Measuring Cybercrime in Europe: The Role of Crime Statistics and Victimisation Surveys

Proceedings of a Conference Organised by the Council of Europe with the Support of the European Union, 29-30 October 2020

Marcelo F. Aebi
Stefano Caneppele
Lorena Molnar (Eds.)

eleven

Cybercrime has become part of everyday life. We live in hybrid societies, fluctuating between the material and the virtual world, and we are hence confronted with online, offline and hybrid offences. However, the few victimisation surveys conducted in Europe reveal that victims of online crimes seldom report them to the police. Consequently, cybercrimes – which according to the best estimates represent between one third and more than half of all attempted and completed crimes in Europe – seldom appear in national criminal statistics. The State seems powerless to prevent them and private security companies flourish.
During two days, experts from all over the continent gathered together in the framework of a virtual conference organized by the Council of Europe and the European Union to discuss what we know, what we do not know, and what we could do to improve our knowledge of crime in our contemporary hybrid societies, develop evidence-based criminal policies, provide assistance to crime victims, and implement realistic programs in the field of crime prevention and offender treatment. This book presents their experiences, reflexions, and proposals.

Marcelo F. Aebi, PhD, is Professor of Criminology at the University of Lausanne, Switzerland. He is also a consultant expert of the Council of Europe, head of the European Sourcebook Group, executive secretary of the European Society of Criminology and chair of the Scientific Advisory Board of the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). He publishes regularly in scientific journals in English, French, Spanish and Italian.
https://orcid.org/0000-0002-3449-1093.

Stefano Caneppele, PhD, is Professor of Criminology at the University of Lausanne, Switzerland. Among his research domains, he is interested in the study of the interaction between technology, crime and its social reaction. He is also a consultant expert of the Council of Europe and member of the European Sourcebook Group of Crime and Criminal Justice Statistics. *https://orcid.org/0000-0003-3924-4937*.

Lorena Molnar, MA, is a PhD candidate and research assistant at the University of Lausanne, Switzerland. Her main domains of interest are comparative criminology, innovation in methods and hard-to-reach vulnerable populations. She is a member of the SPACE (Statistiques Pénales Annuelles du Conseil de l'Europe) team and of the European Sourcebook Group and co-author of the sixth edition of the European Sourcebook of Crime and Criminal Justice Statistics.
https://orcid.org/0000-0001-8692-9256.

ISBN 978-94-6236-245-1

Measuring cybercrime in Europe: The role of crime statistics and victimisation surveys

Measuring cybercrime in Europe: The role of crime statistics and victimisation surveys

Proceedings of a Conference Organised by the Council of Europe with the Support of the European Union, 29-30 October 2020

Marcelo F. Aebi, Stefano Caneppele & Lorena Molnar (Eds.)

With presentations and interventions by (in alphabetical order):
Marcelo F. Aebi, Andri Ahven, Annie Devos, Billy Gazard, Marianne Junger, Pieter Hartel, Michael Levi, Fernando Miró-Llinares, Matti Näsi, Lieven Pauwels, Francisco Sánchez-Jiménez, Alexander Seger, Nicole Samantha Van Der Meulen, Mari-Liis Sööt & Johan van Wilsem

eleven

Published, sold and distributed by Eleven
P.O. Box 85576
2508 CG The Hague
The Netherlands
Tel.: +31 70 33 070 33
Fax: +31 70 33 070 30
email: sales@elevenpub.nl
www.elevenpub.com

Sold and distributed in USA and Canada
Independent Publishers Group
814 N. Franklin Street
Chicago, IL 60610, USA
Order Placement: +1 800 888 4741
Fax: +1 312 337 5985
orders@ipgbook.com
www.ipgbook.com

Eleven is an imprint of Boom uitgevers Den Haag.

ISBN 978-94-6236-245-1

Recommended citation (APA 7th ed.): Aebi, M.F., Caneppele, S., & Molnar, L. (2022). *Measuring Cybercrime in Europe: The Role of Crime Statistics and Victimisation Surveys. Proceedings of a Conference Organised by the Council of Europe with the Support of the European Union, 29-30 October 2020*. Eleven.

Table of Contents

Measuring Cybercrime in Europe: A Conference Introduction

Marcelo F. Aebi, Lorena Molnar and Stefano Caneppele[*]

The conference 'Measuring cybercrime in the time of Covid-19: The role of crime and criminal justice statistics' took place as a video conference on 29 and 30 October 2020. It was organised in the framework of a project funded by the European Union and the Council of Europe and implemented by the Council of Europe. That project was placed under the responsibility of Prof. Marcelo F. Aebi, who, as a consultant, fulfilled the task with the support of the University of Lausanne.[1]

The conference was organised by a scientific committee composed of four members including the consultant, Prof. Stefano Caneppele from the University of Lausanne, Switzerland; Prof. Michael Levi from Cardiff University, Wales, UK; and Prof. Fernando Miró from the University Miguel Hernández of Elche, Spain. The scientific committee met in Strasbourg on 6 March 2020 and planned a conference that should have taken place at the premises of the Council of Europe, in Strasbourg, under the title 'Cybercrime in Europe now: How we measure it, how we respond to it.' One week after that meeting, the lockdowns introduced in most countries to prevent the spread of Covid-19 forced the Council of Europe to postpone the conference. In spite of that, the scientific committee remained in contact through emails and virtual meetings, and, with time and patience, it was finally possible to organise it as a virtual conference and under an appropriately adapted title.

The readers of this book will soon realise, however, that the contents of the conference and its potential implications for policymaking and research go well beyond what can be done during a pandemic. That is the reason why the title was adapted once more for this publication, which includes the proceedings of the conference. The presentations and interventions during the panel discussions were first transcribed by Lorena Molnar from the University of Lausanne, but the final versions included in this volume are not literal transcriptions. We have removed the breaks in speeches and edited the incomplete sentences and repetitions that characterise oral discussions. We also deleted the usual courtesy exchanges between speakers, and we gave speakers and discussants the opportunity to edit, update or improve their interventions. All that was done while trying to keep the tone

* University of Lausanne, Switzerland.

1 Council of Europe's Consultant's contract N°237/2021.

of the spoken language, and we assume responsibility for any mistake that may persist in this final version.

The conference combined plenary sessions and discussions between speakers and discussants. It was opened by Ilina Taneva, from the Council of Europe, and Annie Devos, Chair of the Council for Penological Co-operation (PC-CP) of the Council, who welcomed the participants and presented the general framework of the conference. The opening speech by Fernando Miró-Llinares summarised the first research results on the impact of Covid-19 on cybercrime and suggested a series of measures to improve that knowledge. After him, Michael Levi (UK) presented the current efforts made throughout Europe to modernise crime statistics by including cyber-related offences, which currently are seldom recorded. In that perspective, the following two presentations were dedicated to the projects put in place in Estonia and Spain to reach the level of modernisation required. In particular, Andri Ahven and Mari-Liis Sööt showed how cybercrimes are recorded in Estonia, while Francisco Sánchez-Giménez concentrated on how they are recorded in Spain. The last presentation of the first day of the conference was presented by Lieven Pauwels (Belgium) who illustrated the way in which alternative indicators of crime can help to measure cybercrime. In particular, Prof. Pauwels showed the way in which self-reported delinquency surveys can help to reach that goal.

In a similar perspective, the presentations made during the morning of the second day focused on the use of victim surveys to measure cybercrime. First, Marianne Junger and Pieter Hartel (Netherlands) presented an overview of the situation at the international level and an empirical test of the comprehension of the wording of the questionnaire used in the Netherlands to measure different types of cybercrime. Then, there were three presentations devoted to how cybercrimes are currently measured in victimisation surveys conducted in specific countries. In that context, Johan van Wilsem presented data from the Dutch survey, Matti Näsi presented data from the Finnish survey and Billy Gazard presented the crime survey data for England and Wales. In the afternoon, Ricardo Estrela focused his presentation on how victims of cybercrime are assisted in Portugal by a specialised association, Nicole Samanta van der Muelen introduced Europol's 'Internet Organised Crime Threat Assessment', and Michael Levi discussed the rehabilitation of cybercriminals focusing on deterrence, diversion and desistance from cybercrime. The conference ended with a long and thought-provoking panel discussion between several of the experts who participated in it.

The organising scientific committee regrets two absences. The private companies that collect extremely useful data on cybercrimes and were invited to participate in the conference declined the invitation, and our colleague Graham Farrell (University of Leeds, UK) could not participate in the panel that we would have liked to organise about the role of rising cybercrime rates in the drop of offline offences observed in some industrialised countries in the 1990s and 2000s.

In sum, the first part of the conference was dedicated to the measures of cybercrime that can be obtained through crime statistics, while the second one focused on measuring cybercrime through surveys, including self-reported delinquency studies and victimisation surveys. The latter received particular attention. Finally, the third part of the conference covered the intersection between cybercrime and organised crime as measured by Europol, and it also introduced the human dimension of cybercrime, by concentrating on cyber offenders and their victims.

Towards Hybrid Measures of Crime for a Hybrid Society

Lessons Learned from a Council of Europe's Conference on Measuring Cybercrime

Marcelo F. Aebi[*]

Introduction

This chapter aims to put together in a coherent framework the different presentations and discussions that took place during the conference on measuring cybercrime organised by the Council of Europe with the support of the European Union in October 2020 (see the previous chapter for details). The Budapest Convention on Cybercrime provides broad-ranging definitions of offences against the confidentiality, integrity, and availability of computer data and systems, computer-related offences, content-related offences, and offences related to infringements of copyright and related rights; however, these definitions must be operationalised in order to know the extent and the characteristics of the different phenomena placed under the overarching category of cybercrime. The conference allowed participants to get acquainted with some of the best practices in that field.

In that perspective, the chapter is organised as a series of questions that we have answered through the presentations and discussions that took place during the conference: what do we know about cybercrime? How do we know that? What do victimisation surveys tell us about the extent of cybercrime? Is cybercrime ubiquitous? If yes, what are the consequences in terms of fear of crime and crime prevention? Are states giving cybercrime the importance it deserves? What is the role of private security against cybercrime? And finally, what can be done to measure cybercrime in Europe both through national crime statistics and a European Victimisation Survey?

Summarising in a few pages the one-and-a-half days of talks and exchanges between experts requires making choices. Our main criteria when prioritising some aspects of the conference over others is to provide a useful and concise text for policymakers. Those interested in implementing evidence-based policies to prevent cybercrime will find here a few concrete proposals. These proposals do not reflect any official position of the Council of Europe, the European Union or the participants in the conference. Finally, we have also tried to produce a text that remains accessible to the general public, written in plain language, and following the oral style privileged throughout this book.

* University of Lausanne, Switzerland.

Marcelo F. Aebi

What Do We Know about Cybercrime?

The General Context: Our Hybrid Society

In the Council of Europe member states, at least two-thirds of the population use the Internet. In the vast majority of them, that proportion reaches at least three-quarters, and in a few, it is over 90%.[1] Broader access to the Internet was triggered by the development of smartphones since 2007, and in most member states there are more mobile phones than inhabitants. Almost all users participate in social media platforms like Facebook, YouTube, WhatsApp or Instagram. The massification of social networks started in 2008; it is true that they are particularly popular among young people – they are used by roughly 90% of Europeans aged 16 to 24 – but persons of all ages participate in them. On average, in the OECD (Organisation for Economic Cooperation and Development) countries, 90% of the population aged 16 to 24 use social media, and those aged 14 to 24 spend more than 4 hours every day on the Internet. Once more, the overrepresentation of young people among users must not hide the fact that we are living in a hybrid society, both digital and analogue, both virtual and tangible. If someone still had doubts about that, the lockdowns proved how societies can survive in a hybrid world and forced practically all inhabitants to use the Internet.

The Specific Context: Crime in a Hybrid Society

If one assumes that deviance is inherent to human nature, then, in a hybrid society, crime should take place offline, online, as well as both offline and online. For example, an offender can harass, insult or attack her or his victim both orally and through social media. However, there are very few traces of hybrid and online offences in the criminal statistics of most countries. In practice, this means that *official* measures of crime are bad indicators of cybercrime and is explained by several reasons. It is a well-known fact that official criminal statistics do not measure crime but only the social reaction to it, in the sense that they refer to the small portion of crimes that come to the attention of the authorities of the criminal justice system. This proportion varies according to the type of crime, and research shows that the percentage of online offences reported to the police is extremely low, perhaps – for some of them – the lowest among all types of offences. That percentage varies according to the type of cybercrime and goes from 1% (if one takes into consideration cyber offences against businesses and industries) or 2% (in Finland) to 10%-15% (for some of the offences

1 All the quantitative information presented in this paragraph is taken from the web portal *Our World in Data* (https://ourworldindata.org/internet).

included in the Crime Survey for England and Wales).[2] In addition, some hybrid crimes will appear in official statistics as offline offences – that could be the case in the example of hybrid harassment or stalking mentioned above – and some online crimes will be veiled because they are recorded under a general category, which originally was an online category. That is typically the case of cyber frauds recorded under the overarching category of frauds, but which represent, in countries that keep track of the distinction in the modus operandi, the vast majority of frauds.[3]

Furthermore, we know much less about cybercrimes against businesses. This is due to two main reasons. The first one is that businesses usually try to avoid the negative publicity they receive when their security failures become known to the general public, which means that many of these failures remain unknown. The second reason is that in most countries there is a lack of victimisation surveys on crimes against businesses. The exception is England and Wales that runs an annual Commercial Victimisation Survey since 2013,[4] though more limited commercial business victimisation surveys had begun already in 1986 and continue with the biennial PwC (PricewaterhouseCoopers) economic crime surveys.[5]

Finally, we know even less about cyber threats to national security. In that field, like in terrorism, the protection of the population often requires treating some of the attacks in a confidential manner, even if the European Union Agency for Cybersecurity (ENISA) collects data on them.

How Do We Know What We Know about Cybercrime?

We know that only a tiny minority of cybercrimes are reported to the criminal justice authorities because some countries are conducting victimisation surveys regularly. Victimisation surveys ask not only whether the person was a victim of a cybercrime but also whether she or he has reported the crime to the police or other authorities. If roughly 10% of the cybercrimes are known to the criminal justice system, then one can say that the vast majority of what we know about the extent and characteristics of cybercrime comes from victimisation surveys. In other words, currently, only cybercrimes against individuals are being measured, albeit imperfectly, in the few countries that run victimisation surveys.

2 See the presentations by Seger, Näsi, and Gazard (in this volume).
3 See the presentation by Gazard (in this volume).
4 See www.gov.uk/government/collections/crime-against-businesses.
5 See Levi, M. (1998). The Prevention of Fraud. Crime Prevention Unit Paper 17. Home Office.

What Do Victimisation Surveys Tell Us about the Extent of Cybercrime?

In Finland, 55% of the respondents in the national survey had reported suffering some form of cyber victimisation during their lifetime and 25% during the previous years. As this is a representative survey, it means that more than half of the population have already been victims of a cybercrime and a quarter of it were victimised in the previous 12 months. In Estonia, 40% of the population have been victims of phishing and 45% of those aged 16 to 26 have been victims of sexual harassment online. The prevalence rates are similar in both countries, and the empirical research presented in this conference goes in the same direction; hence, there is no reason to believe that the rates would be radically different in other Nordic, Central or Western European countries. Of course, some cybercrimes are less common than others. For example, a review of nine surveys – from France, Germany, Luxembourg, Netherlands, Sweden and England and Wales – conducted by Reep-van der Bergh and Junger (2018) revealed annual prevalence rates – percentage of the population victimised during the previous 12 months – ranging from 1% to 3% for online shopping fraud, banking fraud, bullying, stalking and threatening, up to 6% for hacking and up to 15% for malware.[6] At the same time, in England and Wales, the inclusion of fraud – including its current main category of cyber fraud – and computer misuse in the national crime survey led to a one-third increase in the total number of crimes unveiled by the survey.[7] These results mean that cybercrime is part of everyday life.

Is Cybercrime Ubiquitous?

The prevalence rates shown above prove that some online and hybrid offences have become more common than traditional offline offences. In that perspective, Hans von Hofer liked to say that crime 'is a social construct, labelled as "deviant" behaviour, which means that crime cannot rise endlessly, otherwise it would become "common" behaviour' (von Hofer, 2010: 4).[8] However, for those of us whose email is in the public domain, the exposure to the risk of becoming a victim of cyber offence, namely in the form of different types of scams – which could be legally qualified as attempted *phishing* – has become the norm. Every week, we win a lottery, we are required to pay 'taxes' for merchandise we never bought, we are invited to help a widow who inherited a fortune, we are invited to become editors of unknown journals and so on. In that context, measuring the frequency (also

6 Reep-van den Bergh, C.M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7*(1), 1-15.

7 See the presentation by Gazard (in this volume).

8 See, for example, von Hofer, H. (2010). A Scandinavian perspective. *Criminology in Europe: Newsletter of the European Society of Criminology, 9*(1), 4 and 19.

known as the incidence) of such offences becomes useless. Some types of cybercrimes like phishing and computer viruses are omnipresent.

In Terms of Fear of Crime, What Are the Consequences of the Ubiquity of Cybercrime?

When a behaviour becomes omnipresent, one has to learn to live with it and minimise its negative consequences. This creates insecurity and anxiety in the population. It also undermines the fiction of the social contract through which individuals would have surrendered to the state a part of their freedom in exchange for protection. In short, it undermines the legitimacy of the state, which explains why the authorities are reluctant to put the cybercrime discourse at the centre of their public messages.[9]

The ubiquity of cybercrime has certainly an impact on the fear of becoming a victim of it. The Finnish crime survey shows that the population is more afraid of becoming a victim of cybercrime than of becoming a victim of a traditional crime. This fear is rational because we know now that the odds of becoming a victim of cybercrime are higher than those of becoming a victim of traditional crime. This is not the first time that research falsifies the hypothesis of an irrational fear of crime among the population. Even for traditional crimes, the surveys conducted using big representative samples that allow analysing fear of crime by neighbourhoods show that, on average, respondents are quite realistic about their chances of becoming victims of a crime.

In Terms of Crime Prevention, What Are the Consequences of the Ubiquity of Cybercrime?

We have suggested that the ubiquity of crime implies that the state is failing, at least for some types of cybercrimes, to ensure the protection of its citizens. This means that citizens have to find an alternative way of protecting themselves.[10]

Big corporations and many businesses seem to have accepted this state of affairs and seek security by engaging the services of private security companies.[11] For individuals, that is still only partially true, although there is reason to believe that, for better or for worse,

9 See the second panel discussion on rethinking victims' assistance and deterrence models (in this volume).

10 This is not something new in the history of humanity, but in the past, it only happened in the material word. For example, in the US, when the colonisers started to establish themselves in the west of the US in the 19th century or during the great immigration period at the beginning of the 20th century. In the first case, protection was often assured through sheriffs appointed by the citizens, while in the second one the vacuum of power was often exploited by organised criminal groups through protection rackets.

11 See the presentation by Seger (in this volume).

it is only a matter of time. We can draw here an analogy with road safety. Whenever you drive your car, you know there is a risk of crossing some irresponsible – or at least distracted – drivers and that you can also make a stupid manoeuvre in one second of inattention. This means you have to be careful and attentive constantly. Consequently, crime prevention campaigns must draw attention to that fact, and in practice that is what they very often do. Crime prevention campaigns against cybercrime will also have to place self-protection at their centre. This will probably be criticised by idealists – who imagine a utopian world without deviance – as a sort of 'blaming the victim' campaign; but, in fact, it just reflects the crude reality.

In that perspective, one should keep in mind that there is at least one type of cybercrime for which the public has already accepted this reality. In the 1980s, the first time we heard about 'computer viruses', the concept seemed absurd. Viruses – like Covid-19 – attacked only the living organisms. In spite of that, a few years later everyone was using anti-virus software instead of complaining to the government for not fulfilling its obligation of protecting the citizens.

Still, the state cannot fully give up its obligation of protecting its citizens, and the most realistic proposal in that context has been the one presented by Michael Levi,[12] who sees private-public partnerships as the way forward.

In addition, the state could support research on crime prevention because, as pointed out in the same presentation and in the panel discussion that followed,[13] little is known about how to deter cyber offenders. In that perspective, self-reported delinquency studies can play a major role in the explanation and prevention of cybercrime committed by young offenders.[14]

Are States Giving Cybercrime the Importance It Deserves?

As pointed out by Michael Levi,[15] there is a contradiction between public statements about the relevance of cybercrime and what is concretely done to control it. Broadly speaking, governments are confronted with three types of cyber threats: national security threats (cyberattacks on public institutions), threats to the business sector and threats to their citizens. In practice, they seem to have chosen to concentrate their efforts on the prevention of the first kind of threats and also to consider threats to their main industries as national

12 See the second presentation by Levi on counting cybercrimes reduction (in this volume).
13 See the second panel discussion on rethinking victims' assistance and deterrence models (in this volume).
14 See the presentation by Pauwels (in this volume).
15 See the interventions of Levi in the second panel discussion on rethinking victims' assistance and deterrence models (in this volume).

security threats.[16] The answer to the question that gives the title to this section is then 'it depends': national security cyber threats are receiving a lot of attention, while cybercrimes against citizens are not.

What Is the Role of Private Security against Cybercrime?

As anticipated above, there has been a rise in the level of the security provided by the private sector to prevent cybercrime. If one places that rise in a broader context, it is indeed the continuation of a trend towards the privatisation of security that became prominent in Europe in the 1990s. In the field of cybercrime, it first took form with the creation of antivirus software by private companies.

In terms of compensation for the damages caused by cybercrime, there has also been a rise in Internet-related insurances provided by private companies. This corroborates that citizens have become fully aware of that threat, which coincides with the levels of fear of cybercrime mentioned above. A similar trend had been observed in the second half of the 20th century, when the rise of property offences was accompanied by a rise of theft insurances.

The trend towards the privatisation of security seems almost impossible to reverse, but at least could be mitigated, as mentioned before, through private-public partnerships. In any case, research can describe the situation, test potential ways to deal with it and inform about those that were efficient and those that were not; however, it cannot answer the question of what *should* be the role of private security. In democratic societies, that question must be answered by the citizens themselves.

What Can Be Done to Measure Cybercrime in Europe?

Improving National Statistics on Cybercrime

The presentations and discussions held during this conference corroborate that criminal statistics provide a poor measure of the extent and the characteristics of crime, and even more so of online and hybrid crimes. That fact does not mean that nothing can be done to improve them. In particular, two strategies seem promising.

The first one is to collaborate with banks, credit card companies, insurance companies, private security companies and social networks to obtain the data that will allow producing a new kind of criminal statistics. They can be considered as *hybrid* because they combine

16 See the presentation by Seger (in this volume).

the offences known to the authorities of the criminal justice system and the threats identified by the private sector.[17] As shown by Michael Levi, the UK is already using some mixed measures to produce its criminal statistics. The path towards these kinds of hybrid statistics is complex. Banks and credit card companies are probably not interested in the negative publicity they would get if the real number of frauds is revealed. Private security companies that make their living by selling protection for these threats may profit from that fact, but if the statistics highlight their failures, they may not like that marketing either. Some professional politicians may also dislike the negative publicity that such statistics could produce, but transparency is one of the pillars of democratic societies.

The second strategy is to introduce the possibility of 'flagging' the crimes that include a cyber element. This procedure is already in use or being developed in some member states, including in the UK and Switzerland. This allows estimating the percentage of crimes that are hybrid or online. This kind of statistics would require a different kind of analysis than the ones usually performed on official criminal statistics. In particular, the role of the *incidence* or *frequency* of crimes (that is to say the *number* of crimes) should become less important, mainly because many cybercrimes are attempted daily and, at a very large scale, targeting hundreds of potential victims.[18]

Finally, the offence definitions provided by the Budapest Convention on Cybercrime are a good starting point for developing better criminal statistics, but they need to be operationalised with even more detail as some of them include more than one specific offence.[19] From a legal point of view, it is acceptable to record crimes under the existing categories of offences, but if the goal is to understand crime and to develop successful criminal policies to reduce it and prevent it, the distinction in the modus operandi is necessary. This is in fact an old discussion that generally leads to opposition between criminal lawyers and criminologists. The latter usually received support from criminal analysts working in law enforcement agencies, which also preferred statistics based on *operational definitions* of crime rather than the legal *definitions*. For example, the overarching category of *theft* is completely useless to understand the profile of property offences in a country.[20]

17 See the presentation by Miró-Llinares (in this volume) and the presentation on the international effort in the modernisation of crime statistics by Levi (in this volume).

18 In addition, as suggested by Miró-Llinares (see his presentation in this volume), detailed information on the characteristics of the offence, the victim and the offender, whenever available – which is rare for many cyber offences – should be collected.

19 See the presentation by Junger and Hartel (in this volume).

20 See the presentation by Ahven and Sööt (in this volume) for examples in the field of cybercrimes.

Launching a European Victimisation Survey

The key message that this conference brings to policymakers is that there is a need for a European Victimisation Survey. If the word 'victimisation' seems too strong, it can be called 'European Safety Survey' (Euro SASU), a name that was already proposed more than ten years ago.[21] The Euro SASU should cover offline, online, and hybrid crimes. This is the logical conclusion of the fact that hybrid and online crimes are omnipresent in contemporary societies, that criminal statistics do not provide a good measure of them and that almost everything we know about how they affect citizens comes from the surveys already available.

Strengths

Human expertise: The availability of cybercrime experts who could collaborate in the development and analysis of a European Victimisation Survey is one of the major strengths of a potential Euro SASU project. The experts who participated in this conference and those affiliated with the working groups on cybercrime, victimology, and quantitative methods of the European Society of Criminology could easily collaborate in such a project.

Technical expertise: Several countries are already conducting victimisation surveys that include cybercrime modules. The experience gained through these surveys can provide a solid basis for a unified project, both in terms of the questionnaire to be used and the method of administration. In that perspective, the Covid-19 pandemic forced changes in the method of administration of at least one victimisation survey,[22] which will allow measuring the impact of such a change in response and victimisation rates.

Mapping crime in Europe: A common survey placed under the responsibility of the Council of Europe, ideally with the collaboration of the European Union, could provide a real map of crime across Europe, which should allow the development of at least some common criminal policies. One should not underestimate the impact of such an indicator on the economic experts of the European Union, which seem to have been trying for years to distribute the budget for justice affairs on the basis of an objective index.

21 Van Dijk, J., Mayhew, P., van Kesteren, J., Aebi, M. F., & Linde, A. (2010). Final report on the study on crime victimisation. Tilburg: University of Tilburg.

22 See the presentation by Gazard (in this volume).

Weakness: Existing National Victimisation Surveys

We have mentioned that the already existing national surveys can provide the basis of a common European survey, but at the same time, they may block its development. The few countries that already routinely carry out national victimisation surveys, especially if they cover cybercrime, may oppose the organisation of a Euro SASU invoking budgetary reasons – as they will be contributing to two similar surveys – and fearing, as it happened in the past, that a common survey will show different results than those of the existing national surveys.[23] This could be solved by not making the participation in the survey mandatory and by explaining clearly to the public that different methodologies and questionnaires will provide different results. Both strategies have been applied successfully with the Council of Europe Annual Penal Statistics (SPACE). It is true that not all countries participate in every annual wave of SPACE, but the participation rate is usually more than 90%.

Opportunity: Lack of Activists

A common misunderstanding among many activists is that the higher the figures they show, the better for their cause. This mistake has polluted the way in which several major problems faced by contemporary societies are perceived by the public.[24] Criminologists has clearly identified it, for instance, in the field of money laundering.[25] In fact, when research is based on surveys, it is quite easy to obtain high prevalence rates by manipulating the questions. Using very large questions produces constants (e.g. everyone, at least once, has felt himself or herself discriminated; everyone, at least once, has used illegal copies of songs or books) instead of variables that can be used for understanding and preventing crime. In the field of cybercrime, we have not identified individual activists interested in dramatising the situation. The perception could be different among private companies

23 For example, the latest *International Crime Victim Survey* (ICVS) conducted on a large scale in 2005-2006 showed that England and Wales were among the countries with the highest victimisation rates for some offences. This result did not contradict the fact that crime was decreasing in the UK according to their national crime statistics and crime surveys. It just showed that, even if crime was decreasing, it remained still at a higher level than in most continental West-European countries. A plausible hypothesis – that could be tested through interviews with the public officials in charge at that time – is that this fact played a role in the delay observed in the publication of the final results, which were made available only in 2008, and could have played a role in the lack of interest shown at that time by the representatives of some countries in the development of European Victimisation Survey.

24 See Rosling, H., Rosling, O., & Rönnlund, A. R. (2019). *Factfulness: ten reasons we're wrong about the world – and why things are better than you think*. Sceptre.

25 Levi, M. (2020). Evaluating the control of money laundering and its underlying offences: the search for meaningful data. *Asian Journal of Criminology¸ 15*(4), 301-320. https://doi.org/10.1007/s11417-020-09319-y; and Levi, M., Reuter, P., & Halliday, T. (2018) 'Can the AML system be evaluated without better data? *Crime, Law and Social Change*, *69*(2), 307-328. https://doi.org/10.1007/s10611-017-9757-4.

interested in selling security products. That is precisely one of the reasons why it seems better to develop a national victimisation survey, organised by a public institution with the support and advice of independent researchers.

Threat: If It Bleeds, It Leads

The mainstream mass media will surely highlight in each country the 'worst' results found in their own country, that is to say, the highest victimisation rates. A typical headline will be 'Our country has the highest rate of cyber fraud.' This cannot be avoided because the media prefers bad news (Pinker, 2018).[26] The experience with the publication of the SPACE reports is that the impact usually lasts three days and that the number of journalists who are interested in providing quality information and understanding the way in which figures are produced and their potential in terms of crime prevention has been increasing year after year. In that context, the presence of experts in criminology across the whole European continent should assure a proper explanation of the results of the survey and their interpretation. Finally, one should not underestimate the positive impact that a common measure of crime could have on governments that want to improve their national and international surveys through the use of evidence-based criminal policies.

Conclusions

We live in societies that fluctuate between the material and the virtual world. In such hybrid societies, we are logically confronted by online, offline and hybrid offences. However, most of the hybrid and online offences are not recorded in national criminal statistics. This knowledge comes from the victimisation surveys conducted in a few countries, which reveal that victims of these crimes seldom reported them to the police. The same surveys show that some types of cybercrime have become part of everyday life. Consequently, citizens are currently more afraid of becoming victims of cybercrimes than of traditional crimes. States can seldom protect their citizens from some types of cybercrimes, and, subsequently, private security companies have flourished. In order to improve the quality of national statistics, a collaboration with such companies – as well as with social networks – to obtain at least some of their data seems mandatory. However, the best indicator of the extent of online, offline, and hybrid offences would be a European Victimisation Survey, which could be conducted under the title of the European Safety Survey, or Euro SASU. Through such a survey as well as through self-reported delinquency studies and

26 See Pinker, S. (2018). *Enlightenment now: The case for reason, science, humanism, and progress*. Penguin Books.

experimental research, it would be possible to learn more about cybercrime and cyber offenders, and to develop effective prevention policies and ways of handling crimes and treating actual and potential offenders.

Welcome Addresses

Ilina Taneva (Council of Europe)

Good afternoon, everybody. I see that there are about 34 persons who are already online. This is going to be an entirely online meeting, something that we need to get used to. Thank you all for attending this meeting, despite these difficult times. As you know, the Covid-19 infections are rising in Europe, and, yesterday evening, the French president, Monsieur Emmanuel Macron, announced that there will be confinement measures since tonight until, at least, the 1st of December. So, all the meetings that were hybrid meetings – partially attended online, partially attended here – will now have to be cancelled or will have to be held in the remote mode only.

Another misfortunate event or a chain of events happening: the terrorist attacks that are happening lately in France. You know, of course, everybody knows about the beheading of the French teacher Samuel Paty because he was teaching about the freedom of expression. And today another terrorist attack happened in Nice: there were three persons who were killed: one of them beheaded, two of them were killed in a church. So, these are very difficult times for everybody. And all our condolences go to the families of the victims and to all the innocent people who are suffering because of this. We have to cope with that.

Of course, this also impacts the cybercrime as part of all other types of crime. And this is going to be the topic of today's and tomorrow's conference: how in times of Covid-19, the cybercrime is developing? What is the impact and how are the cybercriminals behaving and changing in the past days?

I also want to stress once again that this conference is organised in the framework of a project financed by the Council of Europe and the European Union. This is the beginning of a third phase of this project, and the outcome will be the publication of the proceedings of this conference, which will inform on the way cybercrime is defined and present proposals on how to measure it, as well as the problems faced by researchers when measuring such types of crime. But of course, I will leave the experts to explain to you in greater detail what is the aim of the meeting. So, without further ado, I would like to give the floor to Annie Devos, Chair of the Council for Penological Co-operation and also Director of the French-speaking probation service of Wallonia-Brussels, in Belgium.

Annie Devos (Chair of the Council for Penological Co-operation, Council of Europe)

Thank you, Ilina. Ladies and gentlemen, on behalf of the Council for Penological Co-operation, it is my pleasure to welcome you and to open the conference *Measuring cybercrime in the time of Covid-19: The role of crime and criminal justice statistics*. As stated by Ilina Taneva, the conference has been made possible thanks to a project jointly funded by the European Union and the Council of Europe. My special thanks go to Alexander Seger, head of Cyber Crime Division at the Council of Europe, and to his team with whose help we were able to contact and invite some of the experts. I do hope that the outcome of this meeting will be useful also to all of you and thank you for the very important and vast work done by the cybercrime division.

The aim of this meeting is to discuss how to measure the definitions of cybercrime according to the *Council of Europe Convention on Cybercrime*, *ETS No. 185*, also known as the *Budapest Convention*, as well as to its *Protocol on Xenophobia and Racism Committed through Computer Systems ETS, No. 189*. The world is rapidly changing, and new technologies and artificial intelligence have contributed a lot to rethinking necessities, to shaping the ethics, socially acceptable behaviour and responses to an unacceptable act. Security and public safety are facing new challenges. Human rights and freedoms are constantly endangered by new forms of crime, on the one hand, and by the reaction of the authorities to these crimes, on the other. A number of criminal acts are committed online; therefore, such notions as *territory*, *jurisdictions*, *time* and *perpetrators* as well as the enforcement of the respective measures to prevent and protect society have become difficult to define. In order to take action, it is really necessary to define and measure the phenomenon and its characteristics. It demands valid and reliable crime statistics. Therefore, the aim of this meeting is to identify all crime and criminal justice statistics, as well as how crime and victimisation surveys could be improved to capture the real extent and characteristics of cybercrime, which can take a variety of forms and can lead to an even bigger variety of consequences. Such an evaluation of the phenomenon is even more pressing in this time of Covid-19, during which the rise of cybercrime in different forms is palpable.

The team of experts who will deal with analysing the outcome of this meeting is headed by Marcelo Aebi, professor at the University of Lausanne. He is well known for collecting and publishing, since 2002, the Council of Europe Annual Statistics on Prison and Probation – also called *SPACE I* and *SPACE II* projects – as well as for publishing with a group of international experts the *European Sourcebook on Crime and Criminal Justice Statistics*. I wish you a resourceful and successful conference. Thank you very, very much to be there to share your experience. And I hope it will be a great time for all of us. Thank you very

much and see you very soon in this very special environment. And now the floor is to Professor Marcelo Aebi.

Marcelo F. Aebi (University of Lausanne)

Thank you very much, and welcome to everyone. I would like to start by thanking the trust put on me by the Council of Europe to organise this conference and also, as it was mentioned by Annie Devos, to produce since 2002 the *Council of Europe Annual Penal Statistics (SPACE)*. Even before that, in 1996, I entered for the *first* time in the *Palais d'Europe*, in Strasbourg, to participate in the *first* meeting of the enlarged group of experts who would produce three years later the *first* edition of the *European Sourcebook of Crime and Criminal Justice Statistics*. Almost a quarter of a century later, we are combining the strengths of these two projects. They both collect data, but they also collect something that is even more important in terms of measuring crime and the social reaction to it: *Metadata*; that is to say *data about the numerical data collected*. How are offences defined? When and how are the data collected? Which counting rules are applied?

One of the goals of the joint projects of the Council of Europe and the European Union that Ilina Taneva mentioned is to clarify the links between different indicators of crime and criminal justice. For instance, the hypothesis that imprisonment rates are completely independent from crime rates has been rejected by empirical research, but the relationship is extremely complex and selective. In Europe, for example, homicide rates are correlated with prison population rates, both when you conduct cross-sectional research – comparing countries in a given year – and when you conduct longitudinal research by analyzing trends in both rates[1] On the contrary, property crimes do not have any influence on levels of imprisonment, and the same is true for cybercrime. At the same time, property crimes represent the majority of crimes recorded by the police, while the few available surveys suggest that cyber-related crimes are currently the most common source of victimisation. In spite of that, cybercrimes are practically absent from crime and criminal justice statistics and, consequently, our efforts to collect such statistics – both through *SPACE* and through the *European Sourcebook* – proved unsuccessful.

It is not that *cybercrime does not exist* – as some constructivist friends would say – but that most of the time we have been trying in vain to operationalise it, to measure it. Hence, when I was asked to organise this conference, I followed Steve Jobs' advice of creating an 'A' Team, of putting together 'A' people, chosen from among the best specialists in the field. That is why I turned to Michael Levi, from the University of Wales, to Fernando

1 See Aebi, M. F., Linde, A., & Delgrande, N. (2015). Is there a relationship between Imprisonment and Crime in Western Europe?. *European Journal on Criminal Policy and Research*, *21*(3), 425-446.

Miró, from the University Miguel Hernández of Elche, Spain, and, of course, to my friend and colleague from the University of Lausanne, Stefano Caneppele. The three of them are globally renowned experts on cybercrime, and together we planned this conference in Strasbourg, just one week before the beginning of the lockdowns. Everything that is going to happen in these two days would have been impossible without them and, of course, without the efforts of Ilina Taneva and Christine Coleur from the Council of Europe.

During these two days, we will be discussing how is cybercrime currently measured by different crime indicators – specifically, crime statistics and crime surveys – and how it could be measured in a better way at both the national and international levels. That is why we will have interventions that adopt a European or international perspective and others that focus on the experience of specific countries.

After going carefully through the available research, the main hypothesis that Stefano and I have been considering is that measuring cybercrime requires surveys and may also require a different way of producing and analysing crime statistics. We are used to work with indexes and delinquency rates, but cybercrime is a very large concept and has many, many forms. It includes cyber-enabled crime and cyber-dependent crimes, and also all sorts of *hybrid crimes* that previously could only be committed offline. Hybrid crimes – think for example of bulling, harassment or some types of fraud that may start offline and continue online, or viceversa – are a key element of today's world.

Consequently, one plausible solution is to have an alternative indicator, which would be the *percentage of crimes that involved a cyber factor*: for instance, a computer, a smartphone, an online social network and so on. It is a different way of measuring delinquency, but it deserves to be discussed, and this conference seems to be a perfect forum for that. Hopefully, by the end of it, we will have some concrete proposals to improve the way in which we measure cybercrime. We are here to learn and discuss, so I really hope that we will all enjoy the conference!

Opening Session: Cybercrime in Times of Covid-19 and in Post-Covid-19 Era

Covid-19 and Cybercrime: What We Know, What We Do Not Know and What We Shall Measure

Fernando Miró-Llinares[*]

I would like to start, of course, by thanking the *Council of Europe* for organising this conference, and particularly Ilina and Marcelo Aebi, for giving me the opportunity to participate and also for inviting me as a speaker. I would really like to be in the beautiful Strasbourg and not in my own home, to be honest, but I still generally wish that this conference would help us to have a little break, even if only mentally, from the complex situation we find ourselves in because of the pandemic we are living in and which is worsening in Europe. So, maybe I should apologise from the very beginning, as my presentation may not help us much to forget, if I may, the *dumb virus*. The reason for saying this is that, as you will have noticed, I am going to talk about Covid-19 and cybercrime, although we will soon see Covid-19 is not the main argument here but only a context to reflect on what we know about cybercrime, what we still do not know and how we should collect the data and measure it in order to react better to this threat.

Therefore, the aim of this presentation is not to ask whether cybercrime grew during the pandemic, something that everyone took for granted even before there were any data available. From Europol to the United Nations to the FBI. Nor is it to give specific numbers of cybercrime increase, although I will provide figures and data from some recent research. The objective of my intervention, framed within the proposals of this conference that have been highlighted, consists basically of highlighting the enormous shortcomings that still exist in terms of both measuring the rate of cybercrime and the need to combine efforts to better understand a set of phenomena that encompass the concept of cybercrime, which is going to continue to increase in the future due to the process of social digitalisation that we were experiencing before the pandemic but one which Covid-19 has surely accelerated.

The presentation is therefore divided into three parts: in the first one, I will try to answer the question of what we can say barely 6 months later and with little official data about the Covid-19 crisis for cybercrime, starting with some very basic theoretical considerations that explain at least partially what has happened and then continuing with

* Miguel Hernández University of Elche, Spain. Additional material: the author's visual presentation is available at https://rm.coe.int/presentation-fernando-miro/1680a0339d.

existing data from official as well as private sources. This is the part that will take up most of my time. From there, and once we think we know something, I will reflect on how much we still do not know about cybercrime, pointing out the deficits of existing data sources, and ending with a brief thought on how we should measure cybercrime in order to have a clearer picture.

So, let me start from the beginning: what do we know about the impact of the Covid-19 crisis on cybercrime, or rather, what do we intuitively think the Covid-19 crisis means for cybercrime? I already said that even before we have had any data available, we all took an increase in cybercrime for granted. Why was that? On what basis did we think that what indeed happened, as we will see later, would happen? I think the answer is we were taking into account a very basic theoretical framework, which says that crime, like any other social activity, is determined in part by the context of the environment in which it occurs and, of course, by *opportunity* and that this has influenced crime and its evolution more than it seems. This can be made concrete, first of all, by the fact that in order for there to be crimes, offenders have to converge at a certain place with the victims, and, due to the lockdown, people stopped doing things on the streets and began doing them at home, which above all included leisure, working from home and so on, through the Internet. So, the opportunities and the crimes with it also moved online. And when the lockdown is over, they will return to the streets.

I am not saying anything that we do not already know; the graphs that I have made using Google data for Spain (Figures 1 and 2) show how the lockdown led to a drastic reduction in activity in the commercial areas and a corresponding increase in the time spent at home, and it will not be a surprise if I say that the increase in the amount of time spent at home led to an increase in both online leisure activities and online shopping.

Figure 1 Percentage of change in mobility in commercial and leisure areas in Spain from baseline (Source: Google Trends)

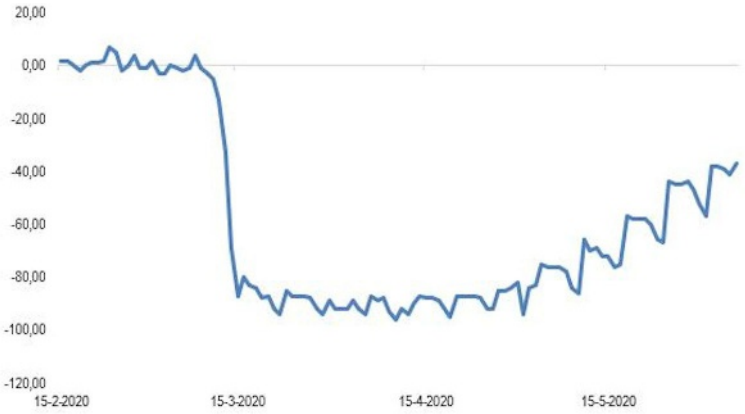
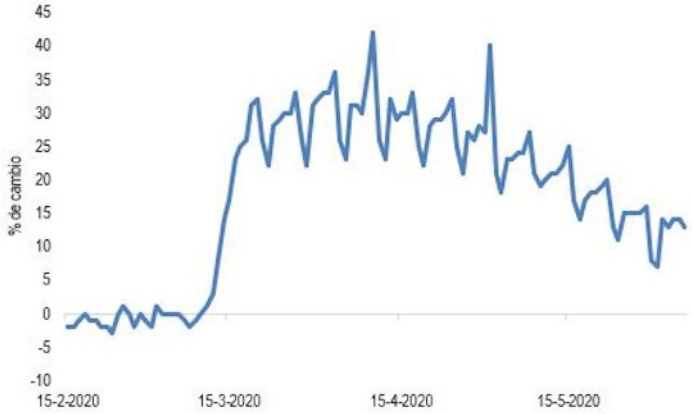


Figure 2 Percentage of change in mobility in residential areas in Spain from baseline (Source: Google Trends)



We call this a 'shift in opportunities', and it is the main hypothesis used to forecast a growth in cybercrime during the pandemic, and this criminal activity may decline but not return to its previous rates when the crisis ends, as long as working from home or online shopping continues. And this simple theory tells us something else: just as regular criminals move from place to place in the physical space to avoid surveillance or to improve the results of their crimes, so too the Internet cybercriminals change their targets to more vulnerable

population on the digital space and become more adept at conning them on the cyberspace. We could call this 'cyber offending opportunism', and it can be summed up in the idea that cybercriminals take advantage of people's weaknesses and interests to carry out their attacks; for example, as has happened during the crisis, when people are looking for terms like 'facemask', 'telework' or 'Covid-19' in Google , as these Google Trends graphs show (Figures 3 and 4), then cybercriminals will try to sell fake facemasks or create domains called Covid.

Figure 3 Covid-19 Google's search trend (Source: Google Trends)

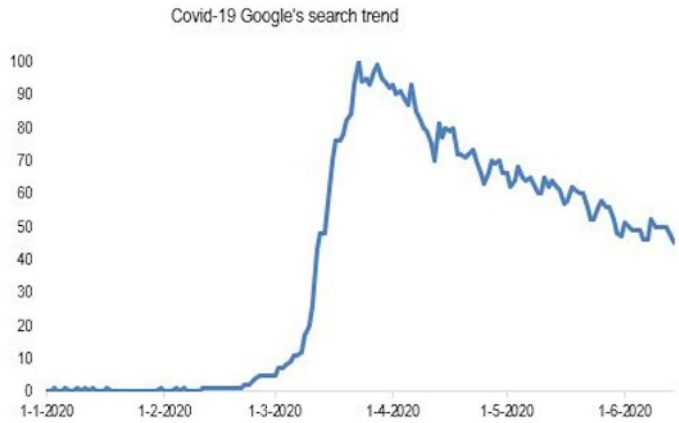
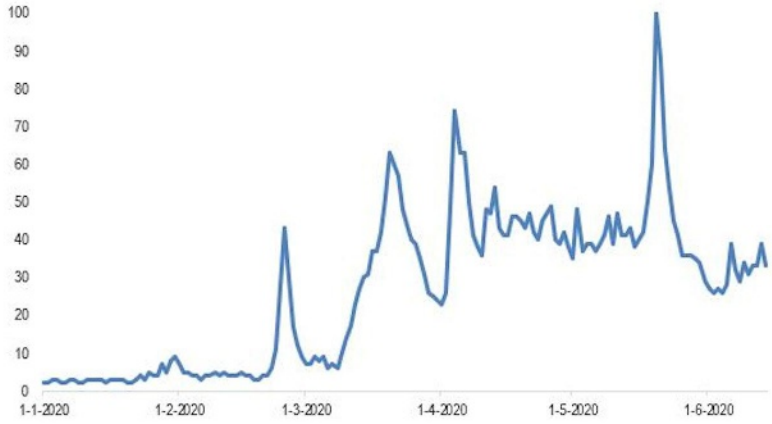


Figure 4 Facemask – Google's search trend (Source: Google Trends).



Well, what do the data tell us about this? Following this differentiation between shift of opportunities from the physical space to cyberspace on one hand and cybercriminals' opportunism on the other, let's see what private companies tell us about the impact of Covid-19 on cybercrime. Some interesting data are in accordance with the hypothesis of the shift of opportunities. The generalisation of teleworking produced by the lockdowns, with different times in different countries, according to the date of the lockdown, implies that workers use their home network to work and use different connection protocols, with a lack of knowledge of the risk that implies and seems to be in line with the increase of attacks by means of the remote desktop protocol detected by Kaspersky, used by criminals taking advantage, moreover, of vulnerabilities.

Some data sources also show us the opportunism of cyber criminals. This table of checkpoint shows an increase of more than 500% of the domain names registered between February and March in relation to the terms *Covid* and *Coronavirus* (Figure 5).

Figure 5 Coronavirus domains registered weekly (Source: Checkpoint)

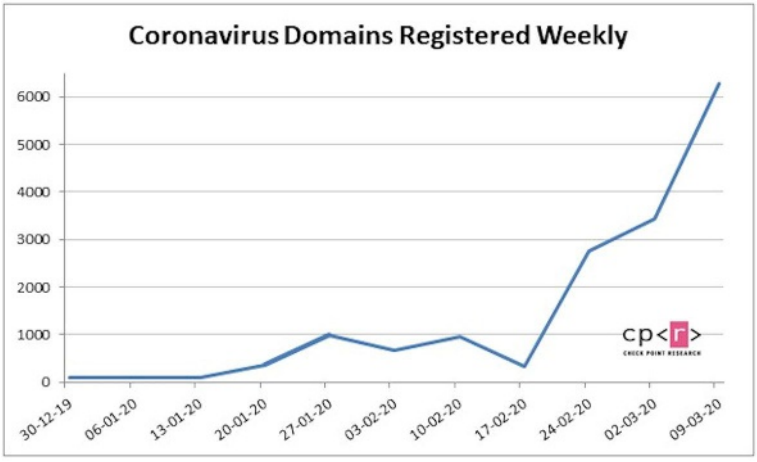
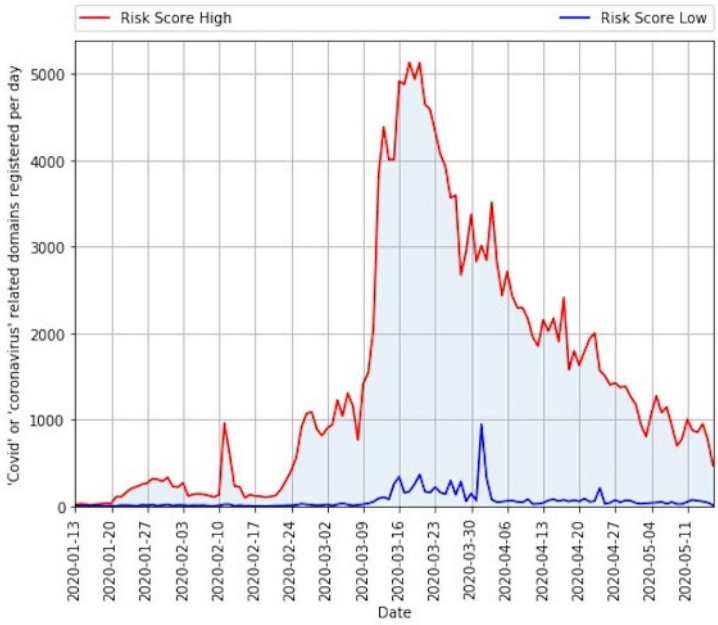


Figure 6, which depicts data from Domaintools, shows that in the same period the creation of malicious domains increased by 400%. The same relationship between the appearance of new domain names related to Covid-19 and a strong increase in the creation of malicious domains for sending a spammer scam is shown in Figures made with data from TrendMicro and Domaintools and not shown here, but available in the PowerPoint presentation. There is a change in the names of the cyber places from which cyber criminals attack, and there is also a change in the targets chosen by the cyber criminals.[1]

Figure 6 Risk domains created by week (Source: Domaintools)



1 See also Miró-Llinares (2021).

Figure 7 is based on data from the latest VPN report. It shows a significant change in the sectors attacked in 2019, and the data also show there has been a significant increase in the number of cyberattacks against information, health and manufacturing sectors as well as the transport and tourism sectors.

Figure 7 Percentage of change in the number of violations by sector affected, 2019 (Quarter 1) versus 2020 (Quarter 1) (Source: Own elaboration from the atlasvpn)

But what about the official sources related to cybercrime and opportunities? We have found many emails which warn that the health sector is being targeted by different types of attacks, such as phishing, ransomware or hacking. And there is also news about the appearance of networks that sell fake or spurious health products. But the information given in these ways is extremely broad and limits the scope for scientific observation. In relation to the shift of opportunities from the physical to cyberspace, and in order to know if the hypothesis that cybercrime would have grown is confirmed, we can look at the reports from Germany, Italy or Portugal – and some reports will be shown today – that inform us about changes in criminality during the pandemic, including specific reports about cybercrime. In general, these reports present details on the number of complaints against cybercrime and treat cybercrime as a single category. In some cases, they do not compare time periods or they analyse only very short time periods and, in turn, show inconsistent results. Thus, it is even harder to establish the evolution of cybercrime. Again, the lack of raw data, the lack of details on definitions in the reports, the lack of information on less serious crimes clearly show the limitations in drawing a clear picture on how cybercrime has changed, although it certainly seems to have changed.

As an exception, we have found some very interesting data in the Netherlands and some very interesting data provided by Action Fraud, which manages cybercrime complaints in the UK and which, in addition to being regularly updated, presents much more

information than the simple number of complaints, for example, a classification built up of crime, information on the type of victim (individual or organisation), the organisation that recorded the incident, all the value of the losses, among other interesting data. These data have allowed us to carry out a study in which some colleagues and I evaluate the impact of Covid-19 on cybercrime and online fraud, and we observed that it has certainly grown significantly. In the study, we calculated the relative change between the complaints registered in May 2019 and May 2020 about cybercrime and fraud. We observed that the total number of registered cybercrimes was much higher in May 2020 than in May 2019, with a 43% increase in the number of complaints registered in May 2020. This increase is remarkably large and is statistically significant in the case of PC hacking (77%), social network and email hacking (54%) and online fraud (50%; see Figure 8).

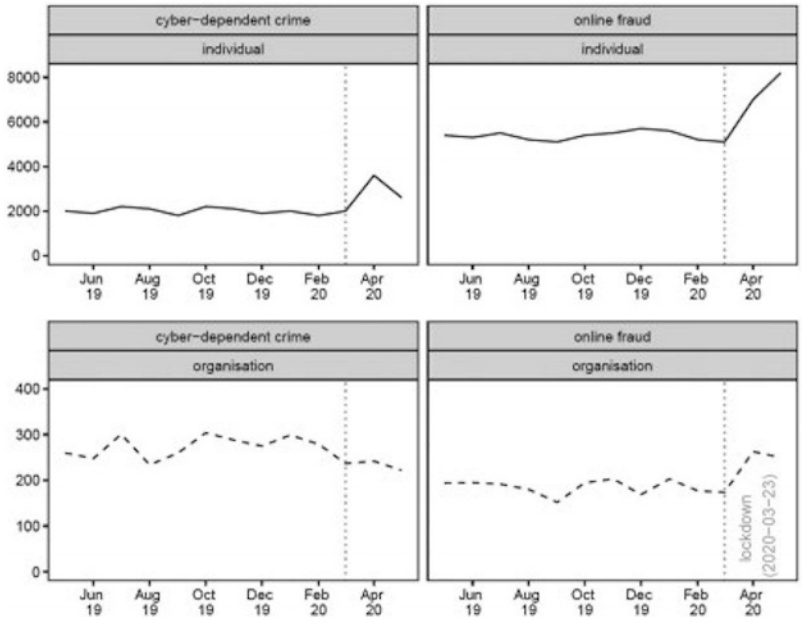
Figure 8 Relative change in the number of cyber-dependent crimes between May 2019 and May 2020 (Source: Buil-Gil et al. (2020))

	Count in May 2019	Count in May 2020	Relative change (%)
Computer virus/malware/spyware	742	648	−12.67*
Denial of Service attack	14	18	28.57
Hacking – Server	24	25	4.17
Hacking – Personal	270	479	77.41***
Hacking – Social media and email	939	1,449	54.31***
Hacking – PBX/Dial Through	9	7	−22.22
Hacking combined with extortion	313	251	−19.81*
Online fraud – online shopping and auctions	5,619	8,482	50.95***
All cybercrimes	7,930	11,359	43.24***

***p-value < 0.001, **p-value < 0.01, *p-value < 0.05.
Source: own elaboration (data from Action Fraud UK).

Nevertheless, the increase in cybercrimes has not happened homogeneously across crimes and types of victims, or depending on whether individuals or organisations were the affected parties. Furthermore, it is striking that crimes related to malicious software or hacking combined with extortion seem to have decreased. Maybe this is related to the fact that they affect mainly organisations. In contrast, the review of data for the month of June 2020 showed a strong increase in all cybercrimes. Then, the reports of crimes such as fraud in online shopping made by users began to fall in July, but reports of organisations for this type of crimes grew strongly again, possibly as a result of the delay in the detection of them by the organisations, which started noticing them with the reopening and the return to face-to-face work (see Figure 9).

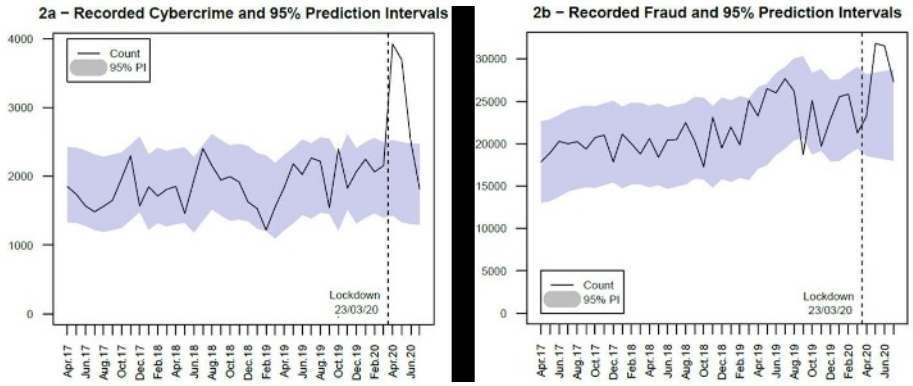
Figure 9 Trends for cyber-dependent crimes and online fraud based on types of victims (Source: Buil-Gil et al., 2020)



To try to understand whether these trends were only due to the lockdown or whether they will continue post-lockdown, we are now carrying out another study that uses data collected since 2017. We try to identify trends using a specific type of series prediction technique which allows us to generate a model with a confidence interval for past time-series data and evaluate whether the observed values fit the model.

This analysis shows a significant increase in cyber frauds, which is outside the predictive model only in the months following the outbreak of Covid-19 (Figure 10; see also the additional Figures included in the PowerPoint of the presentation). However, the trend changes when we look at different kinds of fraud. These data, collected monthly, allow us to make comparisons with other statistics on daily activities in order to seek explanations for changes in cybercrime beyond simply looking at two time periods – before and after the pandemic. The data show that cybercrimes seem to have risen, but are now beginning to stabilise. Furthermore, some modalities such as online fraud are beyond the scope of our forecasts, because they seem to continue increasing even after the end of lockdowns. Finally, the patterns of online shopping show that the growth in e-commerce denotes a concomitant rise in cyber fraud as well.

Figure 10 ARIMA models for cyber-dependent crime and online fraud (Source: Kemp et al., 2021)



Something else: with the data we now have, we know better what we still do not know about trends in cybercrimes, and, in the few minutes left, I will try to express it. First, we do not know how much cybercrimes have really grown and whether the growth has been above the expected trend, except in the case of the UK. Most countries do not provide monthly updates on the statistics presented in the annual reports and, since the calendar year 2020 has not yet ended, the annual reports have not been published. Hence, we do not know which countries have been affected the most. This makes it impossible for us to know whether countries with more severe confinement measures have been the ones more affected by cybercrimes and therefore whether our assumptions are true or are due to other factors.

As we have already indicated, the lack of data while waiting for the annual reports makes it impossible for us to compare the situation between countries. Also, the lack of proper definition of what cybercrime really is makes it difficult to compare between countries, and that problem will remain even with the arrival of the annual report. We also do not know which forms of cybercrime have grown because, with few exceptions, we only include generally a single category, namely, 'cybercrime', for all types of cybercrimes. And even in those cases where substantial data exist, there is still much to know. We have had problems even in the case of Action Fraud's cybercrime data published on a monthly basis that distinguish between various categories of cybercrime. First, in many cases, the data do not coincide with the data of the monthly report produced by the agency itself. Second, this type of data aggregate the raw victims, so the data do not allow us to differentiate between types of victims and identify population groups at risk. Nor do they allow us to know if the profile of the victim has changed: who are the most affected, how sociodemographic and other factors influence cybercrime and so on. And, last but

not the least, these data are from complaints. Although it is relatively easier in the UK than elsewhere to report cybercrime, we know that a significant number of crimes have gone unreported. Hence, we do not know how many crimes have actually been committed. The pandemic has also modified how we work and communicate, and this could also affect the capacity to detect cybercrime, especially the capacity to report or collect complaints. We know there have been more complaints, but there may be a temporary distortion if complaints are collected with a longer delay than usual or even different levels of dark figures. It is a possibility that crimes with a small impact and, therefore often not reported, may have grown disproportionately.

Well, in this situation, what should we do, what data should we collect and how? Of course, I am not going to solve this here. We have a conference to begin to do it. But I will say a few words. First, we must mention that there are no statistics on cybercrime at the European level as there are for the other categories of crime which are collected by Eurostat, for which it would be necessary to establish what Marcelo and Stefano were proposing,[2] or a common definition of cybercrime or a common way of identifying that. I believe the first step to be taken is to avoid treating cybercrime as a single category, collecting data on the type of cybercrime collected and entering information on personal characteristics of the victim: age; gender; personal, professional, leisure relationships; and the means used to commit the crime, especially if it was through social network, type of device and so on. Similarly, the information should be recorded using smaller geographical units, rather than collecting data at the country level. And finally, I believe we must take seriously the need to promote transparency and a concrete and common methodology in the collection of data from private organisations dedicated to cybersecurity, which complements our efforts to have a better understanding of the phenomenon of cybercrime and its real dimension, promoting partnerships with official boards.

Also, I want to mention the need for victimisation surveys: it is true that some of the surveys conducted did not find a statistically significant increase of cyber victimisation during the first months of the pandemic; however, we must be cautious when assessing the meaning of these results because respondents were asked about victimisation during the 12 months or the last year before the survey, and not in the pre-Covid and during-the-Covid periods. But we need more victimisation surveys, maybe at the European level.

Thank you very much for your attention. And again, thank you very much to the Council in Europe for this opportunity.

2 See the welcome address of Marcelo Aebi (in this volume).

References

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*, 1-13. https://doi.org/10.1080/14616696.2020.1804973.

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty streets, busy Internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*. https://doi.org/10.1177/10439862211027986.

Miró-Llinares, F. (2021). Crimen, cibercrimen y COVID-19: Desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. *IDP: revista d'Internet, dret i política*, (32). Available at www.raco.cat/index.php/IDP/article/download/373815/473802.

Session 1 – Modernising Crime and Justice Statistics

The International Effort in the Modernisation of Crime Statistics

Michael Levi[*]

Hello, everyone. Well, it is a great pleasure to be here, even if not in person. Well, I was asked to try to address some general background, international efforts at crime measurement reform, and that is what I am going to do. So, if we think about the question, well: *why* should we measure? *What* are we trying to measure? I would put cybercrime in the context of a range of newly criminalised acts: online stalking, xenophobia, ransomware, money laundering, transnational bribery and eco and wildlife crimes. And make the point that every one of these, except maybe fraud, have come for financial online components, and that is quite important to keep that in mind. And when I say ransom, one of the things that we need to think about coming back to Marcelo Aebi's earlier point is that many cybercrimes are partly online and partly offline, and we need to take account of that.

That is also the challenge that is changing in criminality. It is not only with cybercrime that we witness a change from local to global victims and their relationships. Fraud has always had an element of internationalisation. So, this was not just invented with the cyber. But then, there are crimes without specific individual or business victims, crimes with victims in multiple countries – again, fraud happened offline. I can speak about it in multiple countries, but the whole point is this is now a routinised experience. And to come back to a different dimension of the Council of Europe, which is the whole mutual legal assistance process, it was not designed for routine internationalisation. Then there is the politics, the measurement, the non-measurement and the culture of statisticians: at a recent government meeting where we were advising the government, one of the problems about these new methods is that people say: 'Well, we do not really have the time series and we need time series.' Well, of course, you can either measure what is going on around you, as Fernando Miró said, or you can keep to the time series and not measure what you should be measuring. I mean, I did my PhD before computers were invented. So, I am aware of the shift. And what do we measure and what should we choose to measure – I used to have arguments in the 1990s with what was said in crime surveys: why are you not into questions about fraud? And the answer was just that there were not enough fraud victims. We think maybe that was wrong. So, that is one reason we do not have time series that include fraud

* University of Cardiff, UK. Additional material: the author's visual presentation is available at https://rm.coe.int/presentation-michael-levi-reforming-crime-statistics-coe-2020/1680a033b1.

or other cybercrimes. And there are multiple victimisations of the same individuals we normally think of in terms of violence and sex offences. But in fraud, multiple victimisation is very important. And in xenophobia, racism, hate crime. Message: I want to raise the question that fear, including fear of specific forms of cybercrime, is something that is not developed well enough in the crime barometer: measures, frequency of offending, measured recidivism assistance, which we will talk about later on the conference. And one may aim for deconstructing and dismantling crime. We know that for different kinds of offences, there is a difference between the time when a crime happened and the time we became aware of it. And particularly during Covid-19 times, there may be a bigger gap. Now, this, in a sense, is not a problem for annual statistics and for the most part. But some frauds may take years to appear, and we need to think about that now.

So, let us summarise, the reform efforts are going on in the US – they always have to come first. There was a National Academy of Science (NAS) report called *Modernising Crime Statistics* recently, which mainly fought the classical wars against the narrowness of the Uniform Crime Reports which exclude fraud and cybercrime. And that really neglects, even the NAS report neglects cybercrimes and offline fraud; and money laundering – it has almost nothing to say about them. The proposed classification includes a list of behavioural definitions that is meant to evoke the familiar classification schema. And I am just going to summarise this because you can read it at your leisure. But there has been very little follow-up or implementation under the Trump administration. So, what we are left with is still just *personal identity fraud* that is measured every couple of years, covered by the National Victimisation Survey, and which is separate from the general victimisation survey. There are no corporate or government cyber victimisation survey efforts or reforms to official data, apart from some of the consumer sentinel data that one of the agencies – the FTC – produces. The FBI is moving to the national incident reporting. We do not have to worry about the general implications of that for this conference, but it could mean even more confusion. But since the Uniform Crime Reports do not include fraud or cybercrimes, the difference may not matter so much.

Let us turn to non-US reform efforts. I am not going to go through every country because we have national representatives in this conference. In the last published version of *The European Sourcebook*,[1] almost all countries provided data on fraud; but only a few of them could adopt the standard definition. And data shows quite a big range between countries. In Eurostat crime data, cybercrime is largely absent. We are not going to cover the UK in detail because we have a speaker tomorrow who is going to do so. But cybercrime and fraud against individuals and businesses, we in the UK are pretty good at that. They are not yet including frauds and cybercrimes against government. We have data breach surveys by one government department, and, we, at Cardiff, did some work for them on

1 Aebi et al. (2021).

Small and Medium-Sized Enterprises, and UK Finance does a good job with card fraud, which is integrated into our general crime statistics. Now, I had the pleasure of being on the committee that did that.

Australia, they have identity crime and misuse in Australian Institute of Criminology surveys. The Australian Cybersecurity Centre does its own work. The Australian Competition and Consumer Commission (ACCC) does annual scam surveys. They are pretty well developed, and I have just finished a study on fraud, including cyber fraud since the Spanish flu with the Australians.[2] The ICVS, which, well, we will speak about a little bit more in the next session, does have some tags which are very important. And finally, there are private sector surveys. Some of them are really commercial. The idea is to attract people to give them some consulting work by the antivirus firms, but they contain a lot of good data within that range. PWC puts it in its biennial general Economic Crime Survey. So, there is some quite good data, some of it more serious than others. But you really have to look at the methodology. The antivirus firms are the closest to the events and they can tell us. And you can see this afterwards, but the disaggregation data for the ICVS is in theory, quite good, if only we adopted it. It may need to be thought about a little bit more, particularly for cybercrime. And in a lot of these, we will have gaps. I mean, we know from the British data there is a lot of missing data in the reports and acts involving fraud, deception and corruption. There you have some very interesting body of thought through carefully considered understanding to work on. But one of my questions is: who is going to fill this in? And we have to look at the realities of pressures on policing and other organisations to fill in this kind of data.

So finally, some threats and responses. There is a very aggressive threat landscape from cyber and crypto currencies, threats of what, to whom, by whom harms. We have the growing elision between national and human security that we can see. How do we decide whether the threat to a country is big enough for NATO interventions? Is it because our toaster is invaded or our car? Obviously not. But what is the threshold? That is a big issue that I raised in the NATO summit when it was held in Wales. But nobody was interested at the time or seemed interested. There is the issue about how firms and individuals carry out cost–benefit judgments in practice, and the point for the cybercrime data is that it is easier to design in relevant data at the incidence or crime reporting stage than it is afterwards. You know, afterwards, who has got the time to go back and do this?

And a sceptical point about the impact of data breaches: who and how many use Facebook, Equifax, Marriott or British Airways *less now* than they did *before* the revelation of data breaches? We need to think about what the impact of these things are. So finally, I have a picture. The guesstimates of the cost of cybercrimes are controversial, and we have done some interesting work in the UK on this. Why are these things important? Well,

2 Levi and Smith (2021).

because they might lead us to prioritise our responses differently and to know whether things are getting worse or better: sometimes that we are weak in the case of some kinds of cybercrime. But there is the problem of what I call *facts by repetition*, not real facts. But facts just because we see them often in the newspaper and that is a dangerous one. And the Dilbert cartoon that I have there really put that: I did not have any accurate numbers, so I just made this up. Studies have shown accurate numbers are not any more useful than the ones you make up. How many studies that Dilbert makes up?

Are past trends much guide to the future? We do not know; data breaches opportunity factors that were discussed by Fernando Miró. And the final thing, which we will probably know by the end of this conference, at least provisionally, what can the Council of Europe do to assess data collection? It has already done an important thing by getting us together to talk about it, but we shall see. You will be the judges of whether we have done good or done well at the end of it. Thank you very much for listening.

References

Aebi, M.F., Caneppele, S., Harrendorf, S., Hashimoto, Y. Z., Jehle, J.-M., Khan, T.S., Kühn, O., Lewis, C., Molnar, L., Smit, P., & Þórisdóttir, R. (2021). *European Sourcebook of Crime and Criminal Justice Statistics - 2021.* 6th edition. Göttingen University Press. https://doi.org/10.17875/gup2021-1787.

Levi, M., & Smith, R. (2021). *Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19.* Research Report No. 19. Australian Institute of Criminology. Available at www.aic.gov.au/publications/rr/rr19.

The Budapest Convention and the Classification of Cybercrime for Statistical Purposes: Some Observations

Alexander Seger[*]

Thank you for having me today. We have, when it comes to cybercrime statistics, more challenges and questions than solutions. And the presentations so far are pointing in the same direction. We need your guidance. I am heading the Cybercrime Division of the Council of Europe, meaning that I am responsible not only for the Cybercrime Convention Committee of the parties to the *Budapest Convention* but also for capacity building. I am sitting this week in the Cybercrime Programme Office of the Council of Europe in Bucharest, Romania, from where we support global capacity building. We have a budget for projects with a volume of some 40 million Euros to work with over 120 countries around the world.

Nobody seems to have a full understanding of the scale of the cybercrime problem. My presentation will come up with more challenges and issues. And we are looking to you, for the answers to this.

Why, from practitioners' perspective, do we need statistics or data on cybercrime? It is to not only identify threats and trends and for policy decision but also to allocate resources. Why would a cybercrime unit need huge amounts of money and why would a computer forensic unit need more resources? We need to justify that.

A very important point is the legitimacy of criminal justice action. The legitimacy issue is the following (and this is just an example to illustrate this): there was in 2006, the EU Data Retention Directive, which came about after terrorist attacks in London and in Madrid, and thereafter member states of the EU had to report on the implementation of the directive. They also had to provide data on how often data retained by service providers was accessed by law enforcement. For example, in 2008, there were 1.4 million requests for traffic data. There are also many other requests for other types of traffic data. As many as 1.4 million requests in 17 EU member states at that time had transposed the data retention directive. But there was very limited information on the actual use of such data in criminal proceedings. And following controversy around the directive in 2014, confirmed in 2016

* Council of Europe. Additional material: the author's visual presentation is available at https://rm.coe.int/presentation-alexander-seger/1680a0339b.

and confirmed again a few weeks ago into 2020 by the Court of Justice of the EU, the data retention directive was invalidated because the interference with the rights of individuals was not considered proportionate. One of the reasons was that criminal justice authorities could not explain what they did with all the data accessed.

There were some questions this morning, just a while ago by one of you: what is cybercrime? Is it an extension of traditional crime making use of computers and so on, just situations where the computer is the agent? Is that too broad? Or is it only offences against computers? That would then be too narrow.

If you look at the list of offences in the Budapest Convention's Articles 2 to 10, then you find offences against computers, illegal access, data system interference and so on. You find some offences by means of computers, where there it is a qualitative change, computer forgery, fraud, child pornography, IPR offences. And if you look at offences today, most cybercrime consists of a combination of these types of offences that you find in the Budapest Convention.

We know that the substantive criminal law provisions of the Budapest Convention have been implemented so far by about 110 countries around the world. As we have the information on the laws of these countries, we can compare what is available in Argentina with what is available in the UK and Ukraine. And we can give you the data of how this translates into specific offences in criminal codes around the world. So that data is available.

And as I said, Budapest Convention has been with 65 parties, another 12 states that have signed, that have been invited to accede, but at least another 50 countries or 70 countries actually that have used it to define their domestic criminal law.

Let us take one example, the federal German police is annually extracting from its crime statistics a report, a situation report on cybercrime. The last one was published a few weeks ago. They recorded 105,000 cybercrime offences, in a narrow sense in 2019, out of which most of it was computer-related fraud, the interception of data or misuse of devices and so on.

The Covid-19-related cybercrime, because this was also mentioned, is one of the topics of this conference; but cybercrime is phishing, ransomware or critical infrastructure attacks as well as different types of fraud or child abuse, online child abuse, which is also increasing during these times. And even if the Budapest Convention does not talk about botnets, we have guidance notes that show which of the offences is linked to botnets and malware and so on. Hence, we can pick a new type of offence in a way that it matches in many cases with the cyber offences of the Budapest Convention which is almost 20 years old.

We are also asking ourselves whether the international classification of crime for statistical purposes of UNODC can be useful (some of you made already references to that) for the offences of the Budapest Convention, which are also reflected in that framework. To the extent that framework is applied (quite often it is not but to the extent

it is applied), you can also relate it to the Budapest Convention and the information we have about criminalisation of that type of conduct.

Now, there is a problem: the challenge for cybercrime, and that is something that had not been mentioned really this morning: the German criminal police, in its situation report, concludes that there has been a total loss of about 82 million Euros due to the 100,000 cybercrimes that they recorded and registered in their system and that probably they also investigate. However, if you listen to the German Industry Association, they concluded that the damage caused by cybercrimes to German industry amounts to about 100 billion Euros in a year. You see that there is a 'slight' difference, and that is a problem.

Most cybercrimes and most damages caused by cybercrime never enter the criminal justice system. I talked to some people in Germany, and again, this was just a response by some people, people who were supposed to know because they were in high-level positions. They are saying that any major cybercrime against industry, against any sector of the industry, against institutions, is considered as a national security issue and is therefore dealt by constitutional protection service in Germany, for example, and not by the police. So, it does not enter the statistics: that is already a problem. So less than 1% of cybercrime that exists is actually reported to or reported by law enforcement, by criminal justice authorities. It is a very important problem. And I say that because the majority of people in private sector entities think that criminal justice is useless, that criminal justice system cannot offer a response to crime, that there is no follow-up, no remedy; thus, attacks against anything beyond the individual level in many cases are considered a matter of national security. Companies do self-defence, and they fear damage to their reputation on account of cybercrimes: if it affects a bank, in many cases, insurance pays; we all experience that. We do not even have to go to the police anymore if we are defrauded in cyber-ways; insurance pays directly. It is too complicated to even go to the police. And very often the legislation is unclear; when it comes to bullying, for instance, and all sorts of cyber violence. Law enforcement would not know what to do because it is not clear in criminal law beyond the type of offences I mentioned before.

And out of this, less than 1% is reported and recorded by criminal justice authorities, and it seems that less than 1% is actually leading to a criminal justice outcome. So, from 10,000 crimes, you make 1 to 10 convictions. That is a very important problem.

And another important point I want to mention: here we only talk about cybercrime. We are not talking yet here about any offence involving electronic evidence. And this is an issue: the Budapest Convention has substantive criminal layers, covers a number of offences, the ones I mentioned before, but it also covers procedural powers and measures for international cooperation related to any crime where evidence may be on a computer system. And now try to give me one type of crime, where, in principle, there may not be evidence on a computer system yet: even in a rape case, the offender may have groomed

the victim on the Internet, or the location data may prove that the offenders were at the place where the rape was committed and so on.

And this creates a major rule-of-law problem, and it leads to the question of whether governments are able to meet their obligation to protect individuals against crime, like the Court of Human Rights in Strasbourg ruled in 2008 in the case of K.U. versus Finland. And we also have to keep in mind that this may lead to a situation where more and more powers and competences may shift from the criminal justice arena to the national security arena, as we already experienced with terrorism. And that means that the criminal justice's response may become more and more residual. In that sense it is also worrying to look at some court decisions in which national security issues are given a margin of appreciation, but that is not the case when it comes to the criminal justice response. And I would be worried about a recent decision, again, of the EU Court of Justice in Luxembourg, where governments asked: *what shall we do about access to data?* And the Court responded to the question saying that the problem is related to the way the courts decide when access to data is based on national security, and therefore they put some obstacles there, and *de facto*, they are limiting further the powers of criminal justice authorities to access data. That is very worrying.

Again, I mentioned before, the Budapest Convention covers not only cybercrime, but, according to Article 14, evidence on a computer system in relation to any crime. The question is how do we capture that in criminal justice statistics? Any crime may have a cyber element, may have evidence on a computer system.

And another challenge in terms of statistics is that cybercrime often involves a combination of different offences. Cybercrime may be a tool to commit more serious offences, and, therefore, it is not recorded as a cybercrime but as the most serious offence. And then there is the issue of transnational nature of cybercrime, that is, what you really count and how you count it if offenders, victims, computers and so on all over the world. There was a recent case earlier this month the Trickbot 'Take Down' ('Take Down' in Inverted commas, because it was only partially taken down and then moved to other servers), which involved different offences, that is, data system interference, misuse of devices, forgery, fraud, extortion, election interference, IPR infringements and many more. You had victims in many, many countries, offences, offenders, victims and systems in many countries around the world. Something like 2.7 million computers were infected with this Trickbot through at least 128 servers all over the world. How do you reflect that in statistics? It is complicated.

Some more challenges: everybody says, 'yes, we need better data. We need statistics.' But very few countries have them. And very few countries have domestic regulations requiring keeping of statistics. And while in a number of countries there are statistics, there is no common approach and they are not comparable internationally.

And private sector sources that may provide data on cyber security, cybercrime to computer emergency response teams that have incidents data, you can have statistics extracted from databases like crime databases, like the UNCCS report I mentioned a short while ago, different reporting platforms specific for specific forms of cybercrime like PHAROS in France, action fraud and what was called ACORN in Australia, and the famous Internet Crime Complaint Centre (IC3) in the USA and so on. But there is no experience of integrated systems from the crime reported, investigated, prosecuted and adjudicated. In the EU, a few years ago, evaluations were carried out in the criminal justice area. And all of the evaluation reports recommended keeping statistics, having more reliable reporting on cybercrime. But there has been no documentation for the follow-up given to that.

We try to use capacity-building programmes to support reporting systems and statistics. The largest project is called *Global Action on Cybercrime Extended* and supports regions outside Europe. We just published today in cooperation with Interpol a *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence*, which is promoting a more strategic approach to this. The link was shared with you this morning.[1] Hopefully that will lead to better statistics, better assistance to collect data and statistics.

In conclusion, we need clear guidance from you on how to go about it.

1 www.interpol.int/content/download/15731/file/Guide%20for%20Criminal%20Justice%20Statistics%20on%20Cybercrime%20and%20Electronic%20Evidence.pdf.

Cybercrime Data in Estonia: Surveys and Statistics

Andri Ahven and Mari-Liis Sööt[*]

Mari-Liis Sööt

My name is Mari-Liis Sööt, from Estonia and working for the Ministry of Justice. Me and my colleague Andri Ahven will explain to you a little bit in detail how we collect criminal statistics about cybercrime; but first of all, I would like to thank all the organisers of this conference for bringing up this very important and interesting topic. I would also like to thank previous speakers, Fernando Miró, Michael Levi and Alexander Seger for their very interesting presentations and the issues that they raised, which are the same issues that we are facing.

The aim of the discussion is actually to find ways to better grasp the extent of cybercrime in Europe and in our country. I think it is needless to say that cybercrime, the extent of cybercrime, can only come in conjunction with the data collected officially, namely official statistics and data collected through other sources such as victimisation surveys, but also big data, which, of course, contains data misuse threats and therefore must be accompanied by strong data protection requirements. However, I think this has been forgotten by many states.

What I also wanted to stress is that the usual distinction between *cyber-enabled* and *cyber-dependent crimes* does not actually often help in everyday data analysis of cybercrime. This is because the offence can fall into both categories. The borderline between them is really blurred. The hacking into computer systems in order to steal someone's money is an example of such case, which could fall on both categories.

So, before we look into our official statistics, let me say something from the surveys' side (Table 1): in Estonia we asked people about their personal experiences, about the offences they have probably faced. And according to the annual victimisation survey, we get to know that 30 to 40% of the respondents were victims of various forms of phishing. For example, they have been threatened of closing their email or social media accounts, they have been threatened with encryption of files and so on.

---

* Estonian Ministry of Justice. Additional material: the author's visual presentation is available here: https://create.piktochart.com/output/50198798-cybercrime-stat.

Table 1 Exposure of people to computer data and system crime according to the survey data (2019). *Question: Has there been /… / on the Internet in the last year (asked by those who use the Internet at least once a week)?*

You have been notified of a lottery win or inheritance for which data has been requested	30%
You have been offered to participate in a profitable business and asked for data by a stranger	20%
You have been warned about closing your email or social media account and asked to click on an attached link	15%
You have been asked for money by a stranger to help their acquaintance in trouble abroad	12%
You have been threatened with encryption of files if you do not pay the required amount of money	7%

We also ask about cyberbullying: 15% of 9- to 17-year-old children say that they have been victims of cyberbullying. From another survey, we get to know that 45% of youngsters have fallen victims to sexual harassment and so on. So, this is one source of statistics or information that we get to know about the cybercrime and the extent of this.

Then we collect data about Computer Emergency Response Team [CERT] incidents. As you probably know, the CERT organisation exists worldwide, and they cooperate closely. This is one source of data where we could get internationally comparable statistics. I also decided to show you the survey results to stress that these kinds of surveys actually allow for international comparisons pretty well, once everyone agrees on the methodology.

Now, coming closer to the topic that we are supposed to talk about, let's look at the official statistics and the Budapest Convention, which categorises cybercrime into four offences against computer data and systems. We have better data on these offences domestically in Estonia and we know better what we are measuring and what kinds of provisions we are actually measuring, as compared to computer-related offences, such as fraud, or content-related offences, such as child pornography and copyright. We are less successful in collecting the whole statistics we should have collected, as you can see in Figure 1 and Table 2, and I will show you why. The total number of computer-related crimes in Estonia is a very small; it is 965 computer-related crimes last year and the majority of it contains computer fraud, and then we have a small amount of computer data system crimes, which makes 20% of it. Just for comparison, around 20,000 crimes altogether are registered in Estonia. Just to put it in context.

Figure 1 Computer-related crimes: registered offences – 2009-2019

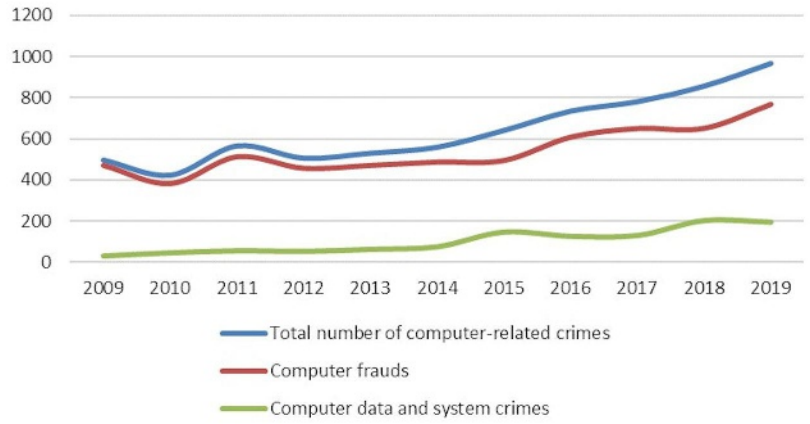


Table 2 Computer-related crimes: registered offences – 2009-2019

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Total number of computer-related crimes	499	426	567	508	532	561	642	735	781	856	965
of which											
Computer frauds	470	381	512	456	470	486	494	608	650	651	768
Computer data and system crimes	29	45	55	52	62	75	148	127	131	205	197

So now I throw out the problem. What is the problem number one in the statistics? You can see it in Table 2: the number of offences included in the statistics refers almost exclusively to computer-related fraud. It is based on the provision of the Penal Code of Estonia, which is precisely computer-related fraud, and therefore it does not contain the offences recorded as other types of frauds, such as the so-called *ordinary fraud, investment fraud, insurance fraud* and so on. Why is this? It is not because they are not committed via electronic means (in fact most of them are), but it is because it demands a lot of manual work to filter them out. Therefore, today we just do not include them in the statistics, which leaves the statistics half-true. We hope tomorrow we will have more automatic analyses that would help us to filter out cases related to a computer in other types of fraud too. This needs the development of various IT systems. And this problem and its solution also affect other offences related to cybercrimes; let it be child pornography or any other. We need IT solutions for that to be investigated, so that later we can access the data from

the databases. And this is something where we can see that the Council of Europe can stress the need for the development of good IT systems for the law enforcement in order to actually acquire the statistics automatically. So, Andri, will you now explain this point of view with two examples?

Andri Ahven

Hello, my name is Andri Ahven. There are a lot of examples, of course, about cybercrimes, but I present here only a few of them. One example is where we use different classifications for very similar offences. First example: ordinary fraud. Another, very similar, is computer-related fraud, which already is a different type of crime according to the Penal Code. And one of the most typical things concerning frauds, and also computer-related frauds, is the unauthorised use of an ID card for digital signing of financial contracts; for example, to take quick loans, to arrange payments by instalments and so on, and also for ordering goods. And it appeared that victims themselves had often given away their ID card to relatives or acquaintances. For example, a daughter got from her mother an ID card, and, in one case, the daughter gave it to her boyfriend who abused it. And also, another example concerning computer-related fraud, where a daughter arranged a loan using her mother's ID card. Very similar cases, but registered as different offences.

Second example: child pornography. According to the relevant section of the Penal Code, in this case we may find both offline offences and online offences. First, for example, if you prepare pornographic material, you are using cameras and you do not need any electronic means; but, additionally, if you storage the pictures or videos you will be using electronic means.We can say that such kind of offences may take place offline and online. Of course, online offending has increased and, as I understand it, it represents a majority of such offences. Downloading pictures and videos from the Internet and uploading pictures or videos are currently quite common offences.

Mari-Liis Sööt

The point that we are trying to make here is that, when a country provides information about computer-related frauds, it might not contain the whole picture of computer-related fraud. This is what has happened in Estonia. And probably we are not the only case in the world.

The second problem is that we still have to put a lot of effort to filter out the cybercrimes with major impact or influence. These include computer data and system-related crimes, like the real computer crimes, which are complex in nature and procedure; these may

cause bigger harm, which includes commitment in groups and so on. In reality, these represent only a small number in the official statistics, let us say 5% as reported in the previous year in Estonia, while it takes a lot of effort and demands a lot of money from the law enforcement and other resources, too. So, there we have problem number 2.

When we look into the cases of computer data and system crimes, which is a highly influential computer offence, the majority of these offences are actually categorised in Estonia as *digital family violence*. We call it *digital family violence* because it includes mostly changing or capturing the passwords of social media or email accounts of family members. This makes up about half of computer data and system crimes, but it does not give an accurate picture of data and system crimes. So, this is a growing crime. Of course, people report more, yet in terms of investigation it is a small fish and its impact is rather modest on internal security. So, it rather resembles a common or ordinary crime. Nothing sophisticated here, but when we want to filter out the really influential crimes, we have to sort them out manually. They can become more influential if more data are stolen and so on. The most serious and highly influential cybercrimes, for example, are entering a router – or server or a network interference in email trafficking – and sending, for example, a false invoice or something, then phishing congestion or corrupting the system with traffic, and so on.

Before giving the floor again to Andri, who will bring an example to illustrate the point for international comparison, we clearly suggest first taking small bites, namely comparing only what is comparable. Let us take the case of highly influential crimes, namely *offences against computer data and systems*, and let us spread them into small pieces so that we would not have to compare offences against computer and data systems. But the first category in the Budapest Convention pertained to very specific provisions that we can really compare. So, we have to decide whether we would like to have that so-called domestic digital domestic violence included there or not. Our suggestion is to compare very specific offences under this category, not the category itself as a whole. Andri will now give the final words to conclude our presentation. And I thank you very much for listening.

Andri Ahven

A few examples of the crimes Mari-Liis just described. There is an official category, *illegally obtaining access to a computer system*, and if we look at the description of crimes, we may find very different crimes in that category. First, huge crimes which had caused financial losses, and the damage may go up to several millions of Euros. One type is sending fake invoices: I found a case where losses were about 60,000 Euros, and there were several other cases. Also, there have been several cases in which the clients' databases were stolen, and in one of the most serious cases, which is still under investigation, the loss was estimated

to be more than 10 million Euros. It was committed by installing spyware while Bitcoins were bought during several months. Those types of crimes are relatively rare but may cause huge damage.

However, in the same section of the Penal Code, the absolute number of crimes is much higher concerning digital stalking. For example, surveillance of social media often allows finding cases of *unauthorised distribution of personal information and messages*, or *uploading embarrassing pictures and videos*. It happens quite often that the same offender has committed a large number of crimes, and usually each crime is counted separately. That is how the number is constructed. So, I think that we are approaching our time limit, and we are happy to listen to the next presentation. Thank you everybody for your attention.

Cybercrime Statistics in Spain

Francisco Sánchez-Jiménez[*]

Good morning. Firstly, and foremost, I would like to express my great pleasure at being able to be here with you, especially in these hard times that we are living with the Covid-19 pandemic. Therefore, I would like to send a warm message of support to all people who are suffering from this horrible disease. In order to take a broad vision of the Spanish experience, I will answer your questions at the end of my speech. Nevertheless, you have my mail. Please, do not hesitate to contact me.

Let me introduce myself: I am Francisco Sánchez, Chief of Service at the Spanish Ministry of Interior. Currently, I am working in the Cabinet of Coordination and Studies. As you can see, among other functions, my department is in charge of developing, implementing and managing the national crime statistics. Additionally, we are responsible for coordinating different aspects of the cybersecurity through the Cybersecurity Coordination Office and the National Centre for the Protection of Critical Infrastructures. We believe that bringing together different units with statistical and cybercrime-related responsibilities allows an advantage to face the challenges in this field that we may have in the future.

Before starting my exposition, I would like to show you the situation in my country. In Spain, we have detected a significant increase in cybercrimes, which is similar to the cybercrime trends observed in several of our neighbouring countries. In fact, within the first six months of the present year and with special conditions related to the pandemic and the lockdown, we have reached a 15.6% increase in this type of criminality in general. Together with the evident risk for every victim of these crimes, we have to place severe prejudices to the national economy. In my country, 50.8% of the cybercrimes correspond to purchases originating in Spain which have been carried out through e-commerce websites in foreign locations.

Well, we can say that we agree that cybercrime is a serious problem. Furthermore, if we want to implement preventive and active policy measures to tackle this phenomenon, we need to have a real knowledge of the situation. In this sense, if each country has a different methodology, how can we compare our country with another one? Therefore, at the global level, a methodological harmonisation is necessary to be able to really measure

* Spanish Ministry of Interior. Additional material: the author's visual presentation is available here: https://rm.coe.int/presentation-francisco-sanchez-jimenez/1680a0339e.

this problem. With this aim, I am going to tell you the Spanish experience, and which was the procedure that we have carried it out.

On the one hand, there has to be a legal framework to regulate statistics. In Spain, there is a specific law for the collection and production of the official statistics. In the area of the crime statistics, in 2013 The Secretariat of State for Security made an internal regulation on crime statistics. Some key points of this legal text are the following: a working group was made up, in which are represented all the Police Bodies. This group holds an annual meeting, and, inside it, the members decide how to harmonise the methodological rules of the crime statistics. Additionally, internal rules were developed to specify in detail how each criminal act has to be recorded.

On the other hand, this is a key subject, because there should be clear rules, at least at the European level, on how to compute every event of cybercrime. In other words, we should start to work in a similar classification to ICCS but specifically related to cybercrime. Among the issues that should be addressed are the following:

1. *The refinement of a definition for statistical purposes about the term cybercrime*. In Spain, we have statistically considered all the events covered by the Budapest Convention. But it cannot be denied that the definition of criminal offences should be expanded. Perhaps it would be a good example of good practice to establish a specific statistical regulation at the European level with every way of cybercrime: cyberterrorism, online scams, computer attacks, sexual offences, hate crimes and so on.
2. Another important issue is *how we count every event associated with cybercrime*. For example, the location of the event, when the offender who commits the crime lives in another country.
3. A particular concern is related to the *economic valuations of the goods*. For example, in the cases of organised piracy and counterfeiting, we have at least two options: the price of the original good or the real price that the counterfeit product has actually been sold.

These and many other issues must be resolved, in order to have a common measurement instrument and with which we could develop concerted national policies. The advantages of this new way of approaching and resolving this problem seem to be obvious: a better knowledge of the situation can lead us to better knowhow to tackle it. Nevertheless, there are more fields in which we must make an impact from our perspective: the core issue concerns police training. To carry out this task, there should be a deep change in our mind-sets. In my country, we are getting used to set up strategic public/private partnerships, especially with universities. This would bring us knowledge, experience and talent to face this great challenge with success.

All this has to be undertaken by active policies which can drive these developments. Our Secretary of State for Security recently announced the development of a National Plan

on Cybercrime. Our objective is to create operations and digital transformation units that, from an operational point of view, facilitate the adaptation of the response of the Police Bodies to the new technological crimes. Also, we will implement mechanisms and tools of technical coordination with the specialised units of the Police Bodies and the prosecutors, to set up a procedure that allows establish the lines of action in terms of coordination with the police investigations.

We also consider essential to support and promote the work of Europol's European Centre against Cybercrime. It should be necessary to create an innovation laboratory that would help to position Interpol at the forefront of innovation and development; at the same time, we would share not only resources but also projects. Consequently, one of the aspects that needs to be reviewed in our plan will be related to statistics on cybercrime, because only with a better knowledge of things will we be able to deal with these future challenges.

I would like to sum up my speech with the popular African saying, 'Not to know is bad, not to wish to know is worse.' This means that we must go quickly ahead, and we have to work together. Thank you for your attention.

Self-Reported Delinquency Surveys and the Study of Online Offending/Cybercrime

Looking Back and Forward from a Total Survey Error Approach

Lieven J.R. Pauwels[*]

First of all, I would like to thank you for having invited me. This has been a very interesting experience so far, and, from the presentations so far, I can see the necessity of also disposing of additional measures of cybercrime and offline offending. The previous presentations already demonstrated that it is very difficult to get a grip on the phenomenon because of the huge dark number, and this is actually one of the issues that I want to raise.

If we want to increase our understanding of complex phenomena like cybercrime or digital crime in general, I think it is necessary to combine different methods. What I want to do is talk to you about the possibilities and the challenges that await us if we use another methodology, namely *survey methodology*. And I am going to talk about *self-reported delinquency studies*. Now, my personal relationship to this topic is the following: I have been conducting self-report studies for 20 years, and the past 10 years I have been involved in studies of online violent extremism. And so, this is how I got involved in studying also online offending from a theoretical point of view, because it is one thing to know to what extent some phenomenon is happening and is targeting victims, but it is also important to understand why and to understand the mechanisms behind this phenomenon. And this is my personal interest in this field. Self-reported studies are extremely important not only to give you an accurate image of the dark number but also in understanding the core variables, the characteristics of persons and environments which are related to online and offline offending and victimisation. I am going to stress, of course, offending because there will be a separate lecture on victimisation, although there will probably be some overlap.

First of all, my key message is that if we really want to understand and, of course, prevent both cybercrime and on a broader level, online offending and victimisation, it is important that we take an analytical approach. And by this, I mean that it is important to reflect about the underlying mechanisms, the mechanisms underlying the stable predictors of online offending and the stable predictors of who is going to be the victim or offender,

* Director of the Institute of International Research on Criminal Policy, Department of Criminology, Criminal Law and Social Law, Ghent University, Belgium. Additional material: the author's visual presentation is available here: https://rm.coe.int/pauwels-council-europe2020-cybercrime-final/1680a033c8.

statistically speaking. So, besides the technical problems, we also need useful theory, and our understanding of the phenomenon of cybercrime should really be guided by the best 'available evidence', and that is between inverted commas, because knowledge is never perfect; it is an ongoing process. I think new facts and new concepts will definitely steer the evolution of a field, and I think self-reported delinquency studies really can play an important role because much of the things that have been brought up – how shall we define and how shall we measure, operationalise different kinds of cybercrimes – also need to be translated into other methodologies in such a way that we can compare prevalence rates and compare covariates; for example, covariates of online offending are the same as variants of, for example, measures of self-reported delinquency, and the same as the scores of measures of officially known delinquency.

There is actually an increase in research, but I think it still has many challenges. I will try to talk about what I think are the most important methodological challenges today. I am going to try to frame this within the broader framework of self-reported delinquency study from a historical point of view. I am not going to talk in detail about the history, but it is important to understand the history, to be able to show where the actual challenges lie. So, in my view, self-reported delinquency studies are just one important tool of the trade for descriptive and explanatory purposes and also to our standards about theoretical knowledge of the causes of offending. So, I stress one important tool of the trade, because I think triangulation is really, really important here, especially because there is so much that we still do not know about and there are so many measurement issues that remain. Therefore, it is a very legitimate question to ask ourselves today to what extent the methodology of self-reported studies really can be applied successfully to online offending and victimisation. There are some conceptual methodological challenges, and, when we discuss them, we can try to find some solutions together.

For those who are not familiar with surveys for delinquency studies, maybe just in a nutshell, why do scholars use these self-reported questionnaires? This is survey methodology, first of all, for descriptive research, and, *descriptive research* is, I think, one of the important fields which shares a very close connection to what official statistics try to do, to get the grip of the prevalence of a phenomenon. To describe something involves what kinds of offences are being reported, what kinds of offences are prevalent, how things evolve, *modus operandi* and so on. So, 'what kind of' questions are descriptive questions; but besides that, we also have the exploratory research trying to find out who is at risk of becoming an online offender versus – between inverted commas – a 'traditional offender'; how strong is the overlap between offending in the real world versus offending in the, let us say, virtual world? Also, of drawing the connections between offending and victimisation? We know a lot about this, but our empirical knowledge is mainly restricted to traditional kinds of crime. I also have to stress that self-reported delinquency studies historically have

been applied to juvenile delinquency. These are crimes committed by minors, which has changed nowadays, thanks to the evolving field of life-course criminology.

Can we use our established theories to apply to online offending? And from one of the presentations brought to us before, it could already be seen that people use our traditional criminological theories to explain changes in opportunity structure, to understand how the Covid-19 situation may have had an impact on a sudden increase or decrease of different kinds of offences. Hence, self-reports can play a role. When you look at the literature on self-reported delinquency studies applied to online offending in the broadest meaning of the concept, we already can see that most of the traditional theories known in criminology have been applied. And I think this is important because sometimes people have the feeling that new phenomena require new theories. And I do not think that is always necessary. I think the criminological imagination really is about trying to translate existing concepts into an ever-changing world. I mean, dynamic theory is what it is all about. And if I look at the most tested theories on online offending, I think *social learning theory* is one of the most used theories. We also have many studies on self-control theory and routine activity theory, but if you try to count them, the overall majority come from forms of 'social learning theory'. This is probably because of the fact that, when we talk about online offending, we talk about the need *to learn* how to use different systems, to learn technology to apply technology to commit crimes. This is probably one of the explanations of why this social learning approach is so popular and trying to understand individual differences and development and involvement in online offending and cybercrime. But our traditional theories do have some restrictions.

I would like to stress two problems here for self-reported delinquency studies. Humans are more than the sum of variables, so we should not think of just covariates of online offending or cybercrime, but really think about the mechanisms beyond the correlations and many of the variables that appear in different studies on online offending. One problem is that covariates actually belong to different frameworks. Therefore, we really have a lot of work to do from this point of view. Now, people have been using self-reports for many decades, and I am not going to go into detail into the history because there are very interesting books written about the topic. A highly accessible book, which I would recommend, is the book by Janne Kivivuori.

And if I try to make a differentiation between time periods in terms of the use of the self-reported methodology, I can distinguish seven periods:

1. *Exploration and discovery of hidden crime:* crime not known to the police, which corresponds to the 1940s and 1950s.
2. The golden years of *theory testing in the 1960s:* when people started to understand that the methods of self-reported delinquency studies could be used to not only understand how many people are involved in different kinds of crime but also what kind of

characteristics. Social bonds are valued, and norms are also related to individual differences in crime involvement.

3. *The area of nationwide representative studies* since the 1970s.
4. I call the 1980s the *hyper optimistic period*, at least the first part of it. People were very optimistic about the use of self-reported delinquency studies because at that time they were convinced of the fact that all the problems of traditional measures of crime – police statistics, judicial statistics – could be solved by using self-reports.
5. But then comes a period more interesting from a scientific point of view, and that is the recognition of *all kinds of measurement problems*, like *reliability* and *validity*. How reliable are measures of self-reported delinquency, and what about validity problems? Do we really measure what we want to measure? These are the same problems which pertain to the field of the use of police statistics regarding online offending and cybercrime. The same goes for the method of self-reported delinquency studies: there are people who lie, there is a proportion of people who answer in a socially desirable way, there are people who score high on *acquiescence* – this is just saying *yes* to whatever question you ask them – there are problems of memory, recall problems. So, thanks to this critical period, we found some (imperfect) solutions to improve our understanding of measurement problems. This field of inquiry can also be applied to the study of online offending and cybercrime, but I have not seen too many methodological studies. So, this is an important issue for future research on cybercrime, on digital offending.
6. Then starts the *period of the internationalisation*, meaning that researchers start to implement the method of self-reported delinquency studies in different countries with the same questionnaire. And one of the key examples here is the International Self-Reported Delinquency Study, or *ISRD*. Publications are available on three waves, and a fourth wave of this internationally collaborative effort is in preparation, allowing us to see to what extent different mechanisms are at work in different countries. Country comparisons are very important, especially also with regard to online offending and cyber victimisation. I think this is one of the challenges also awaiting the ISRD.
7. We have the last period in the history of self-reported delinquency studies, which I distinguish, and that is the period of *digitalisation*. Traditionally, self-reported delinquency studies were conducted using the paper-and-pencil instruments surveys. If you talk about online victimisation, online delinquency, we should almost immediately think about online measurement instruments. Because of the digitalisation, I think the problem of cybercrime/digital offending should also be studied using online surveys. However, people were very sceptical in the beginning of the 21st century because we were afraid that we would not be able to target every member of the 'population'. For example, not everyone who has become a victim of cybercrime or who commits these cybercrimes is always online. However, I am not going to say I am overly pessimistic

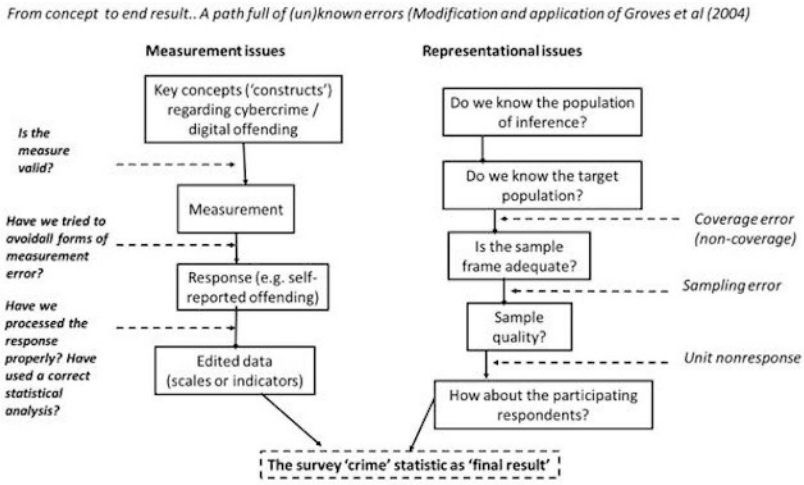
> or too optimistic. I am rather in between – that is to say that I am realistic – because it seems that many of the traditional findings are being replicated using online surveys. This is a very important thing; it is good news. The bad news is that we might need to refine concepts and measures, but speaking as a methodologist, this might be not too bad because we learn by improving measures. [*Joking:*] And trying to solve methodological problems is a way of making a living … for methodologists like me [*Audience laughs*]. I just meant that a joke.

In short, I think the digital area really has a lot to offer, from a criminological point of view, to understand this phenomenon. Self-reported studies are now an established method with many advantages, but there are also many disadvantages – not different from any other method.

If I look at the empirical tests of theories or the descriptive studies on online offending in general, I can see that the international awareness of the necessity to study online offending is not new. Some scholars were already writing about online offending in the 1990s. A few researchers were already recognising the problem of lack of data on perpetrators. For example, one of the first PhD studies on online offending was done by Rogers in 2001; there is also the study of Skinner and Fream in 1997. So, these were the very first published studies, and, if you look at them, you see that they reflect the kinds of online offences which were actually the problem of the day. The number of publications using self-reported methodology has not only increased but has increased exponentially, especially since 2007, when *social media* became rather popular among juveniles and adolescents. We now have much more studies to say something about the possibilities and the challenges of using different methods to study online offending and cybercrime.

Many of the criticisms which pertain to the classical offline studies also pertain to the domain of online studies. And, to explain what I mean, I always start from what I call a *total survey error approach*. I think our understanding of cybercrime and online offending in general can benefit a lot if we incorporate this total survey error approach, which is the famous approach in sociological methodological literature; it is about trying to understand the error, which means that we never can measure anything perfectly. Survey measurement error refers to error in survey response arising from (1) the method of data collection, (2) the respondent or (3) the questionnaire.

Figure 1 Total Survey Error components linked to steps in the measurement and representational inference process (Adapted from Groves and Lyberg, 2010)



When conducting research, we obtain results, but our results are affected by a combination of reliability problems and systematic errors. You can see that in Figure 1, which was borrowed from Groves and Lyberg (2010). When we apply this framework to the phenomenon of digital crime, this means we experience problems arising from the methods of data collection, problems related to the respondent not being honest and problems related to the questionnaire. Take the questionnaire: how are we going to measure online offending? On the left you see the measurement problems, which is a very good guideline to develop new instruments. We start from our definitional issues which have been discussed. What kind of crime do we want to study to understand to what extent it is prevalent in the population? We start by clearly describing our phenomenon. These are the *conceptual issues* from the conceptual definition. Next, we move to the *measurement instrument*. The questionnaire item for which we have a response of the respondent, and this means that the respondent also needs to understand the question. The results of the survey and their statistical analyses are always affected by all these problems. We need, especially in the field of online offending, much more methodological studies to know to what extent the respondents really interpret the questions in the way the researcher meant the questions to be understood. It has been done in the field of traditional crimes, and it should be done much more and on a larger scale.

Also, equally important to the field of cybercrime and visible to the right of the figure, we see problems regarding the representation, and, by representation, I mean who are we talking about, or referring to, in a study of online offending? What is the population of

inference? Who becomes the victim? Who becomes the perpetrator? We have our theoretical population of inference. We have our target population because we cannot question everybody. We have problems of coverage. We restrict our methodology often to the study of juveniles, young adolescents, young adults. I think adults are really important, not only as victims, but also as offenders, as can be seen from life-course criminology studies, but incorporating them goes with some significant challenges. For example, are adults less willing to report crimes than juveniles? They have more to lose. Thus, there are really huge issues regarding the sample frames in studies of online offending. That is why I think self-reported methodology can probably teach us more regarding offending on the covariation between theoretical concepts and self-reported online offending than on the 'real prevalence of online offending'. If I look at surveys in general, I observe a decrease in the willingness to participate in surveys. This also affects our studies of digital crime and online offending. The framework that I presented – the total survey error approach – can be used to improve our existing studies and existing measures of online offending.

If I look at conceptualisations from the first self-reported delinquency study to the studies reported or published a couple of months ago, most studies still deal with 'traditional' items of digital crime and online offending, from trying to steal passwords, deleting files from ones computer, to online threatening. Fewer studies deal with online hate crime radicalisation, which I think is also an important issue nowadays, and it is possible to study this phenomenon to a certain extent. We should really try to move on. Traditional self-reported studies need to move on to include political kinds of juvenile delinquency and more serious offences. The problem of triviality, which was the difficult problem of early self-reports, also applies to the phenomenon of measuring online offending.

From my point of view, we have the following challenges: violent extremism, hate crimes, sexting, child pornography and also the issue of measuring online exposure. These are really tough problems, which should be tested before we can go on and test our theories. We also need to go beyond the traditional measures of self-reported delinquency scales because most studies use standard scales, meaning a number of items referring to, for example, hacking or digital piracy. And they refer to acts which are being committed in the past 12 months or the past 6 months. This is not so interesting from a theoretical point of view, because you refer to a period in the past, and, thus, cause and effects are reversed in cross-sectional survey. There may be some alternative ways of using self-report instruments to understand digital crime. And this is the randomised scenario study – also called randomised factorial design – which can be applied online as well. The method has been applied recently and in many studies on violence where you can actually randomise the situational attractors and you measure the individual characteristics, so you can understand who is tempted, who is provoked and who will probably perceive online crime

as an action alternative and choose that action in response to provocations and temptations. This is, presumably, something that should be tested more. I have seen some examples, but we need more research to be able to know to what extent we can apply this methodology to the different kinds of cybercrime. Also to the types of cybercrime committed by adults.

I also said that measuring exposure is important. Exposure is related to the opportunity structure. People – not only just juveniles – spend many hours online, but spending time online is not necessarily a good indicator of being at risk. It is about being exposed to what we call in criminological theories, *criminogenic settings*. Settings which may invite people to commit crimes. You can translate this traditional concept from criminological theory to the digital world. It is a hypothesis that, when people are exposed to certain contexts online, for example, if they have some risky routine activity that they expose themselves to becoming a victim or may be, for example, being targeted in the field of violent extremism, I mean facing the risk of being recruited online. There are plenty of examples, like people harassed in chatrooms. So, we really need to find out better ways to measure exposure to criminogenic settings. And I think that one way to do this is to invent questionnaires where people are asked what they are doing online, not just how many hours they are studying online, but what they are doing. What kind of websites they are visiting, what kind of chat boxes they are using, with whom they are spending their time online, what kind of social network sites they use and so on.

You can also try to measure the level of online monitoring and the level of law enforcement online to see to what extent this can prevent victimisation and offending. This has been done in the field of traditional theories and traditional crime. Perhaps this can be done to understand why people are exposed to a higher degree regarding online offending: what is the effect of being exposed to explicit content on violent extremism? We know that people are exposed, and in one study that we conducted a couple of years ago – in the context of the discussion about the Sharia law in Belgium – we found that 10% of young adults at least reported to have been contacted by extremists in chatterboxes. This may be an underestimation. I do not know, but the fact is that this study showed that online offending and online routine activities can be studied. This should be an invitation to try to improve what we, and many other scholars, have done. Of course, there remain controversial topics regarding cause and effect, but this is the same traditional criminology, so we need to stay focused on new kinds of exposures to criminogenic settings. There is a huge difference between active and passive exposure, and in the use of social media in regard to cybercrime as well. Can measures of online exposure be improved? I think you need to make a distinction between active and passive exposure. We also need to take into account cumulative exposure.

We need to think about our target population; just like in general self-reported delinquency studies, too many studies target what we call WEIRD people: *Western Educated Intelligent Rich Democratic*, a term coined by cultural evolutionist Joseph Henrich. An

example is the typical undergraduate or graduate student. Not only focusing on WEIRD people is a challenge. And we also need personal data, and this is nowadays, I think, a very huge challenge because of the GDPR (General Data Protection Regulation). It is not just a matter of time; I think it is a matter of resources and a matter of how to deal with privacy issues. Of course, if you want to study people's development through time, panel data usually work very well, but if you want to translate it to the online context, very different methodological questions arise, and some of them are related to the GDPR.

I have said a lot in a short time. Hence a short conclusion: as my colleagues said before, *definitional issues need to be clarified*. That goes for self-reported delinquency studies as well. We need much more descriptive research before we can actually adequately test our theories on online offending. We need better measures of online involvement, of online exposure, and we need to combine these with relevant personal and environmental characteristics, like traits and (online) experience. We need to think about the merging of sources. Now, for example, somebody said *big data*. I think big data are really challenging. Are big data going to be 'the future'? Not exclusively, but they will over time become one of the elements which will be used a lot more. And they have a lot to offer. In the context of theory testing, we can combine information derived from big data and surveys. Can we combine survey data with other measures, can we go beyond traditional self-support delinquency items, for example, the scenario study and can we apply game theory applications to the study of online offending? These are methodological issues, but let us not forget to reflect on the meaning of our findings when we find correlations: where do we have a plausible mechanism? We do not have to test theories just to test them, but to understand what is going on. That is the key to a better prevention.

So, my final message would be: stop the endless testing of seemingly competing theories – which was a typical problem of old self-report studies – because we live in the age of integration, at least I think so. Hence, I would like to say: 'one plus one, equals three, not two', meaning that by integrating our ideas we have a lot more to gain than to lose. Thank you very much for your attention, and I hope this presentation was not too technical. Thank you very much.

References

Groves, R. M., & Lyberg, L. (2010). Total survey error: Past, present, and future. *Public opinion quarterly*, *74*(5), 849-879. https://doi.org/10.1093/poq/nfq065.

Groves, R. M., Presser, S., & Dipko, S. (2004). The role of topic interest in survey participation decisions. *Public Opinion Quarterly*, *68*(1), 2-31.

Rogers, M. K. (2001). A *social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study*. Doctoral Thesis, University of Manitoba. Available at www.cerias.purdue.edu/assets/pdf/bibtex_archive/rogers_01.pdf.

Skinner, W. F., & Fream, A. M. (1997). A Social Learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency*, *34*(4), 495–518. https://doi.org/10.1177/0022427897034004005.

Bibliography

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior, 108*. https://doi.org/10.1016/j.chb.2020.106310.

De Kimpe, L., Walrave, M., Snaphaan, T., Pauwels, L., Hardyns, W., & Ponnet, K. (2021). Research Note: An Investigation of Cybercrime Victims' Reporting Behavior, *European Journal of Crime, Criminal Law and Criminal Justice*, *29*(1), 66-78. doi: https://doi.org/10.1163/15718174-bja10019.

Diamond, B., & Bachmann, M. (2015). Out of the beta phase: Obstacles, challenges, and promising paths in the study of cybercriminology. *International Journal of Cyber Criminology, 9*(1), 24-34. Available at www.cybercrimejournal.com/Diamond&Bachmann2015vol9issue1.pdf.

Enzmann, D., Kivivuori, J., Marshall, I. H., Steketee, M., Hough, M., & Killias, M. (2018). *A global perspective on young people as offenders and victims (first results from the ISRD3 study)*. Springer.

Flores, W. R., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security, 22*(4) 393-406. https://doi.org/10.1108/IMCS-11-2013-0083.

Gunter, W. D. (2008). Piracy on the high speeds: A test of social learning theory on digital piracy among college students. *International Journal of Criminal Justice Sciences*, *3*(1), 54. Available at www.sascv.org/ijcjs/gunterijcjsjan2008.pdf.

Hardy, W., Krawczyk, M., & Tyrowicz, J. (2013). *Why is online piracy ethically different from theft? A vignette experiment*. Université de Varsovie, Faculté des sciences économiques, Working Paper, 24. Available at www.wne.uw.edu.pl/inf/wyd/WP/WNE_WP109.pdf.

Hawdon, J., Bernatzky, C., & Costello, M. (2019). Cyber-routines, political attitudes, and exposure to violence-advocating online extremism. *Social Forces*, *98*(1), 329-354. https://doi.org/10.1093/sf/soy115.

Higgins, G. E. (2007). Digital piracy, self-control theory, and rational choice: An examination of the role of value. *International Journal of Cyber Criminology*, *1*(1), 33-55. Available at www.cybercrimejournal.com/georgeijcc.pdf.

Holt, T. J. (2010). *Crime on-line: Correlates, causes, and context*. Carolina Academic Press.

Kivivuori, J. (2015). *Discovery of hidden crime: Self-report delinquency surveys in criminal policy context.* Oxford University Press.

Lee, J., Onifade, E., Ryu, J., Rasul, A., & Maynard, Q. R. (2014). Online activity, alcohol use, and internet delinquency among Korean youth: A multilevel approach. *Journal of Ethnicity in Criminal Justice*, *12*(4), 247-263. https://doi.org/10.1080/15377938.2014.894486.

Louderback, E. R., & Antonaccio, O. (2020). New applications of self-control theory to computer-focused cyber deviance and victimization: A comparison of cognitive and behavioral measures of self-control and test of peer cyber deviance and gender as moderators. *Crime & Delinquency*, 0011128720906116. https://doi.org/10.1177/0011128720906116.

Marshall, I. H., & Steketee, M. (2019). What may be learned about crime in Europe (and beyond) from international surveys of youth: Results from the international self-report delinquency study (ISRD3). *European Journal on Criminal Policy and Research*, *25*(3), 219-223. https://doi.org/10.1007/s10610-019-09425-3.

Morris, R. G., & Higgins, G. E. (2009). Neutralizing potential and self-reported digital piracy: A multitheoretical exploration among college undergraduates. *Criminal Justice Review*, *34*(2), 173-195. https://doi.org/10.1177/0734016808325034.

Morris, R. G., & Higgins, G. E. (2010). Criminological theory in the digital age: The case of social learning theory and digital piracy. *Journal of Criminal Justice*, *38*(4), 470-480.

Pauwels, L., & Schils, N. (2016). Differential online exposure to extremist content and political violence: Testing the relative strength of social learning and competing perspectives. *Terrorism and Political Violence*, *28*(1), 1-29. https://doi.org/10.1080/09546553.2013.876414.

Pauwels, L. J., & Hardyns, W. (2018). Endorsement for extremism, exposure to extremism via social media and self-reported political/religious aggression. *International Journal of Developmental Science*, *12*(1-2), 51-69. https://eric.ed.gov/?id=EJ1190780.

Rokven, J. J., Weijters, G., Beerthuizen, M. G., & van der Laan, A. M. (2018). Juvenile delinquency in the virtual world: Similarities and differences between cyber-enabled, cyber-dependent and offline delinquents in the Netherlands. *International Journal of Cyber Criminology*, *12*(1), 27-46. Available at www.cybercrimejournal.com/RokvenetalVol12Issue1IJCC2018.pdf.

Smallridge, J. L., & Roberts, J. R. (2013). Crime specific neutralizations: An empirical examination of four types of digital piracy. *International Journal of Cyber Criminology*, *7*(2). Available at www.cybercrimejournal.com/smallridgerobertsijcc2013vol7issue2.pdf.

Staksrud, E. (2009). Problematic conduct: Juvenile delinquency on the Internet. In S. Livingstone & L. Haddon (Eds.), *Kids online: Opportunities and risks for children* (pp. 147-159). The Policy Press.

Session 2 – Modernising Victimisation Survey

Introduction

Stefano Caneppele

Welcome back! My name is Stefano Caneppele. I am a professor of criminology at the University of Lausanne, and I am part of the committee of experts that organised this conference, together with Marcelo Aebi, Michael Levi and Fernando Miró-Llinares. The goal of the conference is to put together different dimensions of the issue of measuring cybercrime.

Yesterday, we discussed about the modernisation of crime and justice statistics. And the goal of the meeting this morning is to share opinions and views on the issue of modernising victimisation surveys. We have seen yesterday that crime and criminal justice statistics at the moment are not able to grasp all the different varieties of cybercrime. And some of the criminologists and criminal justice experts who intervened suggested that victimisation surveys may contribute to improve the way in which cybercrime is measured. And this is the reason why we dedicate this session to a discussion on how we can modernise victimisation surveys. We will start with Professor Marianne Junger from the University of Twente. Marianne wrote a very nice and interesting article on the state-of-the-art in cybercrime surveys. Today, she will be presenting a research on the validity of the questions used in victimisation surveys that we found particularly appropriate to open this session. We will then have three national experiences from Finland, Netherlands and England, and we will conclude with a wrap-up discussion of the inputs received from these presentations.

Crime Victimisation Surveys Measuring Cybercrime

Marianne Junger[*] *and Pieter Hartel*[**]

Thank you very much, Professor Caneppele. I am very happy to be able to present some of our work. I just would like to emphasise that, for this project, Pieter Hartel and I collaborated with Rick Verkade, who now works at the Security and Privacy Department in the province of Overijssel (the Netherlands). Also, if you prefer to ask questions in French, I am quite happy to answer you in French.

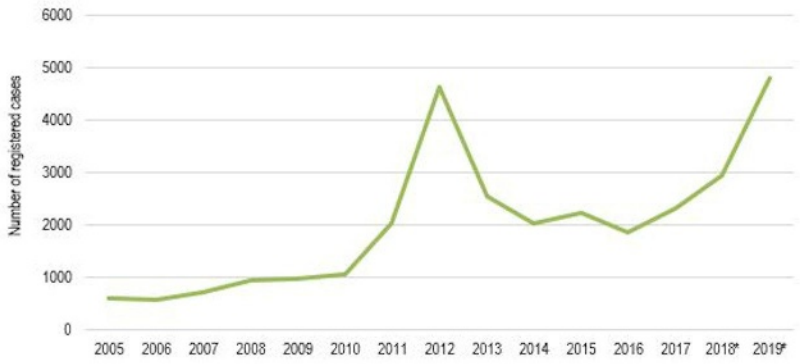
The aim of this presentation is to discuss two methods of measuring 'cybercrime': the officially registered reports from the police and the victim surveys.

Registered Police Reports

First, I will present some data on registered online crime. Let's start with some concepts. As a whole, cybercrime has been described as a vague concept and, to be even more specific, cybercrimes are often difficult to describe. In the Netherlands, we use the legal concept of 'computer intrusions'. 'Computer intrusions', as defined by the Dutch Penal Code, are 'an intentional and unlawful intrusion into an automated work or part of it,' which, I believe is a sort of restrictive definition of cybercrime, made by the Dutch law. You can see in Figure 1 that there is a gradual increase in computer intrusions with a bit of an odd peak in 2012. But overall, the figures are relatively on the lower side and suggest a low level of cybercrime, as measured by computer intrusions registered by the Dutch police.

* University of Twente, Netherlands.
** University of Twente, Delft University of Technology, Singapore University of Technology and Design. Additional material: the author's visual presentation is available at https://rm.coe.int/presentation-marianne-junger/1680a033ae.

Figure 1 Number of officially registered reports of computer intrusions (yearly counts) in the Netherlands



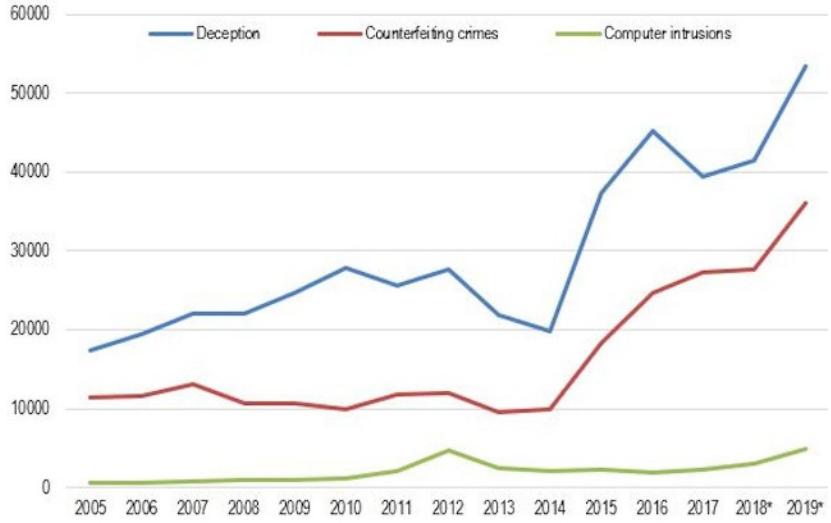
Sources: 2005-2014 CBS statline, 2015 Nationale Politie BVH Stuurkubus. Combined with: https://opendata-cbs-nl.ezproxy2.utwente.nl/statline/#/CBS/nl/dataset/83648NED/table?ts=1603353000816; Hesseling, R. (2016). Wat weten we niet? Paper presented at the Seminar Veiliger in Nederland? Feiten, trends en verklaringen, Den Haag, Nl.

Next, I would like to compare the figures on computer intrusions with the police reports on fraud. In contrast with the general *decrease* in offline crime, which has been established in many countries (Brown, 2015; Farrell, 2013; Miró-Llinares & Moneva, 2019; Pease & Ignatans, 2016), there is a steep *increase* in fraud in many countries. For instance, figures of fraud in the Netherlands, in 2017, show that 'deception' increased by a factor of 2.3 since 2005; 'forgery', by 2.4; 'extortion', 1.8; and 'computer intrusions' 3.9 (Statistics Netherlands, 2018 #15885; Statistics Netherlands, 2018 #15884). Globally, fraud statistics show an alarming increase with newly reached heights in the US (Finklea, 2014; Javelin, 2017), the UK (Financial Fraud Action, 2017), Spain (Kemp et al., 2020) and Australia (Australian Competition and Consumer Commission [ACCC], 2020).

For illustration, the Dutch statistics are presented in Figure 2. The high numbers of the two fraud categories, deception and counterfeiting, stand in contrast with the decline in offline crime, as mentioned previously, and are a lot higher in comparison with computer intrusions which are presented with a green line.

Figure 2 suggests that a lot of cybercrimes, in many countries, might be 'hidden' in the legal categories of fraud and perhaps other crimes as well. We found support for this idea in previous studies. In 2012 already, we found, in a random sample of threats and fraud within police registered reports, that 16% of all threats and 40% of all frauds were 'ICT-related', meaning that somewhere in the process, ICT was used to commit the threat or fraud (Montoya et al., 2013).

Figure 2 Registered crime, fraud and cybercrime



Source: Statistics Netherlands (https://opendata-cbs-nl.ezproxy2.utwente.nl/statline/#/CBS/nl/dataset/83648NED/table?ts=1603353000816).

And, similarly to the registered police data, there is an ICT aspect hidden in court cases as well. Sessink (2018) analysed court cases using machine learning. This is noteworthy, as it also says something about the difficulty in, let us say, distilling the ICT aspect from court cases. She found several relevant ICT aspects in these court cases, 'hidden' in the traditional categories of child pornography; identity fraud; phishing; platform crime, which is website fraud; and threats. Accordingly, she was able to classify part of the court cases within new, online crime versions of these crimes. She reported that the number of online crimes increased gradually, starting with very low numbers in 2003 that grow gradually until 2017 (Sessink, 2018). So, here again, we see that the ICT aspect is hidden within the legal categories of offline crime.

Victimisation Surveys

I would like to continue with a brief discussion on crime victimisation surveys, focus on how to define cybercrime and then explain the findings of a study that we executed, using and evaluating the questions of the Dutch National Crime Victimisation Survey that is run every year by Statistics Netherlands.

Advantages of Victim Surveys

It is important to note that victimisation surveys have been described as the most appropriate mode of measuring crime by the National Academy of Science (2018; see also Aebi et al., 2002; Cantor & Lynch, 2000; Gottfredson, 1986). Victim surveys have a number of advantages:

- Victimisation data are independent from police statistics;
- They can be applied to representative samples, which means that they can provide national figures on the prevalence and incidence of victimisation;
- They led to new classifications of crime, for instance, stranger-to-stranger crime;
- They were instrumental in theory development – think about *routine activity theory*;
- They are, of course, very useful if one needs to make international comparisons.

As mentioned above, it proves quite difficult to operationalise the concept of cybercrime. And one of the main reasons, among others, is that cybercrime is often a more complex crime than others, and it often has a longer crime script. From the point of view of the victim, it is sometimes almost invisible, or what the victim sees is an outcome of a much longer series of steps to defraud him or her. I would like to present a brief visualisation of the crime script of phishing from a Microsoft report (Microsoft, 2020):

1. The attacker must set up a criminal infrastructure, a website that 'feels good', that has the look of a banking website or whatever website he or she wants to imitate;
2. The attacker needs to send email messages to potential victims. To that end, the attacker needs a list with email addresses. He could ask a spammer. He could also approach a website administrator who already has lists of email addresses and who can send the phishing emails to potential victims. Of course, the attacker could also buy a phishing kit online. That phishing kit will install a number of functions for the attacker;
3. When victims fill out their personal identifiable information (PII) on the phishing website, the attacker needs to download that information;
4. Then he has to figure out how to use the collected PII. To actually steal money from, for example, a bank account, one often needs some additional technical knowledge about, for instance, the procedures and the security system of the specific bank. In practice, many phishers will sell the collected PII to people who will know how to use it.
5. Finally, the crucial step is to cash out, that is, collecting the money that is stolen. Usually, the money is transferred to the account of money mules who are paid to collect the money physically from ATMs. If you somehow receive money in a cryptocurrency, in the end you probably want to exchange it into dollars or Euros. Basically, in the end, the cashing-out system is the bottleneck in the entire system (Florencio & Herley, 2012).

The important conclusion here, is that we, the researchers, have to realise that many of these online crimes are more complex than offline crimes used to be, and it is hard to ask questions to victims who are situated at the end of this series of steps, of this 'crime chain' about 'what happened'.

The question becomes: what can victims know, what can they realistically report and what can you ask them? And if the money is gone from their bank account, how can they understand what actually happened, where did their personal identifiable information come from and how did their money disappear? Was the PII bought on the Dark Web? Did they fill out their PII in a return email or on the phishing website or did something else happen?

Comparison of Quantitative and Qualitative Findings

The study I would like to present is set up as a test of the questions that the Statistics Netherlands asks every year about cybercrime to a select sample of the Dutch population. Statistics Netherlands generally measures cybercrime with four questions, '*Were you a victim of cybercrime: bullying, online shopping fraud, hacking and identity fraud?*' Data were collected through a questionnaire that was brought in person to respondents. We first asked the four questions from Statistics Netherlands. When people answered positively to one of these four questions, we asked what happened and invited them to describe the incident in their own words. In brief, we compared the quantitative data based on the questions of Statistics Netherlands with the qualitative data that were collected as a second step.

We collected data from a convenience sample of 225 respondents in several cities in the Netherlands. There were 117 men and 108 women; their age ranged from 18 to 70 years. The results presented below compare the quantitative findings with the qualitative description of each incident.

When comparing the data from both parts of the survey it appeared that the findings were quite comparable for cyberbullying and threats and for online shopping fraud: when these incidents were described in respondents' own words, the descriptions of online harassment matched what was described as 'online harassment' in the question of Statistics Netherlands, and for online shopping fraud, similarly, the qualitative data showed that the question of Statistics Netherlands was clear to the respondents.

However, for identity fraud and hacking, this was not the case. To be able to judge the findings, it is necessary to have a notion of what Statistics Netherlands defined as *identity fraud* and *hacking* (Statistics Netherlands, 2017). The following questions are used:

> *Identity fraud* is when someone's personal data are used without permission for financial gain to withdraw or transfer money, to take out loans or to request official documents. Perpetrators may have obtained personal data in various ways, for instance, by intercepting mail, copying bank card data at an ATM or via the Internet. That is identity fraud.
>
> *Hacking in the past 12 months*: Has it ever happened to you that someone has maliciously broken into or hacked a computer email account, website or profile site like Facebook or Twitter belonging to yourself or someone else in your household?

The first thing to note is that the explanations are rather long and a bit complex.

I want to present the answers of the descriptions of the incidents when respondents had answered positively on the questions on hacking and identity fraud of Statistics Netherlands. I will start with identity fraud.

Identity Fraud

When answering the Statistics Netherlands' question on identity fraud, people described incidents which we believe have a more precise description or consist of something else.

Phishing. Among the 14 respondents who said they were the victim of identity fraud, in 6 cases, the qualitative data suggest that the best categorisation is in fact 'phishing'. In all cases, the incidents are mainly emails trying to get some PII from the respondents. To give you an example, this is what two victims described.

Victim 1: '*Received an e-mail that someone from abroad tried to enter Gmail account. Password changed and nothing else to worry about.'*

This incident did not refer to a '*financial gain to withdraw or transfer money*', or *'to take out loans or to request official documents*', as mentioned in the question of Statistics Netherlands. This person received an email, and the question is: was this a real email from Google or was this a fake email from Google? Probably this was a fake email from Google. So basically, this was an attempt to phish someone.

Victim 2: *'Respondent is regularly called about completing a survey, through these telephone calls advertising is again offered and said that the lady has won everything. Respondent says she never completed this survey.'* As this respondent says she never completed the survey, this is basically an attempt to get information on her bank account.

In other incidents, respondents described the following:

- An attempt to contact someone about a gaming account.
- Filling out bank account information by the partner of the respondent.

- A mother who received a letter that an account (without specification of the type of account) had been made in her name.
- An email inviting the user to login on the bank account.

The main reason for classifying these incidents as phishing is that there were attempts to abuse PII, but nothing happened in the end, whereas the question of Statistics Netherlands focusses on the 'use' of PII. Possibly, victims do not think of 'fraud' when no money disappeared.

Identity fraud. In three cases, the incidents were, in our perception, indeed 'identity fraud', namely that PII was used by an attacker. Twice there was an attempt to steal money when the respondents accessed a website.

Skimming. In three cases, the qualitative description matched most closely to skimming: money disappeared from bank accounts, in the Netherlands or abroad. In these three cases, money was lost.

Bullying. In one case, the incident concerned bullying and consisted of racist remarks.

Unknown. In one case we were unable to categorise the incident, as this concerned with something 'difficult' and the respondent did not want to talk about it.

In many qualitative accounts, respondents do not know what the attacker's end goal is. And it is difficult to make assumptions about end goals without sufficient specific information.

The conclusion is that, of the 14 victims of identity fraud, only 3 were, in our opinion, truly identity fraud; 6 incidents could be best explained as phishing, and the rest were close to identity fraud but were mainly attempts at identity fraud by email, in contrast with the question of Statistics Netherlands.

Hacking

When one looks at the question on hacking, we would also qualify them in a different way.

Phishing. Nine of the so-called hacking incidents were actually phishing, in our opinion, and I would like to give examples of two cases that were actually phishing in our opinion. The two examples are described below:

Victim 3: *Partner received emails from his own account with advertisements*

In this case, the victim's partner received an email with advertisements from what appear to be his own account. The problem is that it probably only looks like it is coming from the partner's own account; it probably comes from a fake email address.

Victim 4: *I got a pop-up asking for my credit card information because I had earned extra flight miles and he wanted to add them.*

Victim 4 also mentions something interesting. He gets a pop-up that asks for his credit card information, with the excuse that he earned extra flight points which need to be added to his account. And so, to us, this is 'phishing via a website'.

Other incidents in this category were as follows:

- Abuse of an email account sending spam to the contacts of the respondent.
- Someone tried to login from Estonia on the account of the respondent's brother who happened to be in India. However, using a two-factor authentication helped to give the brother access to his email account. How all this is possible is not clear to us.
- Respondent believes he was hacked but is unsure.
- Respondents received several emails supposedly from the banks.
- Respondents received a phishing email asking for game account login information.
- Phishing of Facebook account. Probably the respondents' password was leaked at one point.

Malware. Two incidents described malware. In one case, a virus that was installed on the respondent's computer. The second incident mentioned that a website that was visited by the respondent started sending information on the websites that were visited by a third party for marketing purposes.

Hacking. One incident was really 'hacking': so-called friends of the respondent's sister were trying to get his password to log into his account.

Threat. One incident was a threat. This respondent received an email that mentioned he had been watching child pornography on his computer. And if he did not bring money to a gas station, the attacker would call the police. So that was that basically extortion.

A few additional things should be noted.

1. Two respondents mentioned an incident that happened to someone else from the household or in their family, a partner and a mother. So, both incidents should actually

not have been counted by Statistics Netherlands, as their questionnaire focusses on victimisation of individual victims, not households.

2. Two respondents mentioned explicitly the same incident twice, both as 'hacking' and as 'identity fraud' and explained they did not know under what concept it should have been mentioned. We categorised both incidents as 'identity fraud'.
3. One could argue that phishing and identity fraud are very similar, although the question formulated by Statistics Netherlands implies actual loss of money and phishing is often an 'attempted crime'. However, 8 out of 13 hacking incidents also mentioned phishing.
4. Finally, when we went through all of the victims' answers, very often the description of the incident was vague and incomplete. Also, many victims were at a loss to explain what it was that they saw happening. Therefore, it was often difficult for the authors to understand the explanation provided by the respondents.

The results basically show that, in terms of identity fraud and hacking, out of the 27 incidents that were reported, half were phishing, and the rest were mostly identity fraud and skimming. Table 1 summarises the findings.

Table 1 Summary of findings that compare the quantitative findings of Statistics Netherlands with the qualitative findings, in respondents' own words (no double counts)

Qualitative findings, 'what happened, in your own words'	Quantitative findings of Statistics Netherlands			
	Identity fraud: 'personal data is used without permission for financial gain'	**Hacking:** 'someone has maliciously broken into or logged into a computer, email account'	**Total**	**Proportion**
Phishing: 'phishing for personal information'	6	8	**14**	**0.52**
Identity fraud: see definition of Statistics Netherlands	**3**		**3**	**0.11**
Skimming	3		**3**	**0.11**
Cyberbullying/threat	1	1	**2**	**0.07**
Malware		2	**2**	**0.07**
Hacking		1	**1**	**0.04**
Unknown	1	1	**2**	**0.07**
Total	**14**	**13**	**27**	**1.00**

In sum, to measure cybercrime victimisation, we as a research community still have difficulties in finding out how to ask the right questions. Therefore, we would like to end with a few conclusions and some suggestions on how to deal with this problem.

A first observation is that, although victims report phishing, in most victimisation surveys there are few studies that asked questions on phishing (Reep-van den Bergh & Junger, 2018). I believe that the UK did it once, and, yesterday, Andri Ahven and Mari-Liis Sööt mentioned that there is a question about phishing in the Estonian victimisation survey.[1]

We also suggest that researchers have 'an offender bias': we ask questions about what the offender meant to do (get money or credentials), rather than what the victim experienced.

We may also have a 'law bias': victims usually know about basic legal categories of offline crime, such as burglary, auto-theft or rape. But do they know, similarly, the legal categories of cybercrime? If you think about the Budapest Convention, this is incredibly useful for law enforcement. But today, many citizens do not know the legal categories of cybercrime. A recent Proofpoint study showed that 39% of the 3,500 respondents surveyed (employees from seven countries: the US, Australia, France, Germany, Japan, Spain and the UK) are not sure what the term phishing means. The older generation (aged 55 and more) knew this better than the younger generation (18–22 years).

Furthermore, it is difficult to ask questions from the point of view of the law, as it easily leads to lengthy and complicated questions. This certainly happened with some of the questions of Statistics Netherlands presented above. In their effort to somehow copy legal categories they get these slightly odd questions.

Perhaps one could argue that the problems we focus on are, to some extent, a cohort problem. Perhaps our generation of researchers is too old, but our children and grandchildren will know what is happening, and they will be able to answer the questions in a better fashion than most of us today.

And yes, what sort of additional remarks can I make?

Choosing a dimensional approach. I think it has been said yesterday, and I very much agree, that basically we cannot really say that something is 'cybercrime'. It is often more useful, we believe, to conceive ICT as a characteristic of crime. Crime could be conceived as a dimension. At the one end of the dimension, crime is completely physical, and, at the other end, crime is completely digital. A lot of crimes have both physical and ICT aspects (Caneppele & Aebi, 2019; Lusthaus, 2019).

Focus on modus operandi. More generally, it may be useful in cybercrime surveys to focus more on the *modus operandi* to the extent, of course, that victims can tell something about it.

1 See the presentation by Ahven and Sööt (in this volume).

Experimenting with alternative measures. Of course, it is also important to think about alternative ways to measure cybercrime, and I am happy that there will be presentations on this. What we would like to propose is that we need to experiment more to learn better how we can improve our measures of cybercrime. So, for instance, we could experiment with other questions, broader questions, or more precise questions; for instance, 'what happened to you, can you describe this?' We have tried in the past to help people with their IT problems and asked them about their ICT-related behaviour; for example, 'Okay, can you tell us "how do you deal with your PC in practice?"' and then search their PC for any evidence pointing to the presence of malware. That was a plan that we had, but no one wanted to fund it. This is a pity; few organisations seem to be interested in end-users.

Perhaps one could integrate questions on cybercrime with measures of fraud victimisation – I think that has been suggested yesterday – and ask about fraud victimisation and eventually ask about the online and offline aspects.

Multidisciplinarity. Perhaps we can improve by working more with professionals and researchers from other disciplines, for instance, computer scientists. This would help us in trying to understand what happens in the technical sense, that is, what is happening on the computer system. Use alternative measures, such as asking, 'Can we see or measure how much phishing emails are coming in?'

And so, to conclude, let us pay renewed attention to measurement issues. It matters for policy as well as for prevention of crime. Thank you very much. If anyone is interested in more information, you are welcome to send me an email.

References

Aebi, M.F., Killias, M., & Tavares, C. (2002). Comparing crime rates: The International Crime (Victim) Survey, The European Sourcebook of Crime and Criminal Justice Statistics, and Interpol Statistics. *International Journal of Comparative Criminology, 2*(1), 22-37. Available at https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.622.4214&rep=rep1&type=pdf.

Australian Competition and Consumer Commission (ACCC). (2020). *Targeting scams 2019. A review of scam activity since 2009*. Canberra, Australian Capital Territory: ACCC. Available at www.accc.gov.au/system/files/1657RPT_Targeting%20scams%202019_FA.pdf.

Brown, R. (2015). Explaining the property crime drop: The offender perspective. *Trends and issues in crime and criminal justice* (495), 1. Available at www.aic.gov.au/publications/tandi/tandi495.

Caneppele, S., & Aebi, M.F. (2019). 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, 13*(1), 66-79. https://doi.org/10.1093/police/pax055.

Cantor, D., & Lynch, J.P. (2000). Self-report surveys as measures of crime and criminal victimization. In D. Duffee, R. Crutchfield, S. Mastrofski, L Mazerolle, & D. McDowall (Eds.). *Criminal justice 2000. Vol. 4. Measurement and analysis of crime and justice* (pp. 85-138) National Institute of Justice.

Farrell, G. (2013). Five tests for a theory of the crime drop. *Crime Science, 2*(1), 1-8. https://doi.org/10.1186/2193-7680-2-5

Florencio, D., & Herley, C. (2012). Is everything we know about password-stealing wrong? *Security & Privacy, IEEE*. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6175885, doi:10.1109/MSP.2012.57.

Gottfredson, M.R. (1986). Substantive contributions of victimization surveys. In M. Tonry & N. Morris (Eds.), *Crime and justice. An annual review* (Vol. 7, pp. 251-288). The University of Chicago Press.

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research, 26*(3), 293-312. https://doi.org/10.1007/s10610-020-09439-2.

Lusthaus, J. (2019). *The offline dimension of online crime*. Paper presented at the USENIX. Available at www.usenix.org/conference/enigma2019/presentation/lusthaus.

Microsoft. (2020). *Microsoft digital defense report, September 2020*. Available at www.microsoft.com/en-us/download/details.aspx?id=101738.

Miró-Llinares, F., & Moneva, A. (2019). What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks "did cybercrime cause the crime drop?" *Crime Science, 8*(1), 12. https://doi.org/10.1186/s40163-019-0107-y.

Montoya, L., Junger, M., & Hartel, P. (2013). How 'digital' is traditional crime? *European Intelligence and Security Informatics Conference (EISIC) 2013*, 31-37. Available at https://ieeexplore.ieee.org/abstract/document/6657122.

National Academies of Sciences, Engineering, and Medicine (NAP). (2018). *Modernizing crime statistics: Report 2-new systems for measuring crime*. The National Academies Press.

Pease, K., & Ignatans, D. (2016). The global crime drop and changes in the distribution of victimisation. *Crime Science, 5*(1), 11. https://doi.org/10.1186/s40163-016-0059-4.

Reep-van den Bergh, C.M.M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7*(1), 15. https://doi.org/10.1186/s40163-018-0079-3.

Sessink, D. (2018). *Using machine learning to detect ICT in criminal court cases.* Bachelor Thesis, University of Twente, Enschede, Netherlands.

Statistics Netherlands. (2017). Cyberbullying per age group. Available at http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=83096NED&D1=185&D2=7-14&D3=a&D4=a&HDR=T%2cG2&STB=G1%2cG3&VW=T.

Cybercrime Victimisation Research in the Netherlands

Lessons Learnt from Past Studies

Johan van Wilsem[*]

Thank you for the opportunity to give this presentation about cybercrime victimisation research in the Netherlands and particularly, as requested, the lessons learned from these studies. My name is Johan van Wilsem. I am a strategist researcher at the Dutch Court of Audit. And I will tell you something about the victimisation research projects I conducted in the past. My own background is that, for many years, I have been doing cybercrime research based on a panel module from the so-called LISS panel. This is a Dutch research opportunity in a panel design, which includes all kinds of life domains, including the panel I initiated on cybercrime and conventional victimisation. This is a prospective victimisation study that was conducted between 2008 and 2018 – over a 10-year period, including overall 6 waves, surveying approximately 6,000 respondents in each wave. And as a panel study, we tried to include as much as possible the same respondents. I have already published numerous articles and chapters on this study findings. And based on the lessons I learned from that work, I am giving this presentation.

I would like to share four of the main lessons I have learned from these studies.

Lesson number 1 – It is very valuable to conduct panel studies; victimisation studies overall are based on a cross-sectional design, meaning, there is only one measurement. Whether this is a representative sample or not, it is just one measurement over time. In contrast, in a panel study the same respondents are used, but there are multiple measurements over time from these same respondents. This allows for new things to be compared in cross-sectional studies because it enables a career perspective on victimisation. Well, maybe *career* is kind of a peculiar word to use when we talk about victimisation, but my meaning is that we can, over a substantial time period, identify if there are people who are not only high-frequency victims, but persistent over time.

So, each time, we do a measurement about victimisation, we see that a particular group of people are involved in cybercrime victimisation, and this is being labelled in the literature as the so-called *super targets*. In addition, apart from this career perspective, panel studies

* Court of Audit, Netherlands. Additional material: the author's visual presentation is available here: https://rm.coe.int/presentation-johan-van-wilsem/1680a0339f.

also allow for a better disentanglement of cause and effect and, therefore, in policy perspective, also offer better potential to identify what works: what initiatives from victims or from policymakers are actually effective in reducing victimisation risk? To name an example, in a cross-sectional study we ask respondents to report their experience of victimisation as well as the security measures they have taken to protect themselves against cybercrime – for instance, a firewall or having a secured wireless Internet connection; it is very hard to see what actually causes what. Is it the technical protection measure that affects the victimisation or is it the victimisation that leads to more protection measures? In a *panel* study that we conducted quite recently, it seems that the latter is more the case. Therefore, technical protection measures are not so much the cause of less victimisation, but victimisation is actually the cause of increased protection measures.

In order to explore in depth the career perspective from the data that we collected in six waves, I carried out a comparison that is presented in Table 1. In the left column, you see all the data that were collected in a 10-year period, coming from approximately 13,000 respondents who participated at least once in the survey. In the right column, you see a selection of those people who participated in each of the six waves of the study; they participated in the LISS panel each time we asked them to do so. Most respondents were not willing to participate six times in the study; so this is a much smaller group of only 1,000 people. For both groups, when you look at the left or the right column, either way we were able to ask respondents about victimisation over a long period of time. And so, in regular cross-sectional studies, when you ask about victimisation over the past year, you see for various cybercrimes a few percentage points. But when we were able to follow people over time, and in this case a 10-year period, it is at least a quarter of the people. So, if you either look at all the data that were collected or at the people who participated in the six waves of the study, it is a very large number of people who sais, 'yes, over a longer period of time I have been the victim of a crime.'

Table 1 Combining the data from six waves of data collection

	All respondents, participating at least once	Respondents participating in all six waves
N	13,430	1,072
Cyber victim 2008-2018	24%	38%
Victimised 1-2×, among victims	75%	72%
Victimised ≥ 10×, among victims	3%	3%
Share of incidents experienced by super targets	16%	13%

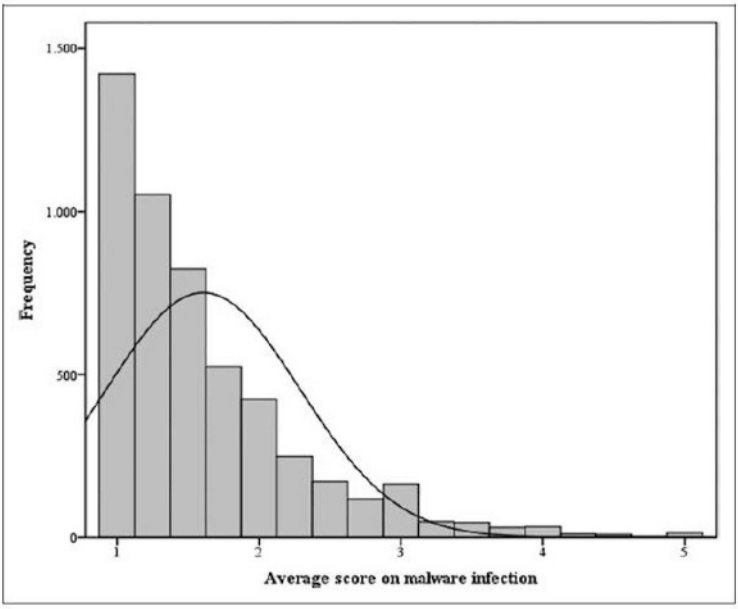
When we look at the group of victims, which is either 24% or 38% depending on the selection, most of them are saying, 'I have over this 10-year period of time been victimised either once or twice.' So mostly not too many times: three-quarters of the group of victims are saying that this is quite a rare incident for them. On the contrary, we also see that there is a group which, over a 10-year period, can be labelled as a so-called *super target*, because analysing the data collected over these six waves, we found that approximately 3% of these people said, 'I have been victimised 10 times or even more.' That small group of people have been involved in approximately one out of six victimisation incidents. So, a large concentration of victimisation prevailed in that group.

Lesson number 2 – The second lesson that I learned from these studies is that, as Marianne Junger said before, it is very worthwhile to think about other ways to ask your questions to respondents. More specifically, it is worthwhile to ask respondents whether they encounter certain computer problems, such as their computer crashed, the home page of the computer changed without their knowledge of how that came about, or a new programme appeared on it. Each of these computer problems may not be a definite sign, but at least it is indicative of malware infection; thus, it is an alternative way of asking people if they have been the victim of a malware infection. Most responders will have a hard time recognising malware infection occurring in their computers. So, the answer to such victimisation questions would probably yield less reliable information than in the case of questions about things that people are much more able to indicate, that is, computer problems. These malware infection indications may actually accompany cyber victimisation at a later point in time, such as the computer getting hacked. Therefore, possibly, if we are able to identify whether people have certain computer problems, then we have a way of identifying early warning signs, especially when we conduct this in a perspective panel study in which we can see if early computer problems are indeed indicative at a later point in time of someone being a victim of a computer crime.

What we did – and the results are shown in Figure 1 – was to ask about four types of computer problems in the examples that I showed to you – ask people how many times they experienced this on a 1–5 scale; 1 means 'This hardly or ever happens to me'; 5 means 'I am experiencing this problem all the time, multiple times per month, so over a year I am swamped in these problems.' So, what we see here is that, if we average out these scores for respondents in a panel study, most of the respondents luckily say that they are at the lower end of the scale variable (Figure 1). So, most of the respondents say, 'I am having hardly any computer problems.' We also see that there is also a smaller group of people who say, 'Actually I am running into some problems quite regularly.' And a very small portion of people say, 'This happens to me all the time.' What we are able to do – and I will tell you a little more about this in the presentation later on – is to relate these answers on the harshness of malware infection indications to all kinds of behaviours and

characteristics of victimisation targets. For instance, is online routine activity related to malware infection? Are low self-control indicators related to malware infection?

Figure 1 Average score on four questions about malware infection



Lesson number 3 – It is worthwhile to pose questions to the victims about the actions they have taken and also about the outcomes of those actions. This is not a new lesson because, as you all know – being familiar with victimisation surveys – it is quite usual to ask victims whether they have reported the incident to the police and what the police actually did with it. For cybercrime victims, these types of questions are interesting as well. But, in addition, I think that *reporting to the bank* is an alternative action – that is in cybercrime terms at least as interesting – as well as the reaction of the bank and whether the victims were actually successful in getting their money back. So, if they were reimbursed by their bank, what were the crime targets' actions to get reimbursed, and, ultimately, what were the financial consequences for cybercrime victims of either theft fraud or ID fraud or the banking fraud that they experienced?

For the group of people who were surveyed over an eight-year period, we asked them questions about banking fraud in 2010 in the LISS panel. We asked them, 'how much money did you lose initially?' and 'how much money did you lose in the longer term after you reported it to the bank or to the police?' What we see here is that the *initial* loss – the amount of cash that was withdrawn illegally from the bank account – varied across victims.

Roughly 10% of the victims said this amounted to as much as 1,000 Euros or more; on the other extreme, a little bit more than a quarter of the victims said, 'well, it was relatively not so harsh.' This group said it was 50 Euros or even less (Table 2). When we look at the *final* loss, we see that the reimbursement policies in the Netherlands seem to be quite generous. So, 80% of these victims eventually did not lose anything – they were completely reimbursed, which left a group of approximately 20% with additional financial losses. And most of the time, not too large amounts. But sometimes these were considerable amounts, for instance, up to 250 Euros or more. This was a minority; nonetheless, here we can relate these outcomes to the actions undertaken by the people in this group and their demographics – for example, age, educational level and self-control.

Table 2 Amount of financial loss after banking fraud (N = 636), data from 2010 to 2018

	Initial loss	**Final loss**
€ 0	-	82.2
€ < 50	27.5	7.4
€ 50-99	16.5	3.0
€ 100-249	13.5	2.8
€ 249-999	14.0	1.7
€ 1,000 or more	10.1	0.9
Unknown	18.4	1.9
Maximum loss	€35,000	€10,500

Lesson number 4 – I want to share a last lesson with you: it is very worthwhile to ask questions among your respondents about their levels of self-control, because in the previous work that I did, it has been proven to be a prime predictor of the issues 1, 2 and 3 that I just talked about. This means that people with low self-control have much higher victimisation risk for all kinds of cybercrime types, varying from harassment to being defrauded to being hacked. When we look at prolonged persistent involvement in victimisation in terms of a group being a super target, this risk is also substantially higher among people with little self-control. They are also more likely to encounter computer problems that are indicative of malware infection. And the consequences of banking fraud seem to be more severe among the people with low self-control because of the fact that they are less inclined to contact the banks after the victimisation. This, in turn, means that they receive less often a reimbursement from their banks after a banking fraud. So, among the 20% who are left with a final loss, we see a concentration of persons with low self-control. And this means, in terms of crime prevention, that we can yield maximum

benefits if we are able to do it successfully among the group of victims with low self-control. This is a very hard task because successful prevention is difficult for people with a personality trait that is relatively stable. So, I think an interesting discussion can be held about how we can do an effective and efficient prevention strategy for victimisation in general, but especially for the group in which we see that the risks are concentrated.

Thank you for the attention.

Finland's Experiences in Cybercrime Surveys

Matti Näsi[*]

Thank you. My name is Matti Näsi. I work as a university lecturer at the University of Helsinki, Institute of Criminology and Legal Policy. And I will be continuing with the same theme, but presenting the case of Finland. Now, in a broad sense, if we ask what the state of cybersecurity in Finland is, I guess it depends on who you ask. Some say that it is in a pretty bad state, and some say it is our strength in the international context. So, I guess it depends on if you are the kind of person who sees the glass half-full or half-empty. But it seems to be dividing experts' opinions in terms of what the state is. Of course, the state of cybersecurity tends to be more general. It takes into account national-level threats, basic infrastructure threats and so on, not just cybercrime threats, but it still divides opinion quite a bit. But I think the same sort of insecurity, or not having a clear picture, does apply in the context of both cybercrime and cybercrime victimisation.

From a criminological perspective, I do not think that we have established a very good picture, or laid very good foundations, in terms of understanding what our situation currently is, especially in terms of the hidden crime aspect, that is, the victimisation experiences of persons that do not come to the attention of police and appear in official statistics. And this is in a way kind of surprising because Finland is a very tech-savvy country; it has had for decades a big IT sector, an industry that does have a big influence on the society in general. But despite this, we have very little information or relatively little information on this matter, either from a criminological perspective or from a cybercrime perspective. So, there are a lot of assumptions, but, to be honest, there is a lot less concrete information. There is clearly a great, great need for good basic research. In terms of looking at the bigger picture in cybercrime victimisation, from a statistical perspective, in all honesty, I can say the problem with official statistics is that they tend to tell us relatively little: according to official police statistics, for instance, in terms of fraud, last year there were 29,000 cases of fraud recorded by the police. However, from the statistics, we cannot really tell whether it was an offline fraud, an online fraud or some sort of hybrid fraud. So, we do not really have the means to establish whether that incident took place or in what environment did it take place. We have seen a steady increase in fraud crime statistics, and we speculate that this is due to increased online offending. But the statistic in itself is not yet a good tool in terms of revealing the details in many of the offences. In the example of

* University of Helsinki, Finland. Additional material: the author's visual presentation is available here: https://rm.coe.int/presentation-matti-nasi/1680a033af.

hacking cases, we see a great variation between years in terms of how many cases are reported to the police. So, there are a lot of instabilities in terms of how good and reliable the information is and what kind of picture does it actually paint. I trust the private sector statistics even less, mainly because the means of data collection, or the sort of methodology applied, is usually very vague. We do not know much about it. And of course, they have their own business incentives in reporting certain types of statistics. So, I do not really count on that as being reliable information.

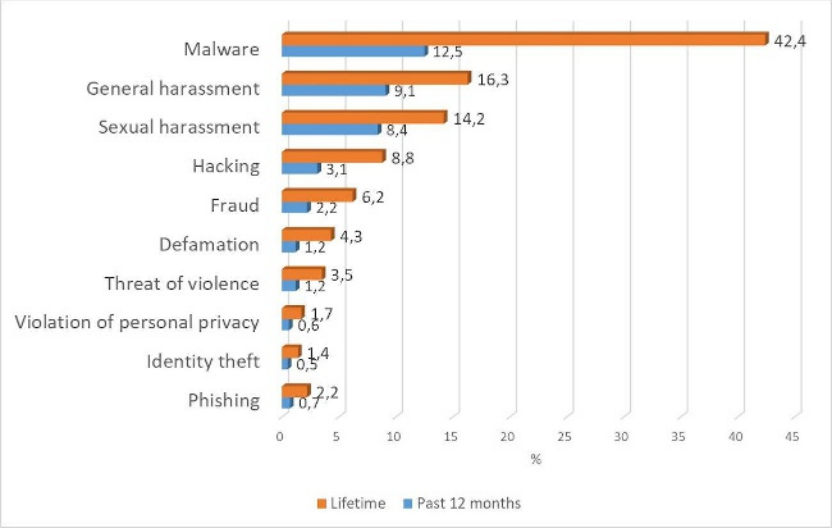
There are very few survey studies. There are a few that focus on young adults and adolescents, but from a population level, a standard that has been one before, which is a public sector survey, there was one in 2009, and it had about 40,000 participants and it was representative of 15- to 74-year-olds. And in it there was a question regarding cybercrime victimisation. However, the question was very vague, very general. It was just asking the respondents if they had been a victim of crime via the Internet. That does not really give a very detailed information about the phenomenon in general. So, there was a lack of detailed information at the population level regarding cybercrime victimisation prior to 2018. Our aim was to try to fill this void a little bit in 2018 through a National Crime Victim Survey that we conduct every year in its current form. It has been conducted since 2012, but the earlier version has been established already in the 1980s. So, it is a very well-established measure, a well-established tool for collecting survey data. It usually focuses on traditional crime victimisation: property and violence. But in 2018, we decided to include a cyber module in it. And the aim is hopefully to include this cyber module in it every four years, so that we have information on a continuous basis. So hopefully we can make that happen. But this survey is conducted by our institute at the university. So, it is not the statistics centre in Finland, but only our institute.

I will describe it a little bit, because this relates to the challenges we have with this survey. Of course, it involves the basic background information: age, gender, education, financial situation and so on, and the questions about offline traditional crime victimisation. Our cyber module has many items, and not just the victimisation items; it has 10 different types of cyber offences and in addition it also has questions regarding behaviour, that is, the online behaviour of respondents. We asked for their online behaviour and activities, their online skills, as well as questions on what sort of measures they take in regard to their protection, password use and so on. Our 2018 survey had a sample of 14,000 respondents, and the response rate was about 39% and it was representative of the 15- to 74-year-old Finns.

Now here, in Figure 1, are some of the items and the prevalence rates regarding lifetime and past-12-month victimisation: we see that malware and forms of harassment were the most common forms of victimisation. If we compare this to the article that Marianne and

her colleagues published in 2018[1], we can see, for instance, that the prevalence of harassment tends to be much lower in many of the national surveys they compiled. So, this may reflect that our survey items might be a little bit different from those studies. Here, you also see that there were some calls for phishing information, and we have that here. Yesterday, our Estonian colleagues found a much higher prevalence rate of phishing, and I predict that this is mainly because our survey items are different. In our survey, we did not ask whether the respondents had received phishing messages or experienced any phishing attempt; instead, what we did was to collect information regarding whether the respondents had given out their username, password or credit card information as a result of the phishing message. So, it is about whether that message or the phishing attempt had been successful and not about whether someone tried to get the respondent to give out information or whether the respondents had received this type of phishing message.

Figure 1 Cybercrime victimisation in Finland 2018 – lifetime and past 12 months (%)



Another interesting aspect with the victimisation prevalence is that if we look at the 2009 survey, 10 years ago, we can see that although the survey item was very general in nature, 2.5% of the respondents reported experiencing some form of cybercrime victimisation during the past three years. However, 10 years later, in 2018, we had 55% of respondents who have had lifetime victimisation experiences and 35% of the respondents reporting

1 Reep-van den Bergh, C.M.M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7*(1), 15. https://doi.org/10.1186/s40163-018-0079-3.

some form of cyber victimisation in the past 12 months. So, in this way, it would seem that the rate of cybercrime victimisation has seen a tenfold increase. But it may also have been due to the study design and the question design which may influence the prevalence rates because our survey asked for much more detailed information. So, this might have influenced the prevalence rate in some sense. But I think it is still an interesting finding that there is a big difference between the 2009 survey and the 2013 survey.

What are some of the key challenges in the survey, planning and design? Well, to begin with, if you think about cybercrime as a more complete approach from a criminological perspective, it is much easier to collect information on victims than on offenders. This also dictates the type of information that we tend to collect; it makes, at least in the case of Finland, the research on cybercrime a bit more one-dimensional compared to research on traditional crime. And I say this because many types of offences are very specific and you need specialist skills on hacking, or it may be malware or phishing. It takes a much more sophisticated approach than, for instance, asking about online harassment – it is easier to know whether someone has been harassing their partner or someone else. So, from an offender's perspective, the research design is a little bit different. And so far – because we are in the early stages of collecting cybercrime information – from a hidden crime perspective, with the survey measures we have been focusing on the victim perspective only. It has been said in previous presentations that it is an umbrella term. It makes it very vague. So, what forms of victimisation should we actually focus on? Should we focus on those more computer-aided, computer-enabled offences, versus malware, phishing and so on, or do we also include items of harassment and defamation and so on, for example, threats of violence? So, whether there should be a separation in the studies – different studies – or whether they should be all brought together in some form of victimisation surveys, I do not know.

Another question is, who is the actual intended target? Has the respondent actually been a victim personally or a victim in the case of collateral damage – for example, the bank is facing a denial-of-service attack and the bank is down for three days and the victim couldn't buy anything or use their credit or debit card? Are you the target of the crime or is your bank the target? Do you perceive yourself as being the victim of the hacking or the denial-of-service attack?

Also, in the past week, there has been a big discussion about a major hacking incident where a hacker downloaded a patient's records from a company that provides psychological counselling services. It was a massive breach of information. And the discussion is also, of course, about the victims, yet it is also about the level of cybersecurity. And some of the discussion is about the level of cybersecurity of these individuals. But in this case, they were not victims because they had a poor password, or because they were active online and exposed to potential offenders; no, they were victims because they were using a different service, they were using a service provider, and that has nothing to do with their online

behaviour. So, it is just that there are so many levels of victimisation here, that it is key to try to establish who is the victim and whether they were primary victims or not.

We also have challenges with the survey design in general, about how to ask, how to set up the questions and how to get the sort of relevant information and detailed information that we are actually looking for. If you look at different articles on cybercrime that are being published, there tends to be quite a bit of variation in the measures. So, there is variation on how to ask about victimisation experiences; there are not really established measures and questions that are in use. I think we could use some international collaboration in terms of trying to set up good measures and establish good questions in terms of collecting this type of information, so that we can actually compare results in the international context as well. Questions regarding the background variables, such as online behaviour or user protection, are even less established. So, in terms of looking at the risk factors and the individual routine activities and behaviour online that might influence the risk of victimisation, we need good background information variables. And I think there are even less established measures and questions regarding this type of information in the field in general. Many of the most quoted studies that used more advanced experimental study designs – and they tend to be American studies – also used data or samples that are not very good. They usually use college-level samples, and they can play around with those samples a bit more and they can be a bit more detailed. However, we do not necessarily have that chance in the population-level surveys, where we have a limited amount of information that we can collect because these surveys tend to be collecting information regarding other aspects as well. So, it is not easy and it costs a lot of money to conduct these population-level studies. I think the emphasis of the future research should be on studies that use good representative data, rather than always use an experimental or small sample data.

But in our case, the biggest challenge is the declining response rate in surveys. And I am not joking about this, but if the current declining trend in the response rate continues at the same pace as in the past five years, by 2030 we will not have any respondents. In the past five years, our response rate declined by almost 20%. So, it is a massive problem if this same trend continues, because we will not get reliable data on this sort of hidden crime aspect. So, it is a big problem.

Finally, a few lessons learned from the survey. We have victimisation trends for traditional crimes in our survey – violence and property crime, but what is also interesting is that we ask whether people are afraid of certain types of crime victimisation. We asked about cybercrime victimisation as well as violence. And over half of the respondents reported being afraid of cybercrime victimisation, whereas regarding violence, only less than 30% reported fear. Well, that is a high number in general, but it is much smaller compared to cybercrime victimisation. So, less than 30% of the respondents reported being afraid of violence victimisation, but more than 50% were afraid of cybercrime. Cyber

victimisation is in a way a big threat, or is perceived as a significant threat, in terms of people's responses.

When we talk about official statistics, the challenge is that hidden crime seems to be particularly strong in the cybercrime context: only 2% of the victims have actually reported the crime incident to the police. So, most or the vast majority of these types of victimisation experiences are not known in official statistics. Of course, there are differences between offences: fraud offences were more likely to be reported the police than some other forms of victimisation. But in the case of fraud, only 10% of the crime incidents have been reported to the police. So, there is clearly a need for this type of basic population-level research if we want to have a complete picture, or a better bigger picture in terms of victimisation in the cybercrime context. And I am keen to participate in international collaborations in terms of developing better study designs, measures and items, to have sort of good ways and solid ways of conducting this type of research. Thank you.

Measuring Cybercrime in the Crime Survey for England and Wales

Billy Gazard[*]

Thank you for inviting us to the meeting and to share an update on measuring cybercrime in England and Wales. I will give you a really brief overview of how we measure cybercrime in our National Crime Survey for England and Wales currently and also how that has been affected by the coronavirus pandemic and what we have done to respond to that – so that we can continue to measure crime and cybercrime – and some of the future work that we are now thinking about given the current circumstances. So, for those who are not too familiar with the Crime Survey for England and Wales, I will just give some brief information. It is a randomly selected cross-sectional survey, representative of England and Wales. as a whole. It is conducted through face-to-face interviews in people's homes using trained interviewers and a structured questionnaire. We interview approximately 35,000 people every year: adults aged 16 and over, living in private households. We also conduct a Crime against Children Survey with an additional 3,000 interviews of 10- to 15-year-olds also selected from those households. We ask people about their experience of crime in the past 12 months. And we have a longstanding time series going all the way back to 1981. And as well as asking about the experience of crime – so we can calculate our crime estimates across England and Wales – we also ask about additional topics such as perception of crime, domestic abuse and drug misuse.

In terms of measuring cybercrime in the survey, in the longstanding time series started in 1981 we obviously concentrated on traditional offline crimes. But given the changing context with more people being online and the ability to conduct crimes with online help, in 2011 the National Statistician's Independent Review recognised the need for an improved measurement of fraud and cybercrime. And we established a project looking at the feasibility of that to cover fraud and cybercrime in the crime survey in 2014. We were then able to publish our first statistics on estimates of fraud and computer misuse in 2016, and our statistics on fraud and computer misuse classified as 'national statistics' in 2018. Regarding the development of our work, I guess the main challenge was around how we classify these offences, and how do we make it in a way that is simple and that our users can understand, so that we can classify if an offence has taken place. And we did that by separating our

* Office for National Statistics, Centre for Crime and Justice, England and Wales. Additional material: the author's visual presentation is available at https://rm.coe.int/presentation-billy-gazard/1680a0339c.

offences into *non-confidence frauds*, where personal information of the victim has been used for gain, for example, and *confidence frauds*, where deception has been used, for example, tricking someone in terms of the characteristics of online goods.

And so, once we actually decided how to best fit our questions so they could be easily understood and would measure fraud, then we faced the additional challenge of making sure that our classification closely aligned with the Home Office counting rules, that is to say with the national standards on how police record crime. Obviously, there are some differences. For example, who is the victim? How many victims? The crime survey is primarily a victimisation survey where we are concentrating on individual victims, whereas police-recorded crime is also about crimes against organisations. And also, in terms of *when* the crime occurred, for traditional crimes we are able to obviously record when an incident took place, but with fraud and cybercrime it is a lot more difficult. So, we move to recording when the victim *came to know* about the fraud, rather than when it took place. And we did this also in the existing victim forms that we had in place before we introduced the fraud and computer misuse questions. It was also important to distinguish whether the crime took place geographically within England, Wales or abroad, but obviously with computer misuse and cybercrime, we do not always know, given the complex nature of these offences and the global nature of them. Hence, we decided not to ask where the incident took place for these incidents of fraud and computer misuse.

Hence what we came up with, and what we are able to now produce in our statistics, are a range of categories of fraud, which include bank and credit card fraud, advanced fraud, consumer retail fraud and other fraud. And we also provide statistics on two offences that are covered by the National Computer Misuse Act: unauthorised access to personal information as well as computer viruses. So, these modules are really formed in a way that we can also measure the online part of a fraud as well. We know that we can divide fraud into offline fraud and online fraud. And then we added questions on computer misuse as well. But in terms of other offences (more traditional crimes), we also wanted to make sure that we could measure if there was an online component to these offences. So, for all other offences, we now also have a *cyber-flag*, so we can keep track of how many of the total offences are in some way related to cybercrime.

In terms of what we know right now, we have been collecting and producing statistics on fraud and computer misuse since early March 2017, so obviously we have a much shorter time series compared to other crimes, which go back to 1981. But just to give you an idea of the picture within England and Wales, currently for the year ending March 2020, there were 3.7 million incidents of fraud estimated using the crime survey and 53% of these incidents were flagged as cybercrime. So, you see that there is a huge volume of incidents of cybercrime, even when looking just at fraud. In addition to that, there were sort of 1 million incidents of computer misuse as well. And this makes up well over a third of total crime in England and Wales for the year ending March 2020. And kind of alluding

to what has been said previously, it is really important data. It gives a much better idea of the extent of fraud and computer misuse across England and Wales, particularly given that the majority of offences are not reported to the police or other reporting bodies, such as our main reporting body in the UK: Action Fraud. For instance, in that year, only 14% reported to Action Fraud. We know because we have further questions on the nature of fraud, and we ask questions about whether they have reported banking fraud to the bank, for example. We also have data on the impact on the victim, the method, the reason for the initial contact with the perpetrator, the satisfaction with the response of the reporting body, as well as questions around the experiences with computer viruses and the security measures that people take online. And a lot of this is reported in our main publication on fraud and computer misuse, and the latest was published earlier this year.

So, we put this set of screeners in place, but we are constantly trying to make sure that we improve the questions. We want to find out more about the nature of these offences and how they take place, so that we can help policymakers in the government. The most recent round of questioning development took place last year and focused on how we can identify the offences that are facilitated by a computer misuse offence. For example, when someone's personal details are hacked and information is gained by fraudsters that enables them to access the victim's bank account; so that we can provide a bit more nuanced data on how computer misuse of fraud offences are connected and what the nature of these incidents is. These questions were due to go into the questionnaire in April 2021, but obviously this has all been affected by the coronavirus pandemic. Due to the pandemic, all government household surveys across England and Wales were suspended on the 18th of March 2020, which meant that our crime survey was also suspended. But this largely did not affect our data up to the year ending March 2020. Our response rate was slightly short of our 70% target, due to losing two weeks of fieldwork at the end of March, and the number of interviews that we usually aim for, 34,500, we were just short of that as well. But what it has meant is that we have had to make some operational adjustments on how we continue to collect statistics on crime across England and Wales. And up until that point, we had not really had a chance to look at what the alternatives would look like.

What we decided to do, and what we eventually did, was set up a telephone-operated version of the crime survey and this went live on the 20th of May. So, we had a really, really short turnaround to get the survey back up and running. It took us nine weeks from the date of the suspension to go back live into the field. We had obviously quite big challenges to get this set-up, and one of the first ones was deciding on sample options: a lot of different options were considered, such as *random digital dialling* or *address-based online surveys*. But we decided to go with *re-contacting crime survey respondents* who had already taken part in the face-to-face interviews over the last couple of years. And so, our telephone-operated crime survey sample is based on those people; obviously, people who agreed to be re-contacted. Then we had to make sure that we had enough sample so that

we could continue to measure crime until we estimated that face-to-face interviews could again become a possibility. We set this up as a panel design, and we set it up with three waves. We are going back to respondents every three months to ask them about their previous three months' experience of crime. And this was done so that we could continue to measure crime up to March 2021. Obviously, with the current situation, it is very possible that we may not be going back into the field in April 2021, which means we may need to extend the telephone survey in some capacity.

The questionnaire itself is very, very similar to the face-to-face questionnaire that has been running since 1981. We have the same screening module and the same victim forms, so that we can continue to measure crime and have our crime estimates for crime and also for fraud, cybercrime and other modules. We did not have space for all those, due to time constraints on the telephone interview, but we did introduce new models so that we could look at particular questions around crime in the Covid-19 context. We also collected up-to-date demographic and social economic indicators. We managed to publish our first estimates from the newly set up telephone survey a couple of days ago, for the year ending June 2020. So, we use the telephone survey to make an estimate of crime over the last 12 months, and we estimated that there were 4.3 million fraud offences and 1.6 million computer misuse offences for the year ending June 2020. But it is important to remember we are unable to make direct comparisons with the face-to-face Crime Survey due to the change in the survey mode; although we would like to see that these estimates lay within the range of those reported since we started collecting estimates on fraud and computer misuse in March 2017.

Obviously, with the pandemic, there is a lot of interest on how it has impacted on crime levels. Hence, we have produced our statistics in a way that we can look for each instance at the particular time period in which it took place within that 12-month reporting period. And what we are able to do is to look at and compare the changes in crime between the January-March 2020 and April-June 2020 periods, when we have had the lockdown restrictions that had the most impact on people's lives and on crime trends. And what we found is that there was no significant change in fraud and computer misuse during that time. But this needs to be seen in the context that we had at the moment a small sample size, because we have only been in the field since the end of May. And also, we are only looking at the instance within a quarter of a year rather than a whole 12 months. So that has an impact on the sample size uncertainty around those estimates. Hence, we will need more data to really see the impact of the pandemic, and what the impact has been on fraud and computer misuse offences.

I alluded just before to some of the challenges we faced during the pandemic in terms of measuring crime, and this includes cybercrime: the impact of moving to a telephone interview on estimates and comparability over time and uncertainty, the smaller sample size, having more complex ways to account for the design and the new wave structure, as

well as being able to meet the user needs in terms of measuring short-term change. So, comparing the number of victims and incidents across time within the telephone survey is challenging. And we have to think around issues like recall bias: the possibility of more instances being reported in more recent quarters than those that happened in the beginning of the 12-month reporting period. As well as the shorter time frame and turnaround needed for data processing, so that we can measure these short-term trends and also address the user needs. And making sure that we are flexible in our data collection, so that we are able to add questions to the survey in a more regular basis to meet all user needs.

In terms of the future work on cybercrime, given that we have this new data source – the telephone data – we are really interested in being able to look at the impact of the coronavirus pandemic on cybercrime, and we plan to publish something on that in the near future, in the next year. We obviously want to continue the development of survey questions to better capture *cyber-enabled fraud* and the evolving nature of these crimes. We also know that there may well be future updates of the Home Office counting rules for reporting crime. And we need to match them where possible, while also balancing the time series. And we need to continue working with our partners to make sure we fill the gap, because in the current situation we may have e a little gap in the data. Hence, we have to complement our survey data with data from reporting bodies to understand the nature of fraud and computer misuse and how it is changing during the pandemic. And we have also done some development work recently around child cybercrime, and we have added a module to the survey for children 10 to 15 years old. The first results of this module are going to be published in February 2021. We are looking at estimates of the prevalence and nature of online activity among children, including speaking to strangers, sending and receiving images, and online security, using data from the 10- to 15-year-olds.

For those who are interested, there are some recent publications up on our website. Our most recent publication on fraud and computer misuse goes into a lot of detail around the nature of these offences. And also, our recent publications on coronavirus and crime give an indication of how we are measuring crime during the pandemic. Thank you.

Measuring Cybercrime: A Panel Discussion

Stefano Caneppele, Billy Gazard, Michael Levi, Matti Näsi, Johan van Wilsem and Marcelo F. Aebi

Stefano Caneppele: I think this morning session corroborates that, even through a survey, we cannot measure every type of cybercrime. In particular, a victim survey has some limitations in terms of what can be measured, because some of the persons interviewed are not aware that they have been victims of a crime or, sometimes, they are only one part of a crime puzzle. Hence, the most important question is: *what should we measure*?

We have seen that, currently, most surveys are focusing on fraud. This is a little bit awkward when you remember that one of the main critics to the traditional crime victim surveys was that they could not measure fraud properly, because in many cases people are not really aware that they are being victims of a fraud. However, fraud is now treated as the best cybercrime indicator to ensure comparability across countries when using a victim survey. This means that even our approach to crime measurement is changing.

And there are of course other major issues, such as how we should monitor crime trends. The presentation from Finland highlights still another problem: Finland expects the declining response rate to reach a potential problematic level in next year's survey.

My question to all participants is: what types of cybercrime should we measure through a victim crime survey? Do you think we should include crimes that have not been monitored yet? Or should we just focus on what we have now and try to produce more consistent and comparable figures across different countries?

Billy Gazard: Since the beginning of the Covid pandemic, in England and Wales we have received a lot of questions from some of our policymakers and some of our users about the impact of the lockdowns on the prevalence of fraud, particularly cyber fraud, given that there are a lot more people working from home, a lot more Internet usage and a lot more people online.

I think there was an expectation that there would be a big increase in cyber fraud during this time. And so, we definitely have a lot of questions about whether that is effectively the case.

I think the telephone survey data that we have can help us answer that question. We probably do not quite have enough data yet, and the sample size may not allow a final answer. However, as I said, while we did not see any kind of significant change in police-recorded fraud and misuse between the pre-pandemic period and the April to June 2020 period, we did see a slight rise in those offences using the survey, although it seems

not significant. But we need a bit more data first to see if that increase does end up being significant when we have a larger sample size. Also, we have the issue of the recall bias: people possibly reporting more fraud in the most recent quarter than in the preceding quarters. So, for me, a very important question is whether we will be able to measure the impact of the pandemic on fraud. And in order for us to do that, we also need to make sure that we are able to measure the method used to commit the fraud and its circumstances, and these are questions that we have kept in the survey. So, we are really hoping that, when we do produce a publication on the nature of fraud and computer misuse next year, we will be able to say something about that and how the landscape of cybercrime, and in particular fraud online, has changed during this pandemic period. So, for us, definitely, that is probably an important upcoming question that we are looking to answer.

Stefano Caneppele: Thank you. Just one last question. Matti stressed the fact that there was a trend of declining response rates to the survey in Finland. Are you facing the same issue in England and Wales? I mean, are people more reluctant to participate in the survey?

Billy Gazard: We have not really had that issue in England and Wales. We have always had a very high response rate to the crime survey. That is actually very different to a lot of other national surveys conducted in England and Wales. A lot of the other national surveys have seen a decline in their response rate for some reason. We have definitely thought about why it is that we have managed to keep a high response rate to the crime survey. And we were thinking that perhaps it is because people are interested in talking about their experience with crime and are more willing to share that kind of experience. But given your experience in Finland, maybe there is something else going on in terms of how we interact with respondents, how we do the recruitment. I am not sure. In recent years, we have only seen once a small drop: we were always above 70%, and we had a year recently where we dip down to 69%. So, we were not too worried about it. It is a trend that we have seen across other surveys, but not in crime.

This year, obviously, the response rate is slightly lower, but that is really impacted by losing two weeks of fieldwork. At the same time, we had to change the survey mode to telephone interviews because of the pandemic, and that is going to have an impact on the response rate. It would be good if we were to go back to randomly selected households and going back into the field. I think it is much easier to recruit people when we are knocking on their doors. Given the current circumstances, I do not know if we will be able to go back to that. So, we will see our response rate. If we continue with telephone interviews or an online survey that is randomly selected, I think that we will see a massive change in our response rates.

Matti Näsi: I think one of the basic issues here is that, in Finland, we are using a postal survey since 2012. Before that, it was a household interview or a phone interview. And that, of course, changes the playing field a bit. During the last eight years it has been a postal survey, and we have seen a drop of almost 20% in the participation rate. The change in the methodology might in part explain the change in the response rate. But why so steep? I do not know.

Then it is interesting to compare the current results to those of older surveys. For example, if we compare with previous surveys conducted by telephone, we see a difference – an increase – in terms of reporting, for instance, of domestic violence. This could be because, if you do a phone interview, you might have the other person, the aggressor, within the room. It is difficult to collect information regarding domestic violence if the other person is in the room.

In sum, we have seen a difference in terms of response rates (a decrease) and in terms of prevalence rates of domestic violence (an increase) when the method of survey administration was changed. However, I do not know if the decline observed in other countries has also to do with the use of postal services or whether it is that people just do not want to respond to a paper survey, although they can actually fill a questionnaire online as well. They have the link in the letter. But I do not know. Perhaps response rates are higher when you do in-person interviews or telephone interviews.

Michael Levi: Thank you, everybody, for the very interesting presentations of this morning. Perhaps a couple of points of information: first of all, one of the unusual features of the British crime data is that the we also add information coming from the banks and from CIFAS (the UK's leading data-sharing Fraud Prevention Organisation), which is a non-profit body.[1] Those data are added to the crime survey data to constitute our crime statistics. That is a very uncommon feature. And it was added only after running reliability tests. The second feature that I would like to add to the England and Wales presentation, which was excellent, is that the National Cybersecurity Centre (NCSC) has instituted a new direct reporting system for reporting of phishing attacks: report@Phishing.gov.uk. Now there is an issue of demarcation between that and Action Fraud.[2] Action Fraud has received a lot of criticisms, and it is true that it is a very clunky system. On the contrary, the National Cybersecurity Centre system is very easy. If you get something that you suspect of being a phishing email, you just forward it to them and they do whatever they do with

1 www.cifas.org.uk.

2 'Action Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cybercrime in England, Wales and Northern Ireland' (www.actionfraud.police.uk/what-is-action-fraud).

it. There is no expected criminal justice outcome, and there is no compensation. There is no need to have an economic direct harm that is anticipated.

Hence, when we start adding these different sources – and paying attention to avoid duplication and overlapping – we can build a better picture. And I suspect that the National Cybersecurity Centre – which tries to intervene on the basis of the volume and nature of phishing to take down websites, for example – produces a better-rounded portrait, which can be combined with the very important data collected through the crime survey.

By the way, it was fascinating to hear the adaptation of the survey to the situation created by the pandemic. So, I just thought that I would mention these peculiarities of the UK system because they can inform us when thinking about how to measure cybercrime.

Now, only the Netherlands have a similar institution to CIFAS, although at a smaller scale. There are no other parallel organisations to CIFAS in any other European country. However, the banks, and the European card producers, could easily join a common reporting system.

Finally, about the trends mentioned by Stefano, I would like to say that I have just done a study – that is now published by the Australian Institute of Criminology[3] – looking at what we know about long-term trends in fraud, and that since the Spanish flu. So, it covers the last hundred years, looking at fraud, pandemics and economic crises. I have a small grant to continue that study. It would not be enough to do any statistical research of the kind that Billy beautifully outlined, but it is a small grant from the British Academy to look at economic crises, pandemics and fraud mostly in Europe since 1850. So that is a longer thing. [*Joking*:] We cannot re-interview people in 1850 for the recall survey, although that could eventually have been useful [*Audience laughs*]. So, there is a bit of academic work going on in this space. Thank you.

Stefano Caneppele: Thank you, Michael. So, there are a variety of institutions that are collecting different types of data on cyber incidents, including cyber fraud. Unfortunately, this information is dispersed and is getting a bit outside of the criminal justice field. In addition, more and more people are aware that the criminal justice system cannot do much when dealing with this kind of issue. Hence, the main conclusion here is that we should set up a sort of partnership between different countries and institutions to provide a more comprehensive picture of cybercrime.

Johan van Wilsem: Just a short contribution going back to your original question on the additional crime types that we could measure via crime surveys. I am not completely sure

3 Levi, M., & Smith, R. (2021). *Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19*. Research Report No. 19. Canberra: Australian Institute of Criminology. Available at www.aic.gov.au/publications/rr/rr19.

about the answer, but I think our main task at this moment is to figure out the best ways to measure the crime types that are already included in the surveys. And we should also discuss whether we stick to traditional victimisation survey questions or, to get answers as valid as possible, we take detours. Because the problem is that, when it comes to computer issues, I am not sure that everybody is perfectly able to assess what victimisation experiences he or she has gone through. That is why I think we need to do more work on the experimental field with respect to question wording. We need to conduct experiments on how to actually label our questions to respondents and see whether they need to be traditional victimisation questions or detour questions.

And in addition, I think much work has to be done as well in trying to understand what victims actually experienced. Developing reliable additional questions could give us more details on what happened to victims; for example, how much money the person actually lost. You can do that in a quantitative way, but also, I think, qualitative work – in which people just tell their stories – is very important. This kind of issues should be addressed in order to understand what the crime actually is about because, in my view, the field is lacking on that point.

Stefano Caneppele: Thank you, Johan. I have two more questions for you. Lieven Pauwels mentioned yesterday the difficulties in carrying out a panel survey due to the restrictions imposed by the General Data Protection Regulation (GDPR) of the European Union. I have seen that you started this panel survey in 2008: is the GDPR affecting your capacity to continue? Or under which conditions are you allowed to continue with the panel survey?

Johan van Wilsem: We are conducting this panel study through the LISS panel from the Dutch research institute Centerdata, and I do not think they have any serious issues with that. So, my answer to that question would be no. To be short.

Stefano Caneppele: OK, that is interesting. So, the GDPR could be an issue from an academic perspective, but not for a public institution.

The other question is related to your findings. You found a huge concentration of serious repeated victims. And you mentioned that the most convincing and consistent dimension to explain that phenomenon – the best predictor of serious repeated victimisation – was a lack of self-control. As you said, this raises the issue of how we can prevent it. It is a persistent rate, and it is almost impossible to change the risk of victimisation through some awareness campaign. So, did you consider or did you already set up any special programme? To your knowledge, is there any special programme in place to work on increasing self-control in cybercrime victims in the Netherlands?

Johan van Wilsem: No, not that I am aware of. If you are thinking on how to change levels of self-control in order to have more victimisation prevention, I think that would be a very hard task. And so, the question becomes: is there an alternative to that?

I think it would be worthwhile investigating if all these message warnings that are focusing on short-term outcomes – like 'if you click this button, then maybe this will happen' – are really an effective strategy for people who have trouble in seeing the long-term consequences of their actions. To me it seems not; and that means, in socio-psychological terms, that you would need to have regular reminders in order to warn people: 'This may cause harm in one way or the other.' That would be only a partial solution, but it is more feasible than changing one's level of self-control, because, again, I think that would be very hard to change other than by aging.

Marcelo Aebi: I have a couple of questions for Billy that are also related to the methodology of the survey: you mentioned that the Crime Survey for England and Wales was getting very high response rates – more than 70% – when it was conducted door-to-door. I was wondering how did you first contact the persons selected. Did you send them a letter announcing them that they have been selected? Because nowadays it is difficult to get people to open their door to strangers. Also, do you think that you will go back to the door-to-door survey after the pandemic? From what we have seen today, it seems clear that switching to a telephone survey leads to a decrease of the response rate. Perhaps that was not the case in the late 1980s and early 1990s, but it is in the 21st century.

Billy Gazard: Regarding the sample, it is a randomly selected household survey using a postal address. First, a letter goes out to potential participants, letting them know about the survey and that someone will be knocking on their door soon to interview them. That is how we recruit the sample.

Will we go back to face-to-face? When the pandemic started, our first thought was that it would produce a break in the series [*because the personal interviews were conducted on a continuous basis that allowed having national representative samples every three months*]. Consequently, we set up the telephone interviews with the idea of going back to face-to-face interviews as soon as possible. However, the longer the pandemic is going on, the more uncertainty around exactly when we would be able to go back to the face-to-face interviews in the field. Then it becomes more and more likely that we would not go back to face-to-face interviewing. And yes, there is an increased possibility of moving permanently to a different mode. I do not have a definitive answer yet. We do not know the future of the survey mode at this point, but definitely we are looking at all the possibilities and also thinking about how the mode impacts our response rates. I think that if we were to move to a different survey mode permanently – whether that is via telephone or online – we would really need to think about how we manage to keep those response rates up. If we do not go back to

knocking on people's doors to get them to participate, for example, if we move to a survey over the phone or online, we would need to find a way to go back to them and remind them to participate.

Marcelo Aebi: And who are the interviewers? Are they part of your institution or do they belong to an external company that goes door-to-door?

Billy Gazard: We have a private contractor who conducts fieldwork for the crime survey, and they have interviewers who, on our behalf, recruit for the survey.

Marcelo Aebi: And now, for the telephone survey, did you change company or is it the same one that provides the interviewers? Because the skills required from the interviewers are not necessarily the same according to the mode of interviewing.

Billy Gazard: We are still working with the same contractor. We thought about this issue – about the quality of the interviewers – and actually the face-to-face interviews on crime are conducted by a team that is separate from the telephone unit that does the telephone interviews. We actually transferred a lot of face-to-face interviewers to the telephone unit, to do the telephone interviews on crime. So, in most cases, we have kept the same pool of interviewers to conduct the interviews.

Session 3 – Rethinking Victims' Assistance and Deterrence Models

Which Assistance for Cybercrime Victims?

Ricardo Estrela[*]

First of all, I would like to present myself. My name is Ricardo Estrela, and I am the manager of the Portuguese Safer Internet Helpline. I am going to talk about the Safer Internet Helpline in a minute, but, before doing that, I would like to talk a little bit about other services that we also operate. Hence, you will understand what kind of services we had in place and how they allowed us to operate when we all went home due to the current pandemic, and mainly from March to May of this year. That allowed us to continue providing support to victims of all types of crimes and especially cybercrime victims.

So first, I would like to talk about the integrated system of support at distance, which basically is the service that integrates several means where people can contact us. Mainly, we have our European victims support number: 116,006, and with that we have all kinds of online services that help us to give support at a distance to victims of crime. We have the *victim support helpline*, *online support through social media* and *video calls*. And we also have a service called *Serviin*, a video service interpreter for sign language and the *Safer Internet Helpline*. Basically, at the victim support helpline, we try to inform, advice and support victims of crime, their families and friends through the provision of free and confidential support, mainly legal support and psychological support. And this service is connected to the local offices that we have at the *Portuguese Association for Victim Support* (APAV). So, it also serves as a number where we can refer, if needed, the victims to our local services, so that they receive a more specialised support. Then, I would like to talk a little bit – going a little bit off the topic, but I would like to talk – about the online support services that we have in place and this specific handbook that is called the *Talk Handbook*. The handbook was published in 2018 and gave us guidelines on how a victim support unit could or should give support at distance. And so, basically, since we already had these guidelines and best practices for online support, it was easier for us at APAV to face these times where we all had to go home, and especially when the state of emergency was declared in Portugal, it allowed us to maintain our services available and have different means for people to contact us and still provide support to crime victims. At the Portuguese Association for Victim Support website, you can find this handbook and you can download it for free. If it might interest you.[1]

---

* Portuguese Association for Victim Support. Additional material: the author's visual presentation is available at https://rm.coe.int/presentation-ricardo-estrela/1680a033b4.

1 https://apav.pt/publiproj/images/yootheme/PDF/Handbook_TALK.pdf.

What are the main means we use to give our online support? Mainly via Facebook, Instagram, Skype for video calls, and WhatsApp as a follow-up with our victims. To aggregate all those services – not excluding WhatsApp and Skype – we have a platform called *Client Skype* that allows us to have all the interactions that people do with APAV via social media in one place. This helps a lot to manage all the social media interactions that we have and all the kinds of requests that we receive. Here, I will talk about the requests for support from crime victims. It is a very important tool for us, because it allows us to already have some readymade messages regarding different types of crimes, and we can use them to start the conversation with the person who is reaching out to us. The fact that it is a centralised platform also helps us to have all the interactions in one place and not to be logged on different apps, which would complicate our job.

Then I would like to talk a little bit about our video service for interpreters of sign language. Basically, this is a service that is available on a web portal where a person who can only interact with sign language can ask for an interpreter to mediate the conversation between APAV and the victim who is reaching out to us. The person goes to this website and clicks on a link indicating that they want to interact with APAV. And then they start to talk with a victim support technician with the interpretation of a person from that portal who mediates or translates the conversation.

Going now to the main topic, I am going to talk about the services that are integrated on the distance support unit called the *Safer Internet Helpline*. Basically, at the national level, we are part of the *Portuguese Safer Internet Centre* that is constituted of different partners. We have the Foundation for Science and Technology; the Ministry of Education; the Portuguese Institute of Youth and Sport; the Altice Foundation, which is an ISP Internet service provider and the telecommunications entity; and Microsoft Portugal. In this consortium, APAV manages the victim support helpline, the Safer Internet Helpline. On an international and European level, we are part of the International Association of Internet Hotlines (INHOPE), that I am sure many of you already know. We are also part of the *INSAFE network*.

In the Safer Internet Helpline, we integrate two types of services: (1) helplines to help cybercrime victims, which is available from 9 a.m. to 9 p.m. on working days, and a platform. It is part of the fact that we are part of the INHOPE Association. (2) People can also report online material dealing with child sexual abuse or encouraging racism or violence, namely hate speech content online. Hence, through the helpline, we aim to assure free and confidential support to cybercrime victims, and we are talking about different situations: from cyber bullying to identity theft, and also online addictions, be it social media, video games and so on, and we provide technical help in promoting the safe use of the Internet.

Regarding our work as hotline analysts, and referring specifically to child sexual abuse material, as part of the INHOPE Association we are linked to a platform called *ICCAM*.

And we have a memorandum of understanding with our law enforcement agencies that enable us, as analysts, to assess child sexual abuse material, classify the content and flag these contents to our law enforcement, namely, our judiciary authorities. Because it is the law enforcement entity that is responsible for cybercrimes against children, and they have the specific authorisation to investigate these types of crimes. And at the same time that we flag this content to the judiciary police, we also notify the Internet service providers, if the content is lodged in Portugal, so that they remove the content. And we check whether the content is removed or not in three working days. If in the three working days we see that the content has not been removed, we once again notify the Internet service providers that they have to do the removal of the content. Now, here in Portugal, things are a little bit different because Portuguese Internet service providers, when they see this kind of content or if they are informed by some entity – like ourselves as hotlines – about such illegal content, they are obliged by law to remove the content in 24 hours. So, we have another way to make them comply with the removal of the content. But in practice, based on our experience, when there is child sexual abuse material, the Portuguese Internet service providers remove the content. So here, in Portugal, we do not have a lot of troubles with that. However, most of the content we assess is not lodged in Portugal. So, we end up notifying other online partners for the removal of the content.

We have another important tool to help cybercrime victims, and that gives or makes our job a little bit more specialised: as a helpline, and being part of the INSAFE network and the INHOPE network, we have the status of *trusted flaggers* in important platforms; for example, TikTok, Facebook and YouTube. The INSAFE network and the INHOPE network are part of the upper and trusted flagger channel, which enables us to have the content pre-emptively removed. Now here, in Portugal, we are noticing a significant increase of self-generated content, mainly from teenagers, and this ends up in adult websites. And these platforms help us a lot in our work by having the content removed and removed fast. For example, social media outlets like Instagram or Facebook help us a lot in the removal of hate speech online, which unfortunately with the current situation has been proliferating a lot on different social media applications.

Another topic that we are concerned with, as a victim support helpline, is on awareness-raising campaigns that we launch with the aim of having a national impact. Last year we had the *Portuguese Safer Internet Helpline campaign*, which basically aimed to sensitise people about the importance of the reports of illegal content. And two days ago, we launched another campaign in Portugal on awareness of cybercrime. You can see the images in the PowerPoint presentation. Basically, it deals with two situations. If I can translate freely from Portuguese, one means 'When Catherine married Gustavo, she thought she would be *www.happyforever.com* and not *www.nakedonthewebforever.com*.' We bought these domains [in portuguese], and when you click on one of them you are redirected to a website where you can see some strategies and some ways to deal with non-consensual

image sharing. And lastly, we also have a campaign called *Respect Battles regarding Hate Speech*, and I thought it was important to present them because we see a lot of this kind of hate speech now in social media. Thank you.

The Internet Organised Crime Threat Assessment

Nicole Samantha van der Meulen[*]

Good afternoon, and for those who are in a different time zone, good morning, and good evening. My name is Nicole van der Meulen. I am the head of the policy and development team at the European Cybercrime Centre at Europol, also known as EC3. And within the next 15 minutes, I would like to provide an overview of our Internet Organised Crime Threat Assessment [*IOCTA*] and talk about the various threats that have been witnessed by law enforcement as well as by our private sector partners. Those who may not be familiar with the IOCTA, we have published it seven times now. This was the seventh edition, and it came out about three weeks ago. Before I continue, it might be good to also say that within the European Cybercrime Centre, we focus on different forms of cybercrime; for those who are not familiar with EC3, it is cyber-dependent crime and child sexual exploitation and abuse material, as well as non-cash means of payment fraud. And we also have a dark web team and a cyber intelligence team.

How do we conduct the IOCTA? For the last 6 years, we have sent out surveys to the member states and third-party countries asking them about developments over the last 12 months in different areas of cybercrime. We would have one survey per cybercrime area. For this year, we wanted to take a different approach, so I suggested we conduct interviews, which is what we did. Basically, I conducted semi-structured interviews of member state representatives, of Europol internal colleagues, and of private sector representatives from our advisory groups. We have advisory groups in three different areas: financial services, Internet security providers and telecommunication providers. The important thing about the IOCTA is that it is really a document that aims to provide a law enforcement-centric perspective of the threat landscape. And like I said, we complement it with private sector input to make it as comprehensive as possible. The idea is that it can serve multiple purposes. It is obviously a public document; so, everyone is welcome to read it, and it is accessible on our website.[1] But it also tries to help set priorities for law enforcement itself, in terms of what the main threats are and what LE should focus. We also identify a number of challenges for law enforcement in its fight against cybercrime.

---

* Europol. Additional material: the author's visual presentation is available at https://rm.coe.int/presentation-nicole-samantha-van-der-meulen-europol/1680a033b3.

1 www.europol.europa.eu/publications-events/main-reports/iocta-report.

What are some of the main developments that we witnessed this year? Basically, the reporting period we take is from June 2019 until June 2020. And we conducted the interviews between April and June 2020. So, in terms of the threats that are going across the different crime areas, there was not that much change. The main threats we face are in the area of social engineering, malware and especially ransomware. These are considered the top threats. When we ask law enforcement for threats, we do not specify between citizens and businesses, so some of these are more focused on citizens and some are more focused on businesses and some concern both. And I think when it comes to social engineering, malware and ransomware, they concern both. Although I will speak about ransomware a bit later on, where it is presently a larger concern for organisations, both public and private.

We also looked at what we call *crosscutting factors*, and one of those is crypto currencies. And what is important here is that even though we, from a cybercrime perspective, really look at criminal abuse of cryptocurrency, cryptocurrency is really a facilitator of other types of crimes as well. So, it does not exclusively focus on cybercrime. Of course, it is largely connected to ransomware, because when criminals attack their victims and take the data hostage, they want to be paid often in Bitcoin or another form of cryptocurrency. Crypto currencies are also very common when it comes to dark web transactions. But at the same time, when it comes to, for example, kidnapping cases or other types of physical or traditional crimes, criminals also use crypto currencies. Another crosscutting factor was really that law enforcement wants to provide a comprehensive overview, but there are a lot of challenges when it comes to reporting crime. They were very transparent and open about the fact that they are aware that what they have in terms of crime reporting is not necessarily an accurate reflection of the number of crimes taking place and the number of victims. What is important there is also that, when it comes to larger cases, for a victim, it might just be one report, but of course, the more victims who report a crime, the more information law enforcement gathers and the more likely it is for them to actually connect the dots and see which perpetrators are behind those different successful attacks.

And the other part, of course – which I am sure you have spoken about as it is also the title of this conference – is: *how criminals took advantage of Covid-19?* I think it is very important to mention that Covid-19 did not necessarily introduce new forms of cybercrime. Rather, it exacerbated existing problems, in the sense that there were many forms of cybercrime that we had witnessed before. But criminals change the narrative. So, they obviously took advantage of the vulnerability of people who wanted more information about the pandemic, about the virus. They took advantage of the fact that many people were in need of supplies to protect themselves, such as medical supplies. And at the same time, it also really opened up new opportunities because many people who may not have been doing anything online prior to the pandemic had to go online because of the physical restrictions. And these people may not have been well prepared to avoid certain criminal

attacks, like social engineering, and became basically easy targets. Another important element was, of course, that because so many organisations had to move their business online or had to have people working from home, they had to temporarily alleviate security measures in order to facilitate teleworking, which also created additional vulnerabilities that criminals could take advantage of.

So overall, what is very important is that the central theme of the IOCTA this year, and I think that really goes for cybercrime in general, is that it is an *evolution*, not a *revolution*. Many of the threats that you will hear about today, or that you will read about in the IOCTA, also featured in it in previous years, for example, last year. That does not mean that cybercrime has been standing still. It means that there is indeed constant change, but it is at a much lower level. Criminals might change the infrastructure, they might change something in their code, but, fundamentally, the type of attack stays the same. And it also demonstrates how persistent it is and how difficult to counter. What is also important is that we are facing a very wide spectrum when it comes to the type of perpetrators. There are those at the top-end who are extremely professional and are enhancing that level of professionalism. And at the same time, we are also dealing with cybercrime as a service, which makes cybercrime, of course, very accessible for people who might not have any technical skills, but who have a little bit of money to, for example, rent a botnet or take care of a DDoS as a service and take a subscription on that. So those are just things in the context that are very important.

What we usually do is that we have key findings for a crime area. I said social engineering is a top threat, but it goes across different crime areas, because sometimes it is also a preparatory action, in the sense that it is what criminals do to gather information, to subsequently carry out another form of cybercrime. We see it returning in terms of phishing, business email compromise (BEC), CEO fraud, but it can also be a preparatory action for ransomware, for example. I spoke about cryptocurrency as well as about the underreporting, creating an inaccurate or incomplete overview. What I also must say in that vein is that law enforcement also indicated they had challenges within their own system, in terms of how they register different crimes, and that, of course, also influences the ability to provide an accurate overview of the prevalence of certain cybercrimes. I think we should definitely look deeper into how the different countries approach these questions. And I think that it is also, of course, a large part of this conference. And the final thing is the technological development. This is where we look into challenges for law enforcement in terms of combating cybercrime. We often speak about encryption, which makes it extremely complicated, sometimes even impossible for law enforcement to get access to critical evidence to be able to execute a criminal investigation. But there are other developments, such as 5G, such as artificial intelligence, which also influence the work of law enforcement and will especially do so in the future.

The cyber-dependent crime indicated, that is, ransomware, was a top threat. What has changed with regard to ransomware is that, as we previously noticed, it is more targeted. So, perpetrators really engage in what we call victim reconnaissance, in that they identify targets, for example, victims who are more likely to pay and who have the ability to pay. They also target third-party suppliers, which means that this can have a chain effect in a supply chain, because many companies might be dependent on that third-party supplier and it can also have an effect on critical infrastructure.

Malware is in general one of the top threats. And what we really see is that there are some forms of malware that are so refined and sophisticated that it is extremely difficult to counter, because once a certain version of malware is detected, they will refine it further, making it even more complicated for antivirus software, for example, to detect. EMOTET is the top form of malware, so to say, the most complicated, the most prominent. And what we see there is that from the private sector's perspective, there are over 200,000 unique versions. And that just demonstrates the diversity and the complexity of such a threat.

When it comes to distributed denial-of-service attacks, it is also more targeted, increasingly adaptive. But here we also indicated that it is a threat that has a lot more potential than what it might actually have demonstrated over the last 12 months, and also what we have been witnessing more recently. So, after the publication there are reports indicating that perpetrators are combining ransomware and DDoS to enhance the pressure. And the other thing that ransomware perpetrators do to enhance the pressure, and which we have witnessed over the last 12 months, is that rather than exclusively taking the data hostage and asking for the ransom, if the company is then unwilling to pay that ransom, they are now threatening to auction off the data they have managed to gain access to. This means that they are exfiltrating the data and are enhancing the pressure for the company to pay, because auctioning off that data could mean the company would most likely be exposed to further types of cybercrime, because criminals would buy that data and then carry out other crimes. And it might also make the company or the organisation more vulnerable to further actions under the General Data Protection Regulation (GDPR), since that would be a compromise on that data.

In the previous presentation of this conference, Ricardo Estrela already spoke about a major area of concern, especially when it comes to developments with regard to Covid-19: we receive a lot of referrals about materials of child sexual material, including self-generated material, of course, and there are really more referrals than law enforcement can cope with. We see that offender communities are obviously cooperating a lot to make sure they stay under the radar, out of reach of law enforcement. And another large concern was that the livestreaming of child sexual abuse, as far as we could notice, has increased and has become more mainstream also in part as a result of Covid-19, in the sense that offenders could not travel and then went to livestreaming as an alternative. What was really disheartening is that even though it is most prominent, as far as we know, in the Philippines,

it is not exclusive to the Philippines, and we even had a case in Romania, and we are not sure to what extent there are more cases when it comes to livestreaming in Europe.

In the area of non-cash means of payment fraud, there were a lot of things continuing, but also a lot of new things were introduced in the document after receiving many reports on them. The steep rise in the area of what we call SIM swapping is an example. So, the criminals basically approach the telecommunication providers in order to get a new SIM card in the name of the victim and, within the span of one hour, they would use that in addition to the other information they have gathered through social engineering to gain access to the victim's bank account and managed to withdraw all the funds. Another area that is worth highlighting, I think, is the increase of online investment fraud, because there are so many victims of that type of fraud, a lot of reports to the police, and there is a wide diversity in terms of how much damage those victims suffer. Some lose their entire life savings, and there are very limited opportunities to help those victims. So that is really an area where prevention and awareness have to be key in order to educate people to understand that they are actually dealing with a fraud. It often occurs with regard to cryptocurrency but also gold or diamonds. There are advertisements of investment opportunities, and, subsequently, people give their money and obviously lose everything. Card fraud is something that continues to increase also because there are obviously a lot of data security breaches, there is a lot of information, credit card information about potential victims available. That is basically almost a business on its own.

Those are the key findings in the different areas, and there is also more detailed and in-depth information in the IOCTA. Phishing attacks are very prominent, also connected to the broader issue of social engineering. And even though not all phishing attacks are necessarily particularly sophisticated, we do notice that perpetrators have really improved their messaging, even in terms of improved language. We spoke to a number of countries, but they say it is really difficult for victims to distinguish between a phishing message they receive from a foreign criminal and one from a native speaker, and this even for less 'popular' languages.

Also worth noting is that we see threat actors share knowledge to enhance their operational security, and they also share knowledge to really basically educate their colleagues, to say it in a bit of an odd way. And that just makes it all the more complicated for law enforcement to counter the threat of cybercrime. And I have touched upon the reporting challenges, which is something definitely worth looking into, also because the number of crimes reported can be a justification for the resources needed on the side of law enforcement.

Now, in the area of recommendations, we have put them into a number of categories that we usually focus on. It was also emphasised that *cooperation is key*. And that is especially so because of the transnational nature of cybercrime, obviously; so, different pieces of the puzzle are within different countries. And as Europol, of course, we are here to facilitate

bringing all those pieces together. That is a key role. We have the *Joint Cyber Crime Action Task Force* for that, but we really tried to sort of look into ways into how we can enhance that. Such coordination is also definitely necessary at the national level, and it is also necessary in conjunction with private sector representatives, because this cannot be done alone by law enforcement or by public sector partners. Information sharing is key, and it is very important there to have trust and acceptance. So, not naming and shaming, especially if, for example, an organisation has fallen victim to cybercrime; it is important that they feel comfortable sharing that, because that facilitates learning and it also helps other organisations to be better prepared for a subsequent attack. Prevention and awareness – as it was mentioned by our colleague Ricardo Estrela who spoke before me about the Portuguese experience – are really important. We try to do what we can. We have a number of campaigns. I have not listed them here, but of course, I will be happy to follow up with anyone who might want more information. It is also already available on our website. We try to do it, whenever possible, in multiple languages to ensure accessibility of different target audiences in many different countries. I think *No More Ransom*, which is both prevention and victim assistance, is the best example. I think we are up to 36 languages now. And the idea there is that we give advice to prevent victimisation. But at the same time there is also victim assistance by providing decryption keys of a number of versions of ransomware, a number of types of ransomware. So, we always advise people that, if they do fall victim to ransomware, they should check *No More Ransom* to see if a decryption key is available, because that will basically allow them to decrypt, to free their data again from the criminals. And finally, capacity building is, of course, key for us. Not just for law enforcement officers who are working within cybercrime, but also for those working in other forms of crime, because almost every form of crime will now have what we would call *a cyber component*. And it is critical for them to be aware of that and to know what to do with that.

Counting Cybercrimes Reduction: Deterrence, Diversion and Desistance

Michael Levi[*]

Today I am going to take you through a number of different areas in the understanding of deterrence, diversion and desistance from cybercrime. The first point I am going to make is that, very often, government strategies – not just my government, but other governments, too – involve adapting counterterrorism control models to all serious and organised crimes, including cyber-enabled crimes. And my aim here is to re-examine public policing and public-private partnership policing to consider what may be required to 'satisfice', and the world *satisfice* may be strange, to *satisfice* by balancing different interests: cybercrime reduction and harm. Reducing victimisation, repeat victimisation and fear of cyber scams.

And the first key takeaway I want to make as a proposition is that *nobody* I have met over the last decades in authority believes we can prosecute our way out of any online crime. But the public often wants justice, and it sometimes wants retribution. So, we need to bear that in mind: that there is a problem of managing expectations that is very important here. And trying to bring people along onside is part of what a modern government needs to do.

I will also summarise key features of deterrence, diversion and desistance from cybercrime in the knowledge that our criminal career data on cybercrime is very, very poor. So, we must not be too confident in asserting what we know, what we do not know or what is promising. And this is because of the dark figure of unreported crimes and, as various speakers over the last day-and-a-half have said, because of unprosecuted offending, because of the attrition rate. Alexander Seger, for example, mentioned that a tiny percentage of cybercrime ever get dealt with by the justice system. Plus, there is the particular problem of the cross-border dimensions. In other words, if the offenders are in China or in Russia or in Romania – even if two out of three are member states of the Council of Europe – what is the realistic chance of getting the offenders being brought to justice: either extradited or prosecuted in their home state? And this is a controversial area.

In my opinion, when we think about what is going to happen to offenders, we need to take account of civil and administrative sanctions, because we cannot just rely on criminal

* University of Cardiff, UK. Additional material: the author's visual presentation is available at https://rm.coe.int/presentation-michael-levi-truly-final-coe-cyber-evidence-beyond-cjs/1680a033b2.

convictions and sentences. We need to look at other methods of *dealing with crime*. I am not going to expand on this very much, but the counterterrorist model my government has been working on, and which is also applied, passes on the 4 Ps: *Prevent, Pursue, Prepare* and *Protect*. But this is just a typology; it does not tell us anything about what to prioritise.

And one of the things which we need to remind – I think Nicole van der Meulen said it before – is that sometimes, with organised crime, some organisations are exposed to a very large amount of drama. For example, ransomware: if a hospital is threatened, if ransomware is stopping a hospital from functioning with all its processes, that is very dramatic. But most things are low drama, and the reality is that they are not even pursued even in legality principle countries, where there is an obligation to prosecute.

I am not going to spend much time on it, but the *Eurobarometer Special Cybersecurity Survey* gives us some data on people who experienced different sorts of online crime, and you get different levels, and it tells us also about repeated victimisation. Well, what is being done about this is not particularly promoting in the UK, and I just happened to be there.

But there is a lot of preventive activity going on, and a lot of it is developed by the private sector. And the private sector is selling prevention, and it is also selling fear; because unless you make the public afraid, you do not get them to buy your product. So, it is selling protection services. And there is a market failure. You do not know which services are better or worse in prevention, because the public authorities do not like to say: 'Well, do not use this method of protecting yourself because it is not very good,' because then they will be criticised. Then there are a lot of police initiatives to deal with this stuff. Obviously, every country has its own way of organising its policing. Ours has become more 'nationalised', but it is still not that centralised. There are still a lot of individual forces as well as the central ones. Public-private partnerships are very important. And there are some explanations for poor cooperation, among which: it is difficult to justify a business case for spending in austere times like now; companies usually want to wait for a while before spending money on prevention – they need to experience the pain. But we also have a crisis in the justice system because the police do not value fraud and digital crime very much, except for child sexual exploitation online, which is very much prioritised, and except for those forms of digital crime that are really national security issues.

So, we have a lot of crime competing for very little police resources. And the result of that is that we have comparatively few prosecutions. So, what do we mean in Europe when we talk about 'effective, proportionate and dissuasive' sanctions? I do not think this means a lot. It is just a ritual phrase that European institutions, on some of which I am represented, use for documents and staff. It means: we take this seriously.

What is the role for *prevention* – that is, trying to stop people from engaging in pathways to crime – in reducing willingness to participate and, for that matter, in increasing

whistleblowing? The main areas we have for this are money mules and hackers, where we do try and stop people from getting engaged in cybercrime.

Incapacitation: it is acknowledged by the European Union, and the Council of Europe sometimes, that putting funds beyond use by asset freezing and confiscation is not working as well as it should do, particularly in the post-conviction phase. And *deterrence*: we need to clarify deterring them from *what.* I have given some examples of different levels, but we need to differentiate the organisational from the individual impact of deterrence. When we see companies losing data on their customers time and time again, and the individuals being scammed time and time again, then we have to think: well, we need to worry about what the impact is, both on offenders and victims, of the actions we are taking.

Now, really, the risks of detection and intervention are more important than the level of punishment; but for highly profitable crimes, we need to consider other rational-choice factors. For example, the very low prosecution rates for all online offences. Take fraud: I have talked to enough of that, I think, but there is a special category of possessing, making and supplying articles for use in fraud that is an important area to sanction. Now online hate, some cyber offences and national security threats tend to get most of the attention of most cyber security units.

The English Sentencing Council did a survey asking people what they thought were the most aggravating features of online crimes. The Council has yet to finalise any recommended sentences, but there are important things in the survey's report, showing what the public feels and stakeholders feel are important in aggravating.

So, I now turn to some of the approaches that are taken. *Mentoring*: normally we have reasonable evidence on mentoring, on different ways of dealing with offences, but in cybercrimes we do not. And that is because little is known about the profiles of cyber offenders. We know from other forms of delinquency that some people can do very big crimes when they are very young and then mature out. Is that different for cybercrime? We do not know whether cyber offenders mature out. Europol and Interpol say, and there are some examples of this, that people turn to making money after just doing things for the excitement. But we do not know how generally true that is, and we cannot know because we do not know most cyber offenders. Some malicious cyber offenders do have histories of family and adjustment problems; but, compared with other types of offenders, they are less linked to routine exposure to violence, abuse, drug and alcohol use, or having parents in jail. And cyber offenders are more likely to show narcissism, anxiety and depression, as well as lack of empathy and ethical flexibility. Maybe they are like some politicians, [*Ironically:*] not in Europe, of course [*Audience laughs*]. So, they are mentoring at present, facing different challenges from mentoring for other offenders. And we do not know whether getting them to work with past cyber offenders – who we believe have gone straight – is really a good thing or not.

What about targeted warnings or cautions? Now, the intention of targeted warnings is to deter those who get them from beginning or continuing offending, by explaining to them what the harm is of what they have done and what the cost to them will be. For example, we are warning in this country people who engage as money mules in money laundering schemes:

> This could affect your credit score, it could stop you getting a mortgage because there will be a black mark on your credit score; and so, there will be a consequence if you continue down a criminal pathway.

So, we try to avoid stigma and the economic consequences of a criminal record and saving prosecution and court time, especially during Covid-19. There are also sanctions that focus on the wrongfulness of behaviour and the harm caused by it rather than the characteristics of the offender. Those are more likely to reduce crime. Targeted warnings can prevent crime if the person who receives them believes that the warning is fair, that the police officer or civilian who delivers the intervention is acting rightfully, and if the intervention is focused on the act rather than the actor, that is to say, on the behaviour rather than the person. There is a lot of research about the legitimacy of interventions for other types of crime. And although targeted prevention messaging has been used in the context of cybercrime, we cannot really say with a great deal of scientific certainty how effective they are.

I will give a couple of UK examples. In 2014, there was a police investigation into *Blackshades* – a remote tool to steal information from personal computers – and 17 people were arrested, 80 received a visit from a police officer and about 500 other people received a warning letter advising that it was believed they had purchased the software and that using it could be illegal. Now, the police, both in Britain and in other countries, for example, the Netherlands, and Europol, and so on, have been learning from these experiences. Another example, in 2015, the database for the *LizardStresser* booter service – which provided DoS attacks for a fee – was compromised and leaked, containing customer details for those who had purchased attacks. Six purchasers were arrested. Fifty others who had registered with the site, but were not believed to have carried out an attack, received a home visit from the National Crime Agency, and were told that denial-of-service attacks are 'illegal, can prevent individuals from accessing vital online services, and can cause significant financial and reputational damage to businesses'. They were also informed that 'committing cybercrime can result in severe restrictions on their freedom, access to the Internet, digital devices and future career prospects.' So, these are the kinds of messages that were put out by the National Crime Agency which believes that this is quite effective. And the truth is that we do not have the resources to prosecute all those people anyway.

So, this area of behavioural economics in the penal system is becoming more and more important and popular in this field.

Europol coordinated another operation, and again, a lot of people were interviewed and cautioned rather than prosecuted. Now, many types of cybercrime are committed for money or peer recognition, so well-targeted cautions that increase offenders' perceived risks of detection could work: like, you know, 'We are watching you' pop-ups on screens. 'Are you really sure you want to do this? This could cause harm,' but these things have to be assessed to see whether they are legal in your jurisdiction.

We know that the likelihood of detection matters to a lot of cybercriminals. So, warnings highlight to low-level offenders that they are not so anonymous as they think online. However, care needs to be given, since personally administered warnings about behaviour that is seen to be legitimate may generate defiance and more delinquency in the future. It could be counterproductive if we are not careful.

What about *positive interventions*? Regarding *diversion*, the evidence is weak for cybercrimes. We might try to say: 'well, you could be rich like Banksy if you engage in legal urban art rather than illegal graffiti'; but some evidence shows that this is counterproductive, for example, with car thieves. It just does not work. So, there is no empirical evidence conclusively proving the effectiveness of positive diversions in cybersecurity. I mean, some prestige cybercriminals have become consultants, but there are security clearance issues and security risks that may make it difficult to obtain support from industry or police for such schemes.

It is a challenge to keep offenders away from negative online influences. And I think we need to challenge the justifications used by cyber offenders through moral reasoning and cognitive restructuring. But nobody knows how this works and does not work in China, Romania or Russia. And there is some evidence: we did some research with Nigerians, and Nigerians really did not care about the harms they were doing, not either in the *rich West* or at home, because many Nigerians do online schemes against other Nigerians as well. So, we need not be too optimistic about this. And desistance evidence depends on good data about cyber careers, which we do not currently have.

So, to try and wrap up: we need to think about efficiency, effectiveness and legitimacy. There is a risk of confusing effectiveness with efficiency. And one of the challenges for the government, the police and the judges – that is, for people who want to nudge to change our behaviour – is that they have to convince the general public and business that these crimes affect them personally. We know they do in the abstract, but it is hard to operate this. As Nicole was saying, we need to focus on *resilience*. And that is a cultural shift that is quite difficult and needs to be repeated.

So, if we think about this round, we get some models for action. The trouble is that the targets are so widespread. We need more understanding of teachable moments to divert offending. Can we do this credibly overseas? Perhaps not, but we can do it at home with

cyber offenders. When is the right time to think about really persuading them? 'This is bad stuff and you should not do it.' Prevention – the Estonians have shown the way – needs to be built from the ground up, through peer groups, community-level bodies and charities. And it needs to be easy: to expect us to do sophisticated stuff – I mean, it may be okay for big business – but it is unrealistic.

And as Europol and member states try and do, we need to look at take-downs of websites, botnets and dark markets to reduce harm. But most of them rapidly re-emerge. Even if, as has happened, you can destroy people's trust and their credit ratings on the web. There is a lot of scope for experiments, warning pop-ups on the screen for those who have fallen victim to offers that could have been fraudulent or fake. But we need to avoid bad publicity for this, to plan this very carefully and in theory. More focused Internet governance could deal with these global bads, but it is very difficult to get international opportunity reduction, just as it is very difficult to get international harmonisation of cybercrime statistics. So, I agree with Nicole's comments on the previous session. We need to try and encourage clusters of countries, perhaps not everybody at the same time, to do so. And show other countries that keeping better statistics on cybercrimes and cyber offending can lead to more effective and more rational control strategies, because one thing is for sure: this is not going to go away. We are going to have to live with this far longer than we are at living with Covid-19, I hope. Thank you very much for listening.

Rethinking Victims' Assistance and Deterrence Models: A Panel Discussion

Nicole van der Meulen, Ricardo Estrela, Michael Levi, Fernando Miró-Llinares, Stefano Caneppele and Marcelo F. Aebi

Marcelo Aebi: We have had three presentations covering very different ways of looking at cybercrime, from the assistance provided to the victims to the potential ways of deterring offenders. Now we have the time to discuss them and perhaps to have also a general discussion about the topic of this conference.

Stefano Caneppele: I have a question for Nicole van der Meulen regarding the coordination of Europol with all the European partners. My question is, have you already discussed the standardisation of the reporting system in terms of cybercrime typology? Because I am aware that it is not the main goal of Europol to focus on statistics. But the problem is, as you said, that if we do not have an idea of the extent of the phenomenon, it would be difficult to justify the need for new resources. So, my question is, is there any reasoning going on about the standardisation of some type of cybercrime across the member states of the European Union?

Nicole van der Meulen: Yes, as far as I know, there has been an attempt in terms of trying to put it on the agenda. From the feedback I received during the interviews for the IOCTA, I am not aware of anyone trying to move further along. I am thinking on how to approach this. I think it would be a bit complicated to go sort of from – I do not want to say zero – but to go from what we have now to a standardisation. How can we standardise it?

I would say, but this is very preliminary, that we should look into a few countries to see how they are doing it, to see the different models before moving on. It will be quite a long process, and I think we might follow up with some countries who have specifically mentioned that they are looking into it themselves to learn from their experience and go along with their developments. But as far as I know, no serious progress has been made in this area. I think that is because it is a very challenging issue, and the way to approach it is maybe not to expect too much in the beginning, but to see how we can at least get some insight into how these systems work in the different countries.

Marcelo Aebi: I would like to ask Ricardo about the profile of the persons who ask for help. Do your statistics show an overrepresentation or an underrepresentation of specific categories of victims, for example, in terms of age, gender or ethnic background?

Ricardo Estrela: We have weekly statistics from last year that cover both the helpline and the hotline. In terms of age, the vast majority are grownups. Young adults and adults from 25 to 50 years old, and they are mainly males.

Since the beginning of the pandemic, we have observed a new trend. We have lots of reports regarding sextortion cases, mainly through sextortion emails. I do not know if you are all aware of these sextortion emails. Basically, that comes from data breaches, and people ask us if the threat is real or not. We have lots of calls regarding that.

And picking up on the cyber resilience theme, I would add that we do not see a raise of awareness about the cybersecurity measures that we should all implement. What we see in Portugal is that a lot of people do not implement simple things, like changing passwords. The cases of sextortion come mainly from data breaches originated by the leaking of passwords. Even though people receive warnings about the fact that their passwords are very old, they do not change them. And hence they lose access, for example, to their Gmail accounts, because cybercriminals try to gain immediate access to the most used applications. So, there is still a lot to be done in terms of cybersecurity measures that we could all take.

Marcelo Aebi: Thank you. Well, perhaps that majority of male victims means that males are more often connected than women to risky websites. Or perhaps the campaigns that you are making do not reach women. I mean, do you think your statistics show something similar to the real distribution of the phenomenon or are they biased somehow?

Ricardo Estrela: I do not think they reflect the reality. For example, we have a big dark figure among adolescents and infants that do not reach out to us. This year we made a campaign in schools, because we know that there are a lot of situations of cyberbullying and non-consensual image-sharing among adolescents. And they do not reach out to us because there is a lot of victim-blaming in the cases of non-consensual image-sharing. The idea that victims are to blame is unfortunately still there, and so, they feel too ashamed to come out and ask for help. In fact, most of the cases that come to our attention arrive through someone else, for example, a peer who knows about the situation and reaches out to us, asking for information to help a friend. And then we can reach to the victim. There is a lot to do, and we still need to change minds regarding this situation.

Stefano Caneppele: I also have a question for Ricardo. From a European perspective: is there any European network of NGOs dealing with assistance to victims of cybercrime? A place where you can share experiences and exchange practices? If that is the case, have

you made comparisons about the profiles of people who have access to your hotlines or your platforms?

Ricardo Estrela: Yes, there is a network called INHOPE,[1] specialised in children, and one called INSAFE,[2] specialised in children and young people. I cannot tell you how profiles compare because my specialty is not statistics. But I can tell you that we share with INSAFE every three months all the information regarding the contacts that we had on the helpline and the hotline. Then INSAFE usually produces annual reports showing the profile of the victims and the persons who contact this kind of lines in different countries. We all follow the same categories; so, in that sense, it is uniformed. Please keep in mind, as I said before, that our helplines do not deal only with cybercrime, but also with other troubles, like only addictions.

Marcelo Aebi: I have a question for Michael Levi. Mike, you managed to make a wonderful presentation about a very complicated topic. It is extremely difficult to make generalisations about deterrence and diversion from cybercrime, because there is a wide diversity of cybercriminals.

Let us take the example of a hacker: usually, when you stop smoking, for example, or when you are trying to lose weight, the experts tell you to put away everything that could tempt you. They tell you not to have cigarettes at home, or not to have a lot of food in your fridge. But, for a hacker, in today's world, how can he live offline when everything is happening online? And of course, as for any bad habit, it is extremely difficult to quit when you are exposed to the risk. How do you see this?

Michael Levi: Yeah, that is a very good question. [*Joking:*] I remember my father said to me when I was 16: be careful with women, as I had, you know, a similar kind of problem; but it was easier because I was at a boys' school [*Audience laughs*]. The only thing I can think of, directly related to this, is that when we look at research on child abuse, for example, physical abuse; one of the differences between parents who beat their little children – and I am talking about children under two – and the rest of the parents is that they have distorted perceptions of the babies and what you can expect from them to do or not do. And the ones who had crying babies but did not hit them were people who learned cognitively to switch off. Mentally, they thought of their favourite Elvis Presley song, their favourite Freddie Mercury number, their favourite Bach cantata, as a way of diverting themselves mentally from the stress that the baby was giving them. And this is one of the findings that some cognitive psychologists have looked at. So, learning to divert. [*Joking*:]

1 www.inhope.org.
2 www.betterinternetforkids.eu.

You know, you can keep that packet of cigarettes, Marcelo, but just do not smoke [*Audience laughs*]. [*Ironically*:] Yeah, as Nancy Reagan used to say about drugs: *Just say no*. But you better divert yourself mentally by thinking of some positive thing, a holiday that you had, how innocent the baby is, or it is not their fault. And so, there are those sorts of techniques of mental diversion, which might be a useful thing to think about. I have not seen this written about. I am just suggesting this because it has come to me, as you asked the question. But you are right about the ubiquity of the cyberspace. I mean, some offenders as part of the sanction are told that they are not allowed to have a computer at home. But, yeah, you can maybe do like Kevin Mitnick [*Note from the editors*: a convicted hacker who became a computer security consultant]. But, you know, that is not a realistic thing given the scale of what we are talking about. So, I think we should probably focus on switching off mentally from temptation. That would be one kind of thing to do.

Marcelo Aebi: That is very interesting, and it reminds me of research on memory conducted by neuroscientists. Studying how false memories work, they discovered that reprogramming memories can be an effective way of dealing with posttraumatic stress disorder. This was presented by Jeremy Grivel and Yves François at an annual meeting of the *alumni* of the University of Lausanne; in 2016, I think. They mentioned the case of a kid who saw his brother fall from a tree and get seriously injured. As an adult, this recollection haunted him. He could not support seeing his own kids climb a tree. The treatment consisted in helping him associate the original memory to something different. Whenever the memory re-emerged, he would think of Spiderman, who of course does not hit the ground when he falls. And somehow it worked. The memory did not disappear, but it was mixed with other images and became less vivid and more bearable. This is similar to what some psychologists do, with the difference that neuroscientists can also distinguish the parts of the brain involved in a real memory and in a false memory.

Michael Levi: Like cognitive behavioural modification, and mindfulness of different kinds. [*Joking*:] Of course, Spiderman was dealing with web crime, so it is very relevant to online crime [*Audience laughs*].

But yes, I think there is a need to be more creative in this process. We might have to have different models. In your case, they were dealing with it as a victim, but you may need a different model for an offender. Oscar Wilde once wrote *I can resist anything except temptation*, so we need to move away from that in dealing with offenders. Otherwise, it becomes like science fiction episodes. We need a lot more creativity.

And I am not being too depressed about the criminal justice system, but it is obvious that 99.99% of these people will never enter the criminal justice system. So, we need to think about this as a general *social harm reduction model*. It does not mean that criminal justice measures are not important, but we need to approach them – to approach the

messaging from prosecutions and from sentencing – in a much more creative and systematic way than we usually do.

Marcelo Aebi: I totally agree. Without creativity, we will remain in the hands of the pseudo-experts who keep repeating over and over again that education is the key to crime prevention, as they had done for several centuries. Yes, of course, but what we need now are concrete interventions. Yours is a very concrete one, which could be tested.

I also have a question for Matti: I was surprised when you said this morning that you are going to use the cybercrime module in the Finish victimisation survey every four years only. Isn't that too long?

Moreover, currently it is extremely difficult to separate the digital world from the physical world. I am not adopting the extreme position of those who say that adolescents can no longer make the difference between them; but, being realistic, both worlds are interrelated all the time, and we are jumping from one to the other, and you are going to ask these questions every four years only?

Matti Näsi: The main reason is that we are using the national victim survey, which has two basic modules: one about violence and one about property crime. The third one is a module that varies every year. One year we might have cybercrime, and the next year we might have a module that focuses on domestic violence. So far we have had this one extra module that we can switch depending on what kind of needs we have. This year we did a special Covid-19 module. But it is also a matter of funding. We cannot really do a separate population-level crime survey because it costs too much money. So, we have to adjust and try to do it and hope that we could do it perhaps at least every three years. I think it would be ideal to have it every two years. But we usually have a different theme or research project within the institute that might become that third alternative module. So, we have to find a balance between the available funding, potential new topics like the impact of the pandemic, and the themes that we are doing research on. So that is the challenge, and that is why we cannot really do it every year.

Marcelo Aebi: Thank you. I see your point. But just as a general reflection: conducting the survey every four years also has consequences on *what we know* about crime. Look at the debate on the *crime drop*: hundreds of articles written about the drop of violent and property crime in the highly industrialised English-speaking countries – what they now call the *core* Anglosphere – and almost not a single word about the increase of cybercrime. When, in 2010, we studied with Antonia Linde whether there was a crime drop in Western Europe, not only did we find that in continental countries there were exceptions regarding nonlethal violence and drug offences, but we pointed out that cyber-related crimes must have been increasing since 1992 – when the crime drop started in the USA and the Internet was

launched in Europe – but there were no reliable indicators of it.[3] And that is because national surveys did not include cyber-enabled and cyber-dependent crimes until the 2010s. By 2017, we managed with Stefano to find data on the losses of credit cards since 1992 and there you can see a skyrocket increase.[4] This means that the lack of crime measures was precluding the academic community from seeing the whole picture and was misleading the debate. And that had consequences on policymakers, too, because they echoed the message that crime was going down, while in fact online and hybrid crimes were increasing.

I am not saying that the increase of online crime caused the drop of many traditional offline crimes, although it certainly contributed to it. Of course, there was a change in the crime opportunities structure in Europe after the fall of the Berlin wall and the Soviet Union, which led to an increase of security measures. We pointed that out with Martin Killias in 2000, in an article that showed the limits of American explanations of crime trends.[5] That was later called *the security hypothesis*. But the Internet led to a change of lifestyles from 1992 onwards, a change that became global with the arrival of the smartphones in 2007, as we suggested with Antonia in 2014.[6] Nowadays, we live in a hybrid world. This conference is a good example of it: we have been discussing in the virtual world while sitting in our homes since 9 a.m. Similarly, you cannot always draw a line between online and offline crimes. Many crimes are currently hybrid. They took place in both the real world and the virtual world, like bullying, stalking or cancelling, if you are in the cancel culture.

And in this kind of world, if you wait for four years to ask questions … well, that is a lot of time. Wouldn't it be nice to include some questions on the modus operandi in the basic property and violent crime modules? At least to know if a computer or a smartphone involved; if there was, let's say, a cyber component involved in the crime. Otherwise, you could end up conveying the message that property crime is going down because pickpocketing or traditional thefts are decreasing, while in fact it is taking place online but you are not measuring it.

In fact, a lot of research – and teaching – in criminology is currently out of step with reality. It is delayed. It relates to a world that no longer exists. Currently, there are more smartphones than humans in the world. Yes, of course, they are not distributed evenly. The latest and most expensive models are mainly in the richest countries, but there are

3 Aebi, M. F., & Linde, A. (2010). Is there a crime drop in Western Europe? *European Journal on Criminal Policy and Research*, *16*(4), 251-277.

4 Caneppele, S., & Aebi, M. F. (2019). 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*, *13*(1), 66-79.

5 Killias, M., & Aebi, M. F. (2000). Crime trends in Europe from 1990 to 1996: How Europe illustrates the limits of the American experience. *European Journal on Criminal Policy and Research*, *8*(1), 43-63.

6 Killias, M., & Aebi, M. F. (2000). Crime trends in Europe from 1990 to 1996: How Europe illustrates the limits of the American experience. *European Journal on Criminal Policy and Research*, *8*(1), 43-63.

smartphones everywhere in the world. And some researchers are still measuring exposure to risk only through the time spent in public spaces at night. That is of course still a valid measure for some types of crime, but life and crime are happening online too. We need to fill the gap, because offenders already filled it, and we are lagging behind. Let's hope that the policymakers who attend this conference or will have access to it through the proceedings hear this message and increase the funding for research in the hybrid world in which we live.

Matti Näsi: I agree with that. It is a problem to collect data every four years only. And you cannot give up because crime is changing rapidly. If you want to be on top of it in some forms, then you really do need to have an active follow-up. And I think we might think about options in terms of whether we could have some type of yearly annual items, an annual group of questions, that we could use in terms of having a track of cybercrime. And then have every four years an extensive module with background factors and so on, which you need when you want to do more advanced statistical analysis. In that context, a collaboration with researchers in any form would be highly, highly encouraged.

Regarding your second point, it was interesting to see at the Conference of the European Society of Criminology in Gent in 2019 – unfortunately, we could not have the *Eurocrim* conference in person this year – that the sessions on cybercrime were getting more and more attention. And I think that was really a year when you saw a lot more cybercrime-related papers and a lot more cybercrime-related research. Some of them are very specific topics, very specific types of crime. But I can certainly see the change in terms of how researchers approach crime. It used to be much more focused on traditional forms of crime, but I can see the change now.

Marcelo Aebi: I agree that there is a change going on, and this conference is a good example of it. Still, I think that much more needs to be done to catch up the gap with our contemporaneous hybrid word, also in terms of how criminology is being taught.

There is another comparison that can be drawn between today's presentations on victim surveys and the crime-drop debate. In most European continental countries, police-recorded assault – and the rate of persons convicted for assault – increased throughout the 1990s and early 2000s. Offline property offences and homicides were decreasing, but assault was increasing. And that contradicted also the drop of all offline offences, including assault, observed namely in the US and the UK. To explain that contraction, many of those who considered that there was an *international* crime drop argued that, as people became more sensitive to violence, they report more violent crimes to the police. To test that you need a victim survey. It is certainly a seductive hypothesis, and there is no doubt that it is partially true, but in fact it has only partial empirical support and it is theoretically flawed. Yes, we have become more sensitive to violence, and that

means that the reporting rate of domestic violence has increased and that fights between adolescent and young men that would have never reached the police in the 1970s or 1980s may now lead to a conviction. However, when you look at the trend in assault reporting rates in the few countries that have regular victimisation surveys, in the best of cases you see a slight increase that does not compare at all with the steep and constant increase – year after year – of police-recorded assault. Hence, there must be something else going on. Apart from that, from a theoretical point of view, if you consider that there is an international crime drop and you propose a general explanation for it, then why this increased sensitivity to violence will have an effect on recorded crime in continental European countries but not overseas and not even across the English Channel?

But that is taking us far from my main point. Let's concentrate on the fact that the violence-sensitivity hypothesis posits an increase of reporting rates. People report more cases to the police, and that leads to an artificial increase of the recorded offences. Now, when you look at today's presentations, one common point is that people seldom go to the police when they are victims of offences committed on the web. This not only means that we are seeing a tiny part of cyber-related crime but also that, as the vast majority of countries do not have regular surveys, we do not have the slightest idea of the trend in reporting to the police. Is it going up, is it going down or does it remain stable? And we need that information to understand the trend in recorded crimes. Otherwise, when debating about crime trends, we will be debating out of nothing at all. We are not seeing the whole picture, but only a part of it …

Stefano Caneppele: I have a question for Michael: actually, it comes out from what you presented today that there is a kind of rhetorical saying that goes 'Cybercrime is a priority,' but few results. And there is also a feeling that what was once public has been delegated to the private sector. The private sector is policing the worldwide web of cyberspace, because there is a sort of untold story that probably countries are not able to deal with this kind of issue. Perhaps because it is something transnational, and then the best thing to do is just to announce a public-private partnership. What is your opinion about it?

Michael Levi: I think that what you say is true, but it is a misconstruction, because I think the private sector is much better at some things. It is quicker, it does not need to take account of powers and bureaucracy, and, in the same way, I think the truth is that the governments do not want to spend more money. They do not want to use extra public resources for cybercrime or fraud, whether online or offline or mixed, because coming back to Marcelo's point earlier, we have to really remember that a lot of it is mixed. It is not just online, it is not just offline, it is a bit of both. So, the governments do not want to spend more money on it. The police do not want to train up on it. They … in fact *we* all have no idea what to do in terms of penalties. So, it is not just the public wanting the private

sector to deal with it, although it is true that they do delegate quite a lot, as they do with credit card frauds, for example, and that bit of the system works quite well. It is when the harms are not just against it, it is when there is a collective failure, a market failure, that the system really breaks down. And I think it is an excuse by a lot of governments and police agencies to say that the private sector should be dealing with it. It is in fact because they do not have the resources and they do not want to deal with it, because if the skills are different, the motivations are different.

And what crimes are you going to do less of, in order to divert yourself to cybercrime? Now the police chief in Britain asked this week whether is it really a good expenditure of police time to spend all the time they are spending on domestic violence. He is probably (metaphorically) dead by now, but he has raised the question.

Is it a good expenditure of police time? Because it is not really police work. Most of the time these people are not going to be prosecuted. Do you need a police officer to do this? As a result, we cannot deal with organised crime; we cannot deal with all these other things. So, we have to accept, even in countries that apply the legality principle, that the police cannot deal with all this. So, in a real world, what are we going to prioritise and why?

Of course, there is a moral that people are competing against emotional claims of seriousness for different things, but, in fact, the impact on many online fraud victims is huge. I repeat – the impact on many online and offline fraud victims is also huge, but nobody cares about them either. Then there are many kinds of impacts. Take hate crime. Questions are raised in the UK. If someone says that trans people are not really women or men, is that a hate crime? Should the police be spending their time on this hate crime? You know, these are all big arguments, both for online and offline, but particularly for online stalking and similar offences.

So, we need to find a way, whether it is – or whether we call it – *rational* or not. But we need to find a way of talking through and thinking through these kinds of issues as a society and as academics. Just like in Marcelo's argument. Some academics do not know anything about cybercrime and do not want to know. So, of course, they emphasise the stuff that they are good at. You know I am 72 years old. I learned about cybercrime because I think it is important, not because I am gifted. You know, we need to adjust our systems and the Council of Europe as well. We need to adjust our systems to think about what we are prepared to give up in order to spend more time on these issues.

Marcelo Aebi: Mike, you are raising a major point there. One that is seldom discussed in public. First, there is the issue of the definition, because domestic violence includes a wide diversity of offences, ranging from insults to femicide or homicide. We conducted research in the canton of Vaud – where Lausanne is – following all the cases registered by the cantonal police during six months: roughly 600 cases, which represents an average of approximately 3 per day. We published that with Julien Chopin in the *European Journal*

of Criminology.[7] We followed all those cases throughout the different stages of the criminal procedure: police, prosecution and courts. There had been two femicides, but more than half of the cases were insults and battery only causing pain, which are sanctioned with a fine. Another quarter were threats, which are sanctioned with a fine or a custodial sentence up to 3 years. If you add common assault, which entails the same penalty, you are up to 80% or 90% of all cases, depending on whether you use police or justice data, because there is a lot of offence reclassification; more than half of the cases are reclassified by the prosecutors or the judges. Still, 20% of the cases led to a conviction. This is higher than in the UK, which is the only country with which we could compare our results, because there is a lot of talk, but few solid research on attrition. Moreover, when you think about the kind of offences involved, that is a rather high percentage; but of course, the press and the activists will say that 80% of the cases do not lead to a conviction, that there is an 80% attrition rate. Well, let's be realistic: the canton has roughly 800,000 inhabitants and 800 prison places, although it usually has more than 900 inmates. With 600 cases of domestic violence per semester, in one year you will have to duplicate the number of places if you want to send everyone to jail … and logically duplicate the current budget of roughly 130 million Swiss Francs, which represents roughly 300 Euro per day of detention of an inmate.

Luckily, we are having here a scientific discussion; thus, we can leave aside any populist discourse and concentrate on finding a realistic solution for a major societal problem. It is legitimate to raise the question: should police officers take care of the 450 cases that will not lead to a conviction? Of course, there is also a work on the prevention of recidivism to be done there, but perhaps it is not the task of the police.

Michael Levi: Then you have to pay somebody else to do it, and, you know that, in public expenditure, marginal cost is always more important than average cost.

Marcelo Aebi: Perhaps some of the NGOs that are already being funded in that field could find there a concrete way of intervening. The key issue is that prevention must be evidence based, and research shows that simplistic explanations of domestic violence led to simplistic programmes that do not work. So, there is also a work to be done to produce much more sophisticated explanations of that phenomenon.

Michael Levi: I think it is important because you can see the rise of NGOs not just in these areas but also in an area of importance to Switzerland while fighting *kleptocracy*. So, should we prioritise dealing with foreign kleptocrats against local fraudsters who are defrauding elderly people, or people like me, or younger people like you?

7 Chopin, J., & Aebi, M. F. (2020). The level of attrition in domestic violence: A valid indicator of the efficiency of a criminal justice system? *European Journal of Criminology*, *17*(3), 269-287.

We do not have these discussions very much in the public space. It is said *fortune favours the prepared mind*, but these are very important public arguments and they are not being discussed. I mean, I have the good fortune of living in a sophisticated governmental world – perhaps more populous than it used to be – but it is very hard for people to argue.

For example, I offered to say publicly that with child sex exploitation online, not everybody should be identified and treated as a user. And I am very secure about this. Thus, I was quite happy to say: look, we should have priorities. We need punishment for those who are in contact with children, but for the others we need alternative methods of disposing of that. Now, I know that if I write that down and it goes public, there would be a lot of attacks against me and that my family would also be attacked. But we have to have these debates because we cannot go on like this.

Marcelo Aebi: I fully agree with you, and perhaps it is because we are not having this kind of debates publicly that the impact of academic research on criminal policy is currently very limited. The vast majority of criminological research comes from the US, but they have the highest imprisonment rate among industrialised countries and half of their states still apply the death penalty, against the advice of the whole scientific community. And the new generation of politicians from traditional parties is also reluctant to debate complex explanations of deviance. That is probably why populist politicians are raising several politically incorrect issues – foreigners in prison, jihadist terrorist attacks, political corruption – and winning votes with demagogic and unrealistic solutions for them.

Which are the main concerns of the citizens in terms of crime and how should we address them? We need to identify them and try to address them. In the early 1990s, it was drugs. There was a huge and increasing number of heroin users, and, as addicts were sharing injection material, AIDS infections were also on the rise. People were really worried, although the percentage of heroin users among the total population remained low. As a policymaker, you have two ways of looking at that kind of situation. The idealistic one is to say 'People should not use drugs' – the Reagan's 'Just say no' campaign that you reminded us earlier, Mike – and then you continue trying to change individuals as we have tried in vain for centuries. And the practical one: 'Harm reduction'. You assume that you cannot change every person, but you try to reduce the negative consequences of hard drugs use. That was the solution adopted in Switzerland, and it meant not only needle exchange programmes but also heroin prescription programmes. Twenty-five years later, Switzerland has divided by three the number of deaths by drug overdose, while the US are in the middle of an opioid epidemic, with three times more deaths by overdose.

Can we find similar practical solutions for cybercrime? I doubt it, but at least we should have an open debate about it.

Michael Levi: And keep in mind that, in cybercrime, you can leverage a lot of crimes with a small number of people. I remember arguing nearly 20 years ago that, for the time being, the proportion of cases in which the identity details stolen were used was very small; but what would it take if we had increasing criminal utilisation of the stolen data? What would then be the effect on crime? You know, there is an under-exploitation of crime opportunities by criminals that are already out there, and we need to think about these kinds of things. Nobody is much interested. I have to say that often cybercrime requires a lot more effort than other crimes. Every criminal justice action that involves cyber offenders, particularly abroad, requires a lot more effort than domestic affairs. So, the implications for mutual legal assistance, for evidence recognition in and outside the EU are huge. And we need to worry a lot about this.

Matti Näsi: A couple of comments. First, in terms of the perceptions of fear of crime. As I mentioned in my presentations, over half of the respondents in the Finnish sample were reporting that they were afraid of cybercrime, while much less were actually afraid of physical violence. You can see there how crime and the perception of crime are changing.

There is a second point that I would like to bring to the table, and it is a huge thing. I was in this cybercrime event in Finland, and there was a prosecutor from one of the Finnish courts saying that the problem with the prosecution process is that most judges do not have the required knowledge of cyber-related issues. Sometimes the sessions can be very, very slow; for instance, when you have to explain to the judge what is an IP address. They have to start from the very, very basics of the process. The court system is slow because the staff lack the skill levels required to deal with cybercrime. Only people who are skilled can actually address these issues at the court.

Then you have the lawyers. Do they have the knowledge in terms of helping their clients who may have been victims of crime online? Do they have knowledge and understanding on what the setting is in the online spaces and do they have the expertise to help them to come to the police?

And the police. If we talk about police training, we talk about traditional crime. So, you have the different ways of use of force and so on. But if you have more and more cybercrime, what kinds of skills do we need in the police training? So, if you think about cybercrime, it is not just about whether you have been a victim of fraud online, but you have to relook at the whole system completely. So, do we have skilled people within the justice system who can actually implement and sort of operate within the context of online or whether it is hybrid offending or completely online? So, at this moment, we rely a lot on the private sector in terms of providing us tools to secure our business. But that is private sector investment and, hence, private sector knowledge. What about the public context?

Marcelo Aebi: We invited the private sector to participate in this conference. We tried with several companies, but, unfortunately, we did not manage to convince them, which is a pity because it would have been very interesting to have them here.

Matti, your results on fear of cybercrime are impressive: people are more worried about it than about traditional crime. Indeed, the more you think about it, the more it makes sense, especially when we take a look at the figures. According to Cybersixgill, 23 million credit cards were stolen during the first semester of 2019. That is bad news for credit card companies and retailers – because most of the data are stolen from them – and they certainly do not want that kind of information on the front page of the media. And in fact, it seldom gets there. Nevertheless, your data show that people are aware of their exposure to risk. A good example of how wrong are those who think that fear of crime is mainly a by-product of the way in which crime is depicted in the media.

Stefano Caneppele: Fernando, you were commenting in the Forum that research is often not considering the part of cybercrime that is about social networking – which is exploited for some criminal behaviours, such as radicalisation – and that it still focuses on individuals against government.

Fernando Miró-Llinares: Yes, related to what Marcelo and Mike were saying, I think it is true that we have to change the focus. Also, as a criminologist, when we do that part of criminology that is creating criminology, maybe we have to do a *new creative criminology*, but related to social networks. I believe that we are not focusing enough on social networks. And I think they are one of the keys on cybercrime because there is an important percentage of cyber hacking taking place there. Social networks have a lot of information that is extremely useful for the study of some crimes. They have the information on how many tweets of hate there were, they can track the evolution of the amount of information that circulated during Covid-19.… We do not have the information, but they have it all. They have the information on the evolution of some kinds of fraud, and they also have the information on the kind of spams that circulated in social networks.

Related to the issue of how to measure crime, I think that we have to focus also on social networks for the measurement of cybercrime. And related to what Mike was saying about deterrence and change in psychology, I think we have to change our perspective on the relationship between the government and the individual. I think that nowadays the government is not the problem. The new government of cyberspace are social networks. We have to put our focus on them, because currently we are not thinking too much on them. I see a lot of research in politics, in sociology, but not a lot in criminology, related to the power of social networks. I do not know if it is totally related with where you would say, but I think it is important.

Marcelo Aebi: Well, it seems that we have reached an agreement in terms of the need to change our framework of study. Of course, we are not going to find the solution this afternoon, but there is that common trend in the presentations and the discussions we are having today. I am not sure it is shared by the whole scientific community of criminologists. And Fernando, Stefano and I have experienced how difficult it is to publish our shared interpretation of the role of cybercrime on crime trends since the 1990s when you have peer-reviewers who support the idea of a homogeneous trend for all sorts of crime and a single explanation for it.

Ricardo Estrela: I was listening to your conversation and just to give a little input and to add to what Fernando said regarding the power of social media, I think you can take a look, for example, at *the community standards*. Every social media platform has their own community standards and their own definitions of hate speech. So, when we try to remove content that one of the victims we support perceives as offensive and that would constitute hate speech under our legal framework, we also have to deal with the legal framework of the platforms. The definitions of hate speech are not necessarily the same. And then the platforms have the power to remove it, and if it complies with their own community standards, they will remove it. But if not, even if we show that according to Portuguese law it is a crime to say that, they would not comply with our demand. And we have to play by their own rules if we want to maintain our main goal, which is to help the person who reaches out to us and to have the content removed.

Closing Session

Marcelo Aebi: I would like to start by saying that I really enjoyed the discussions that took place during these two days. The presentations too, of course; but a strong point of this conference is that we had enough time for discussions today. It was risky when planning the conference to leave more than one hour for the closing discussions, but we trusted the speakers, and of course, you were perfect. An open discussion, with no censorship or limitations imposed by political correctness is always healthy for science.

The Spanish-Catalan philosopher Jorge Wagensberg wrote a book called *El Gozo Intellectual*, which could be translated as *The Intellectual Enjoyment*, or *the Intellectual Pleasure*, and that was exactly my feeling during these two days.

I am also happy because, with this conference, we renew an old tradition of the Council of Europe, which used to organise annual criminological conferences for many years. It was in these conferences that criminologists from the former Eastern bloc and those from Western Europe started to get to know each other and build a common European criminology, later formalised with the creation of the European Society of Criminology. So, I would like to thank again Ilina Taneva and her team in Strasbourg. Who knows? Perhaps we are relaunching that tradition.

It is of course a pity that we could not meet in person in Strasbourg and share the bread and salt which builds friendship. However, they say that every cloud has a silver lining, and perhaps the fact that we were obliged to organise this conference online allowed more people to participate. Perhaps, in the near future, most conferences will adopt a hybrid model with some people in the place of the conference and some online. That is another analogy with cybercrime, which is already quite often a hybrid offence, as we saw during this conference.

The times in which speakers were asked to write down a paper before or after a conference for a book of proceedings are past. Nowadays, top researchers prefer to publish their ideas in scientific journals. However, as we have recorded the audio, we will do a transcription of it at the University of Lausanne, and we will send it to the speakers so that you can simply adapt it. In that way, we will still have a book of proceedings – which of course will be in Open Access – and it will have the advantage of being written following the language of an oral presentation, which should be easier to understand for the general public than a sophisticated collection of scientific articles. And now I leave the floor to Stefano.

Stefano Caneppele: I think you said everything we needed to say. I just want to thank again all the participants and all the speakers. My impression is that we got very good insights

and inputs about the state-of-the-art in cybercrime. I also would like to thank again all the staff of the Council of Europe who were able to set up this conference despite this difficult time. Thanks to the interpreters and the technicians, also on behalf of everybody.

Marcelo Aebi: Thank you very much for attending this conference, and let us hope that we will soon be able to gather together in Strasbourg. And thus we bid you farewell.