system. These are all contexts in which crime, and consequently cybercrime, can evolve. This point will be essential in the present analysis: Covid-19 cannot be considered as a single, isolated crisis. It would be more accurate to refer to Covid-19 “crises”, in the plural form, to refer to the crises resulting from the epidemic, its management and its effects on societies. These crises may be of a health, economic, social and perhaps political nature. But to these crises are added all those having existed before and during the Covid-19 epidemic, an event which took place in a world animated by tensions, conflicts and calamities and which is still immersed in discord. Crises coexist, become interlocked, can be triggered by the pandemic itself, or preceding it, for other motives, but may also become interdependent, producing effects on one another: the epidemic did not spare the populations already facing wars, other diseases, economic difficulties. In addition to the displacement of populations due to the climate crisis or to wars and economic or political crises, citizens had to cope with the effects of the pandemic itself. Cybercrime irrupted into societies hitherto affected by multiple crises to varying degrees. One cannot consider the evolution of cybercrime in the light of the crises strictly related to the Covid-19 pandemic, but should integrate them into a broader context made up of multiple crises, to which the pandemic was added.

I.2. Literature review: works on the theme "cybercrime and Covid"

I.2.1. *Main themes and hypotheses*

The effects of the epidemic on global society have inspired many reflections since the first months of 2020. These explore the impacts of the pandemic on:

– the economy: an increase in poverty together with a health crisis plunging millions of additional workers into it, as well as an increase in unemployment, with "around 205 million unemployed people in 2022, that is, a lot more than the 187 million in 2019" [ONU 21];

– culture [YU 21], education [ONY 20] and science [GUP 21];

– security and defense: the epidemic brought to light the weaknesses of the common European security and defense policy, highlighted the vulnerabilities of member states in terms of infrastructure, supply chain and communications security. The pandemic accentuated the retreat of the United States and the EU from the international scene, to the benefit of China, posing a challenge in several areas, including IT security and cyber capabilities. The pandemic has been described as an accelerator of pre-existing trends and an amplifier of instabilities [MEY 21]. The protection against the pandemic became a matter of national security: both the economic vitality of a nation and its way of life were endangered. Due to the spread of globalization, it influenced all states, whose destinies were more closely intertwined than they had been in the past centuries. The pandemic was destructive and disruptive. It disrupted or paralyzed the security and defense strategies of states, simultaneously exposed to several categories of threats or risks: crime, terrorism and foreign state threats. More generally, the Covid-19 pandemic was categorized as an event with a profound and lasting impact on the international security environment [ORO 22]. The Covid period favored and stimulated the development of new criminal activities [EUR 20b] (fraud, international trafficking, counterfeiting, etc.) feeding on global instability [KEN 21].

From the early months of 2020 – when the pandemic was still in its infancy – articles addressed the question of the evolution of cybercrime in such a context.

Some guiding themes and hypotheses have emerged from the abundant literature produced since then, both academic and non-academic (national and international organizations, cybersecurity companies, private and public sectors, etc.). The following should be retained:

– By reinforcing the essential role of the Internet, the management of the Covid-19 crisis (lockdown, teleworking, social distancing, tracking applications, e-commerce, etc.) created favorable conditions for cybercrime. Organized crime could take advantage of the enlargement of the attack surface by multiplying or diversifying criminal opportunities [TRI 20]. The conditions thus created acted both as a catalyst [BOU 21] and an accelerator of cybercrime.

– The multiplication of vulnerabilities and criminal opportunities acted as a key factor in the evolution of cybercrime since the pandemic onset: the lockdown transformed Internet uses, certain online practices such as e-commerce was auspicious for the theft of personal data; teleworking [TAB 20] isolated employees who could be the target of social engineering attacks [VEN 21]. The changes brought about by the pandemic in everyday life, particularly the uses of "cyber", played a central role in explaining the evolution of cybercrime.

– Attack vectors diversified, involving the creation of new attack scenarios [GRY 21]. The thriving of cybercrime during the pandemic was mainly the result of its ability to adapt, innovate and renew its operating methods [COR 20], its business model [LAA 21] and even the reconfiguration of some of its groups. ANSSI discusses the professionalization of organized cybercrime groups and the specialization process which has characterized the evolution of cybercrime in recent years [ANS 22]. Internet uses changed during the lockdown phases, shifting vulnerabilities or creating new ones: cybercrime also had to adapt to this reconfiguration of the attack surface in order to seize opportunities [LAZ 21]. For example, this was done via "themathized" operations (the registration of several tens of thousands of domain names using the term "Covid" and associated terms) [NAI 20], or by aiming its actions toward essential sectors in times of health crisis (health industry, vaccine research centers, hospitals, logistics, etc). The attacks on healthcare actors were at the core of the research carried out by Chigada and Madzinga [CHI 21]. While crime remained unchanged in its nature or composition, it simply adapted to the new scenario. Cybercrime polished its methods, its targets, in some cases even its organization, matching the new context in which it evolved.

Nevertheless, it should be noted that over the past 2 years, advancements within organized cybercrime have had other driving forces than the Covid crisis alone. One should bear in mind the necessary adaptation of operating methods, the attack tools used, the choice of targets, imposed by technical developments: in that sense, cybersecurity can make certain targets too resistant, require too much effort on the part of the attackers, making the intended targets less attractive. Certain skills may also become necessary while others are no longer required due to technical and technological advances.

– The scarcity of criminal opportunities in the confined "offline" world could have prompted a shift from "offline" crime to "online" crime [PLA 21]. This hypothesis has its detractors [MIR 21] for whom the shift does not occur from offline to online crime, but mainly within the online crime category.

I.2.2. *Theoretical frameworks*

Focusing on the transformations in the lifestyles and daily practices of hundreds of millions of individuals throughout that period at a global scale – something which offered new opportunities for crime – the routine activity theory [COH 79] became popular as the main explanatory framework [HAW 20, KEM 21, GOV 21, HOR 21, PLA 21, CHE 21, KOP 22, OLO 22, IMS 22].

According to this theory, a crime is likely to be committed when three conditions are met: the presence of a motivated offender, the presence of an accessible target to the offender/criminal and the absence of an efficient guardian. Target vulnerability increases when all three elements are present. Hawdon et al. [HAW 20] have argued that the societal changes forced by the compulsory lockdown quantitatively and qualitatively increased those conditions. Vulnerability, or in this case cyber risk, increased because the threat (the motivated malicious actor) and the vulnerability (the presence of suitable targets) converged on the same place (cyberspace) at the same time.

In Collier et al. [COL 20], low-level cybercrime (in terms of technical capabilities) may have increased due to the rise in the number of confined teenagers and young adults who seemed to be launching simple attacks against poorly protected networks just for fun and to earn a little money. This idea was further discussed by Payne [PAY 20] who also claimed that a

significant victimization of people aged 50 and over (less equipped to digitally defend themselves and with poorer cyber-hygiene) was observed during the first lockdown wave. Cybercrimes such as pandemic-themed targeted frauds were particularly used by cybercriminals.

On the whole, there seems to have been both an increase in the number of delinquents motivated by the money and the recreational dimension and the presence of targets meeting the goals of cyberdelinquents, especially those lacking well-established security habits. To this should be added the fact that areas affected by the lockdown also included cybersecurity actors from private companies and government agencies. Unavoidable teleworking forced many employers to focus their attention on helping employees transfer work to their homes, but overlooking network securitization. As network security was not necessarily ensured by cybersecurity services, the responsibility of monitoring a larger part of the networks was entrusted to the police services. Regarding this point, Dupont explains that classic police methods prove insufficient in the case of imminent lockdown: "Classic police investigation and arrest methods are proving insufficient, as they are too slow to produce tangible results on a large scale. They are most effective when combined with innovative damage prevention and mitigation strategies" [DUP 20].

However, the impacts of forced lockdown were too rapid to deploy preventive measures. For example, mitigation advertising campaigns were launched toward the end of March and the beginning of April 2020 in Canada. The reduction in network protection capabilities and resources was a corollary effect of the first lockdown phase.

Several authors have based their analyses on the routine activity theory in order to account for the particular structure of opportunities having arisen as a result of lockdown regulations in the United States and the Canadian provinces. The increase in the attack surface, in the number of cybercrime actors with diverse motivations and resources, and network monitoring issues have all been mentioned as factors influencing user and network vulnerability. Added to this is the great adaptive flexibility of criminal groups, as described by Gayraud, which has facilitated the activity adaptation of such groups to the global pandemic context, by relying on the "diffuse criminological background" of cyberspace.

I.3. Our research questions

This work studies the role of cybercrime in the world and its evolution, during the early pandemic period (in the first days of the year 2020), which is still not over at the time of writing these lines. The case studies discussed contribute to reflections on the link between cybercrime and crises as well as on the explanatory variables of cybercrime.

I.3.1. *Chapter 1 – The evolution of cybercrime during the Covid-19 crisis*[7]

The dominant narrative since the first months of the Covid-19 epidemic expressed that, through the effects produced on societies, there was a significant (sometimes even spectacular) increase in cybercriminal activity. Not only the health crisis scenario but also its economic consequences were believed to foster a context favoring cybercriminal activity, as well as increasing the risk of online victimization.

By consulting statistical series produced in several countries, we intend to call into question such an assumption: do the figures really confirm this assertion? Is the evolution of the cybercrime trend correlated with the various phases of the health crisis?

In an attempt to answer those questions, CERT (Computer Emergency Response Teams) reports and police data will be used as the main data sources on the state of cybercrime, which will then be compared to data reflecting the changes in citizen lifestyles. The lockdown and restrictions on the mobility of individuals being one of the main indicators of these modifications, data on mobility is studied in depth in order to reconstruct the chronology of the lockdown periods.

The central question regarding the evolution of cybercrime trends during the health crisis will also be addressed by focusing on the evolution of cyberattacks on the international scene.

7. Daniel VENTRE, CNRS, CESDIP Laboratory (Guyancourt, France).

I.3.2. *Chapter 2 – The SARS-CoV-2 pandemic crisis and the evolution of cybercrime in the United States and Canada*[8]

As in the rest of the world, the pandemic crisis caused by SARS-CoV-2 in 2020 disrupted the normal functioning of societies in Canada and the United States. In terms of cybersecurity, it is highly probable for malicious actors to have adapted their practices to the pandemic context. This means that cybercrime evolved and became adapted to the new context. The chapter outlines these changes based on government and private organizations' reports on cybercrime, offering a critical perspective. Cybercrime in the United States and Canada during the pandemic crisis is analyzed in its various trends. The need for international cooperation to counter cybercrime and the methodological challenges encountered during the study conclude this chapter.

I.3.3. *Chapter 3 – Online radicalization as cybercrime: American militancy during Covid-19*[9]

The January 6, 2021 attack on the Capitol in Washington signaled the culmination of a broader period of sociopolitical activism in the United States. The trajectory of this period, which in many ways is still extending, closely followed the spread of the SARS-CoV-2 pandemic. The purpose of this chapter is to explore to what extent the basic analytical framework of cybercrime theory is still valid under pandemic conditions. We argue that the unprecedented pressure of accelerationism experienced in the United States during Covid-19 compels us to rethink online radicalization as a form of cybercrime. The extraordinary scope, speed and overall dynamics of accelerationist activity having challenged secular American institutions in recent years are all signs of a new kind of symbiotic association between online and offline elements.

8. Prof. Hugo LOISEAU, École de Politique Appliquée, University of Sherbrooke, Quebec, Canada.

9. Joseph FITSANAKIS, Professor of Intelligence and Security Studies, Coastal Carolina University, United States.

Alexa MCMICHAEL, Special Security Officer, Intelligence Operations Command Center, Coastal Carolina University, United States.