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

Measuring cybercrime in the time of Covid-19: the role of crime and criminal justice statistics

Proceedings of the conference 29-30 October 2020 (Version: 25.12.2021)

Strasbourg, Council of Europe

Participating authors in alphabetical order:

Andri Ahven
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

Contents

Introduction 3

Prelude session: Cybercrime in times of Covid-19 and in PostCovid-19 era .8

Covid-19 and cybercrime. What we know, what we do not know and what we shall measure. *Fernando Miró-Llinares* 8

Session 1 - Modernising crime & justice statistics 22

The International Effort in the Modernization of Crime Statistics. *Michael Levi* 22

The Budapest Convention and the classification of cybercrime for statistical purposes: some observations. *Alexander Seger* 28

Cybercrime Statistics: National Experiences. Estonia. *Andri Ahven and Mari-Liis Sööt* 35

Cybercrime Statistics: National Experiences. Spain. *Francisco Sánchez Jiménez* 42

Self-Report Delinquency Surveys & Cybercrime: The State-of-the-art. *Lieven J.R. Pauwels* 46

Q&A Session 1 61

Session 2 - Modernising victimisation survey 62

Crime Survey & Cybercrime: The State-of-the-art. *Marianne Junger and Pieter Hartel* 63

Netherlands: National Experiences in Cybercrime Surveys: Challenges and Lessons Learned. *Johan Van Wilsem* 80

Finland: National Experiences in Cybercrime Surveys: Challenges and Lessons Learned. *Matti Näsi* 88

England and Wales: National Experiences in Cybercrime Surveys: Challenges and Lessons Learned. *Billy Gazard* 96

Q&A Session 2 104

Session 3 - Rethinking victims assistance & deterrence models 116

The Internet Organised Crime Threat Assessment. *Nicole Samantha van der Meulen* 116

Deterrence, Diversion and Desistance of Cybercriminals. *Michael Levi* 126

Q&A Session 3 134

Wrap-up session 148

Introduction

Ilina Taneva

Good afternoon, everybody. I see that there are about 34 persons that 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 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 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 that 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 that 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 which is financed by the Council of Europe and the European Union, and this is the beginning of a third phase of this project, and the outcome of this conference would be the report on the way cybercrime is defined and the proposals, how to measure it and 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 Cooperation and also Director of the French-speaking probation service of Wallonia-Brussels (Belgium).

Annie Devos

Thank you, Ilina. Ladies and gentlemen, on behalf of the Council for Penological Cooperation, it is my pleasure to welcome you and to open the conference *Measuring cybercrime in a 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 the help of whom we were able to contact and invite the national experts. I do hope that the outcome of this meeting will be useful also to all of you and to 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 the to these crimes, on the other hand. A number of criminal acts are committed online, therefore such notions as *territory*, *jurisdictions*, *time* and *perpetrators* become difficult to define, as well as the enforcement of respective measures to prevent and protect society. 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 2003, the Council of Europe Annual Statistics on Prison and Probation -also called *SPACE I* and *SPACE II* projects- as well as for publishing the *European Sourcebook on Crime and Criminal Justice Statistics*. I wish you a resourceful and successful conference. So, 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. Thank you.

Ilina Taneva. Thank you very much, Annie. And now the floor is to Professor Marcelo Aebi.

Marcelo F. Aebi

Thank you very much, Ilina, and welcome to everyone. I first would like to start by thanking the trust that the Council of Europe has put on me to produce, as was mentioned, since almost 20 years ago, the *Council of Europe Annual Penal Statistics*. This is a project that is very dear to me, and it is related to this issue of how to measure different forms, different manifestations of crime, and, my first contact with the practice of criminology was also the Council of Europe in 1996 in the framework of the *European Sourcebook of Crime and Criminal Justice Statistics*, that was launched by the Council of Europe.

Now, almost a quarter of a century later, we are combining forces of these two groups and trying to produce reliable measures of crime because it is clear that SPACE only measures the final stage of the criminal justice process. It doesn't really measure crime, but the reaction to crime. And so, we have been trying to put this in connection with the other indicators of crime and criminal justice, from police statistics to crime victims surveys. And, in the framework of this work, we realise that we have been trying to measure cybercrime in different ways without a lot of success.

And so, when I was asked to conduct this project, the first thing I did was try to find a team composed of the best researchers in the field. And so that is why I turn to ***Michael Levi*** from the University of Wales, who is a well-known expert on cybercrime. And then I turn to ***Fernando Miró***, from the university Miguel Hernández of Elche from Spain, who has also been working on that for a long time. And of course, to my friend and colleague ***Stefano Caneppele***, who is also an expert on the field. So, everything that is going to happen now would have been impossible without the four of us working together. So, the main issue here is to discuss how to measure cybercrime and how it is being measured currently by different crime statistics. That is why we have also interventions from different countries.

Our feeling -especially with ***Stefano Caneppele*** we have been working on this topic- is that maybe this requires a different way of dealing with the statistics. We are used to having indexes and calculate the delinquency rates and perhaps, as cybercrime has so many forms and it is a very large concept which entails cyber-enabled crime, cybercrime, and traditional crimes that are now being committed through the Internet, one possibility is to have a different indicator, which is the percentage of crimes in which there was a cyber factor. It is a completely different way of measuring delinquency, but we will see… That is why we want to discuss with everyone what the crime victim surveys show. For example, we know that in the United Kingdom, which would be presenting here (see *National Experiences in cybercrime surveys: England and Wales*), including a few types of cybercrime produce an increase of one third percent of crime. So, it is a very interesting topic, which is not well measured. And we would like to come out after, at the end of the project or this part of the project with some concrete proposals. And that is my main message to open. We are here to learn. And so, it is my pleasure to give the floor back to Ilina. Thank you.

Ilina Taneva. Thank you, Marcelo. I just want to remind you that it is almost 1:20 and the next speaker is Fernando Miró-Llinares and I would give the floor to him.

Prelude session: Cybercrime in times of Covid-19 and in PostCovid-19 era

Covid-19 and cybercrime. What we know, what we do not know and what we shall measure.

Fernando Miró-Llinares

Miguel Hernández University of Elche, Spain[1]

Well, thank you very much. First of all, I would like to start, of course, by thanking the *Council of Europe* for organising this conference, and particularly to 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 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 the excuse 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 was 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

[1] Additional material: the author's visual presentation is available here: https://rm.coe.int/presentation-fernando-miro/1680a0339d

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 measuring cybercrime and the need to join efforts to better understand a set of phenomena that we encompass within 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 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 six 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 existing data either from official or from 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 to end with a brief thought on how we should measure cybercrime in order to have a clearer picture on so.

So, let me start from the beginning: What do we know about the impact of the Covid-19 crisis of cybercrime, or rather, what do we intuitively think the Covid-19 crisis meant to cybercrime? I said that before we have 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 that the answer is that 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 influences 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 on a certain place with the victims, and due to the lockdown, people stopped doing things on the streets to do them at home, and above all, leisure, working and so on, on the Internet. So, the opportunities and the crimes with it would also move there. And when the lockdown was over, they will return to the streets.

I am not saying anything that we do not already know if I show these graphs made on Google data for Spain (Figures 1 and 2) and show how the lockdown meant a reduction in activity in the commercial areas and then increasing in time at home, and it will not be a surprise if I say that the increase of time 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.

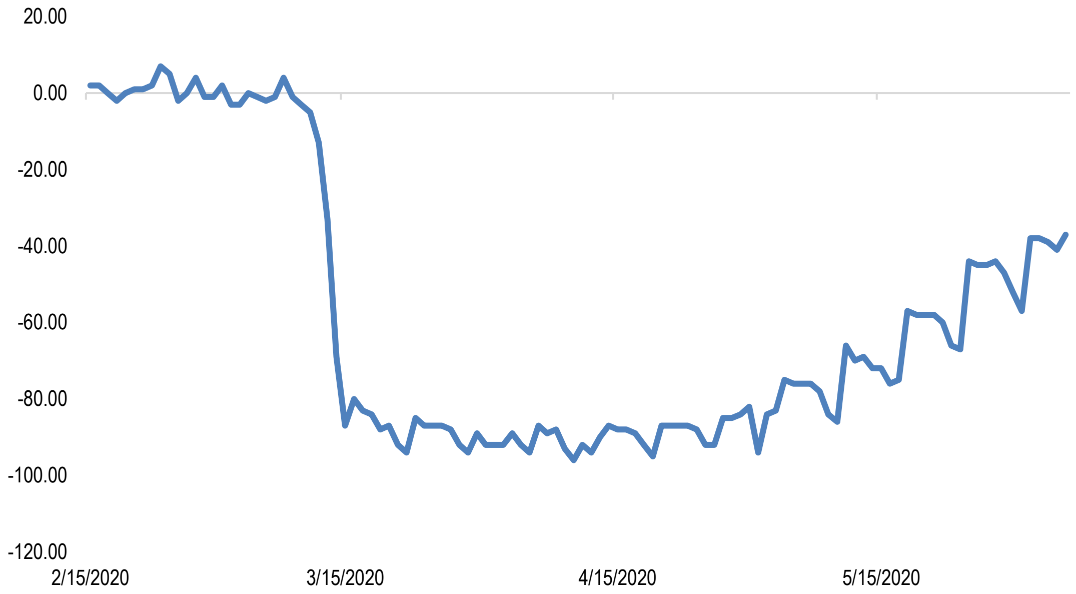
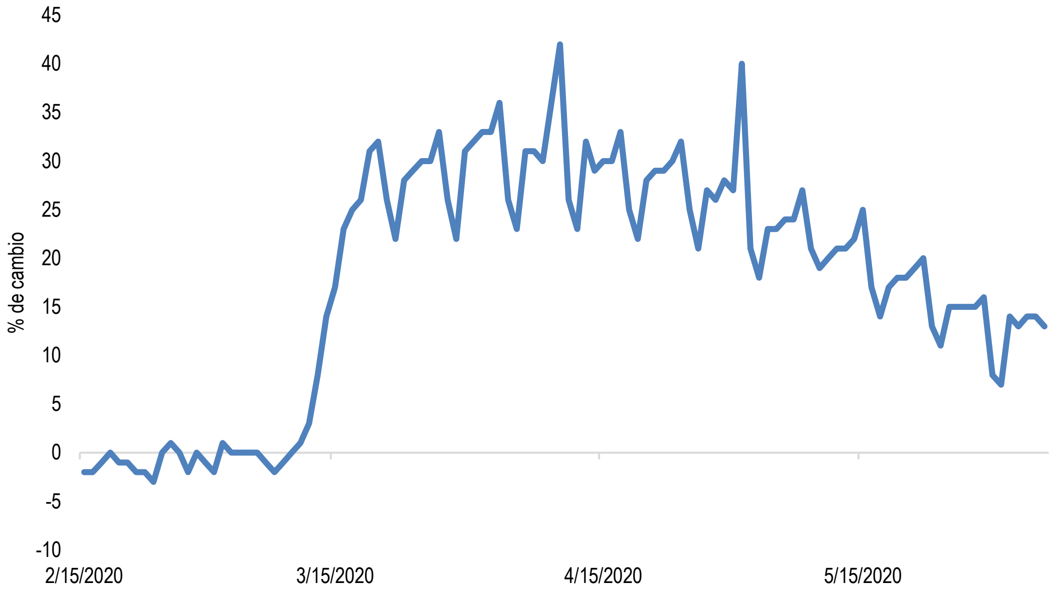


Figure 2: Percentage change in mobility in residential areas in Spain from baseline. Source: Google Trends.



We call this "shift in opportunities", and it is the main hypothesis used to hypothesise a growth on cybercrime during the pandemic and that this criminal activity may decline but not return to previous rates when the crisis ends if still working or online shopping continues. And this simple theory was telling us something else: just as criminals displace in physical space to avoid surveillance or to improve the results of their crimes, on the Internet cybercriminals also change their targets to more vulnerable or valuable ones, and they also adapt the cyberplaces from which they attack to new interests to be more successful. We could call this "cyber offending opportunism" and it can be summed up in the idea that cyber criminals take advantage of people's weaknesses and interests to carry out their attacks, and if, as happened during the crisis, what people is looking for in google, as these google trends graphs show (figure 3 and 4), are terms like facemask, telework or COVID19, then cybercriminals will try to sell fake facemasks or create domains called COVID.

Figure 3: Covid-19 Google´s search trend. Source: Google Trends.

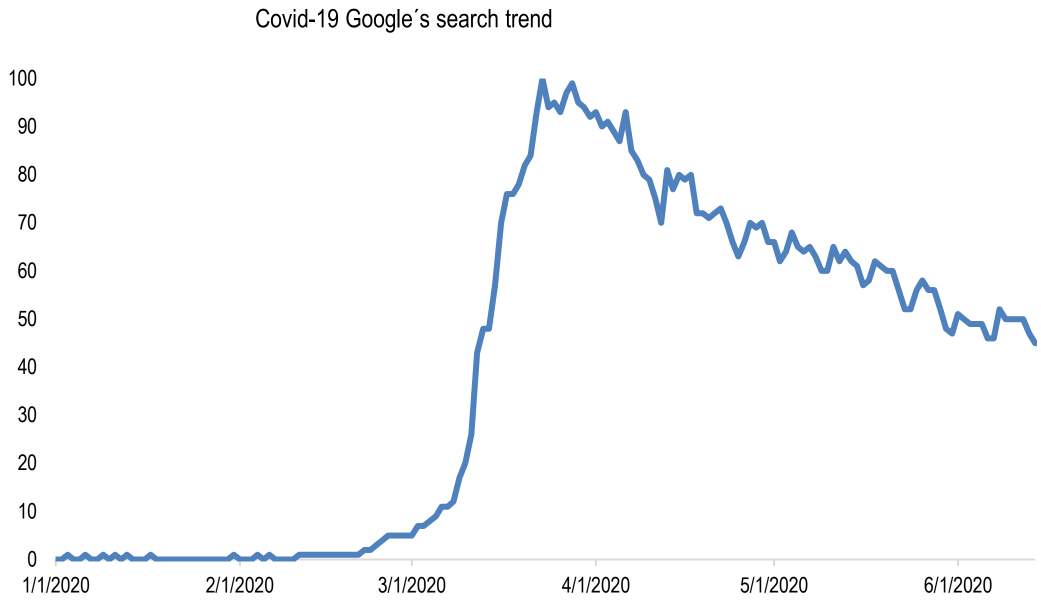
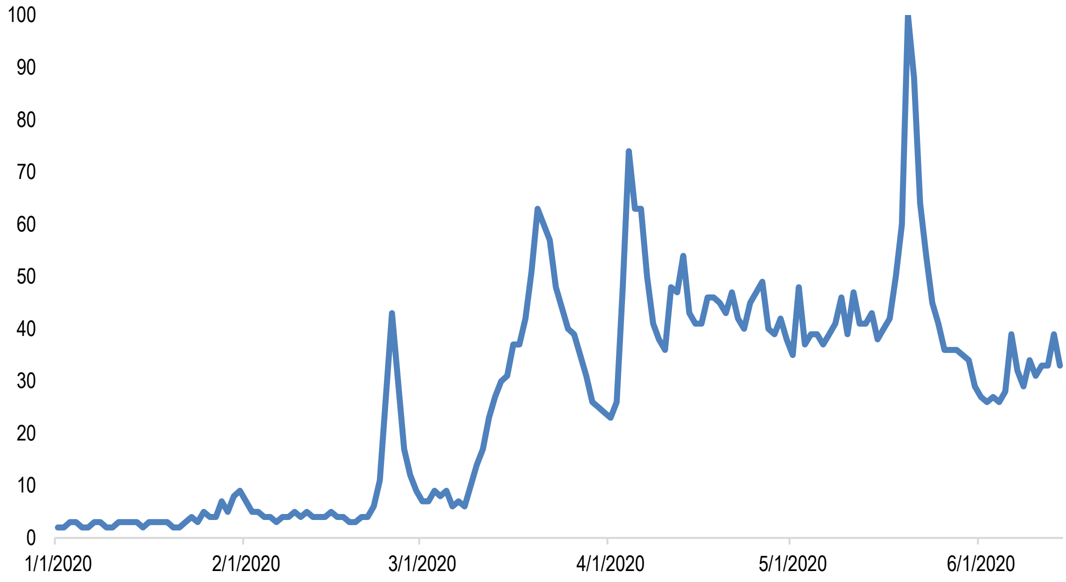


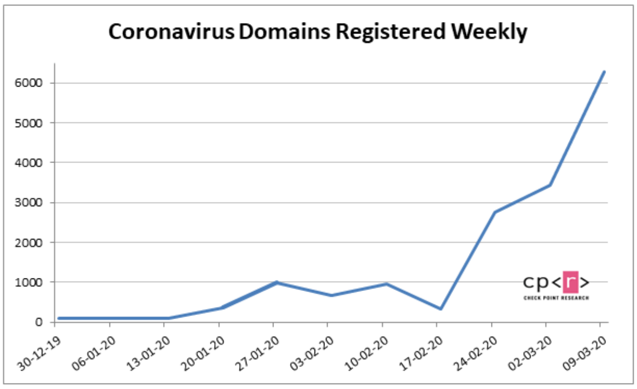
Figure 4: Facemask Google´s search trend. Source: Google Trends.



Well, what do the data tell us about this? Following this differentiation between shift of opportunities from physical space to cyberspace on one hand, and cybercriminals opportunism on the other hand. Let’s see what private companies tell us about the impact of covid19 on cybercrime. Some interesting data are in accordance with the hypothesis of the shift of opportunities. The generalisation of teleworking produced by lockdown, with different times in different countries, according to the date of the lockdown, imply 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.

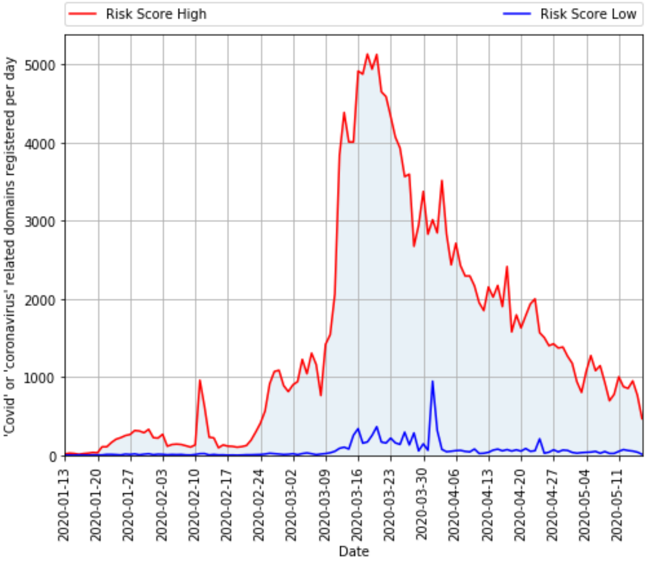
Some data sources also show us the opportunism of cyber criminals. This table of Checkpoint shows the increase of more than 500% of the domain names registered between February and March related to the terms *Covid* and *Coronavirus* (Figure 5).

Figure 5. Coronavirus domains registered weekly. (Source Checkpoint)



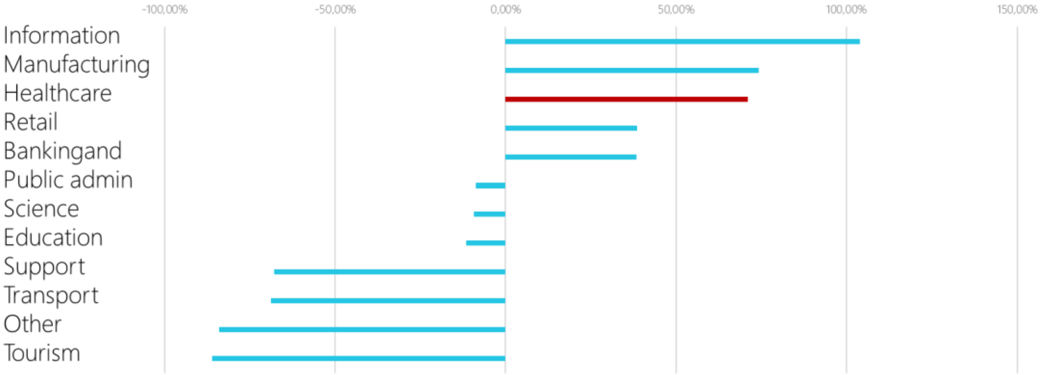
And in the next figure (figure 6), with data from Domaintools, we can observe that in the same period the creation of malicious domains increased 400%, and the same relationship between the appearance of new domain names related to Covid-19 and a strong increase in the creation of malicious domains for sending a spammer scam is shown on these tables made with data from TrendMicro and Domaintools and cyber criminals, not only the names of the cyber places from which they attack, they also change the targets.

Figure 6. Risk domains created by week (Source domaintools)



This table (figure 7), based on data from the VPN at last report, shows a significant change in the sectors attacked in 2019 and this year, with a significant increase in the number of attacks, as you can see, against information, health and manufacturing sectors and attacks against transport and tourism sectors.

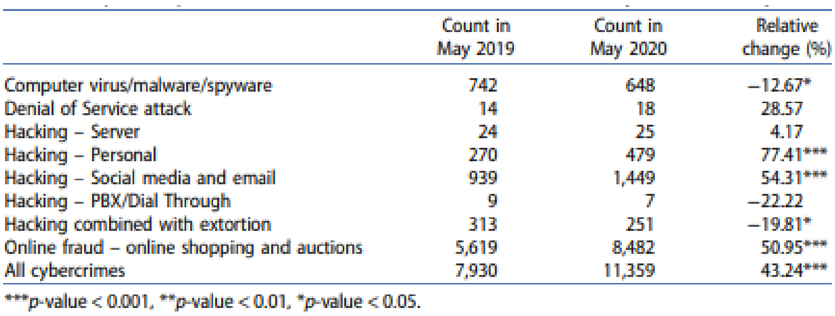
Figure 7: Percentage change in number of violations by sector affected, 2019 Q1 vs. 2020 Q1 Source: Own elaboration from the atlasvpn



But what about the official sources related to cybercrime opportunism? What we have found in 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 dedicated to fraud into the sale of health products. But the information given in these ways to that is very, very broad and limited for scientific observation. Related to the shift of opportunities from physical to cyberspace and in order to know if the hypothesis that cybercrime would have grown is confirmed, we can look at the reports that countries as Germany, Italy or Portugal and some which will show the reports today with us have informed about changes in criminality during the pandemic, including specific reports about cybercrime. In general, these reports collect the number of complaints treating cybercrime as a single category. In some cases, they do not compare time periods or they analyse very short time periods that show inconsistent results. So, it is even harder to determine the evolution. Again, the lack of raw data, the lack of opportunity between reports and definitions, the lack of information on less serious crimes does not yet give us a clear picture of 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 United Kingdom and which, in addition to being regularly updated, presents additional information to the simple number of complaints such 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 observe 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 compared to May 2019, specifically 43% more complaints were registered. 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 of cyber dependent crimes May 19-May 2020. Source Buil-Gil et al., 2020.

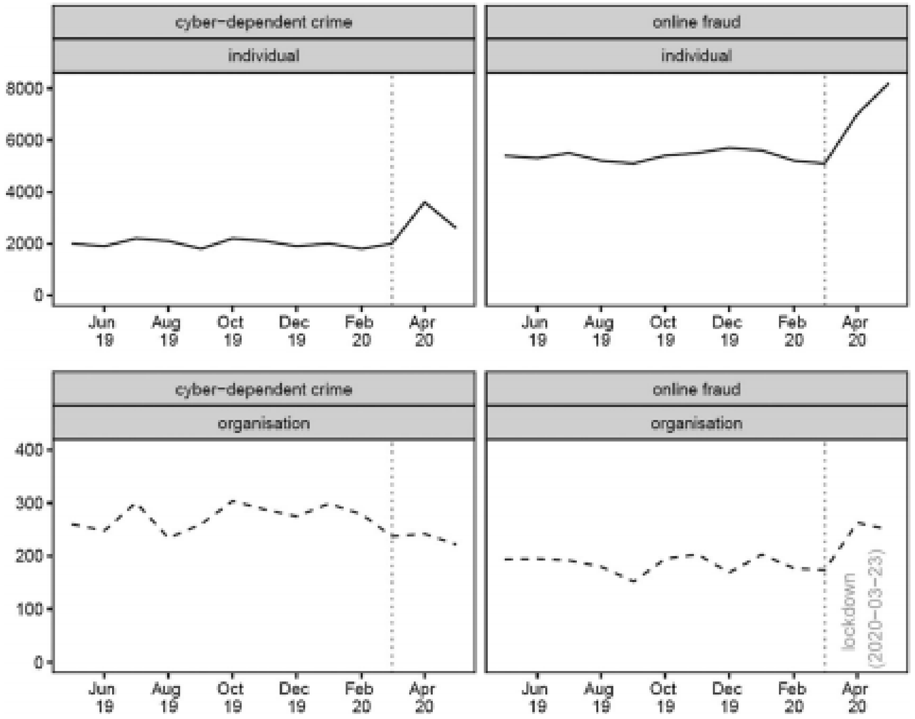


	Count in May 2019	Count in May 2020	Relative change (%)
Computer virus/malware/spyware	742	648	−12.67*
Denial of Service attack	14	18	28.57
Hacking – Server	24	25	4.17
Hacking – Personal	270	479	77.41***
Hacking – Social media and email	939	1,449	54.31***
Hacking – PBX/Dial Through	9	7	−22.22
Hacking 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.

But this has not happened in a homogeneous way between crimes and types of victims, depending on whether they were individuals or organisations. Furthermore, it was striking that some crimes such as those related to malicious software or extortion seemed to have decreased. Maybe this is related to the fact that these affect organisations. The later review with data from the month of June showed a strong increase in these crimes. While reports of crimes such as fraud in online shopping made by users began to fall in July, reports of organisations for this crime grew strongly again, possibly as a result of the delay in the detection of these crimes by organisations detecting many of them with the reopening returned to face-to-face work (See Figure 9).

Figure 9: Trends for cyber-dependent crime and online fraud by type of victim. Source Buil-Gil et al., 2020.

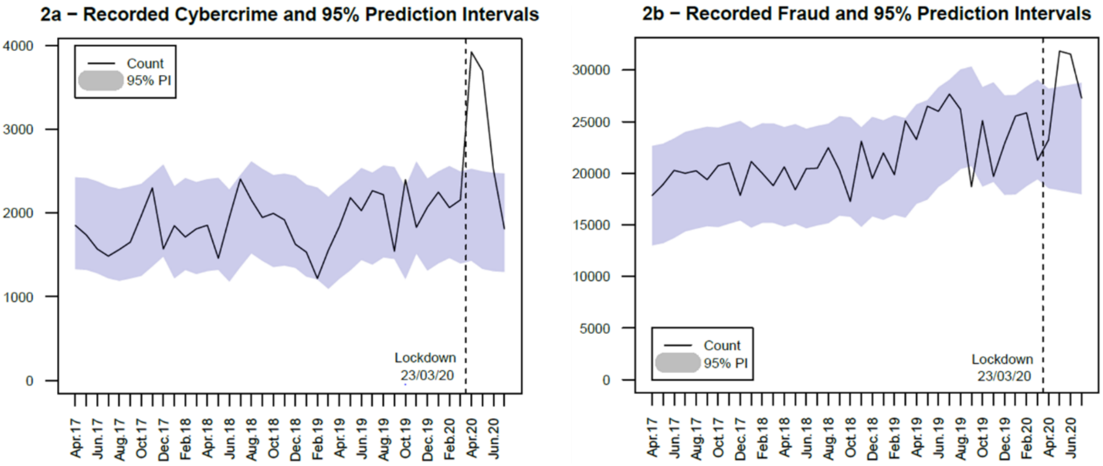


In fact, to try to understand if it was only related to the lockdown or some of these trends will remain in a second, in the study that we are now carrying out with data from 2017 to know, we intend to identify trends evolution for which we have used our specific type of series prediction technique that allows us to generate a model with a confidence interval for past time series data and evaluate whether the observed values feed the model.

This analysis shows a significant increase in fraud, which is outside the predictive model only in the months following the outbreak of Covid-19. But this changes when you observe different kinds of fraud. This data, collected monthly, allow us to make comparisons with other statistics related to daily activities in order to seek explanations for changes in cybercrime beyond simply looking at two time periods -before and after- the pandemic. So, we can see that cybercrimes seem to have risen and are now beginning to stabilise, although some modalities such as online fraud, remain above trend, even when the lockdown has ended. The pattern to online shopping shows us that while

e-commerce continues to grow, cyber fraud maybe it will go up too.

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



Well, we also know something else: we know a lot about what we do not know with the data we have and in the few minutes left, I will try to express it. Firstly, we do not know how much cybercrime really has grown and whether the growth has been above this trend, except in the case of the United Kingdom. Most countries do not provide monthly updated statistics that offer annual reports and as the calendar year has not yet ended, they have not been published. We also do not know which countries have been most affected. This makes it impossible for us to know whether countries with more severe confinement measures have been more affected and therefore whether our assumptions are true or due to other factors.

As we have already said, the lack of data awaiting annual reports make it impossible for us to compare the situation between countries. But the lack of proper definitions of what cybercrime is makes it difficult to compare between countries, even when the annual report arrives. And we also do not know which forms of cybercrime have grown because with few exceptions, we only include generally a single category of cybercrime. And even in the cases with the best data, there is still much to know. We have seen before that even with data of Action Fraud published monthly that distinguish between various categories, we have several problems. First, in many cases, the data does not coincide with the data of the monthly report with which the agency itself is asked. Second, this type of data aggregates the raw victims, so it does not allow us to differentiate between types of victims to identify population groups at risk. Nor does it allow us to know if the profile of the victim has changed, who are the most affected, how socio-demographic and other factors influence and so on. And last but not least, these data are from complaints. And although in the UK, it is easier to report cybercrime than elsewhere, we know that there is a significant number of crimes, so we do not know how many have actually been committed. The pandemic has also modified how we work or how we communicate, and this could also affect the capacity to detect cybercrime, especially in the capacity to inform or to collect complaints. We know that there have been more complaints, but there may be a temporary distortion by collecting complaints with a longer than usual delay 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 and finishing, what should we do, what data should we collect and how? And of course, I am not going to solve this. We have a conference to begin to do it. But I will say only some words. Firstly, 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, maybe what Marcelo and Stefano were saying, or a common definition of cybercrime or a common way of identifying that. I believe that the first step that should 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 and gender of the crime, personal, professional, leisure relationship and of the medium used especially if its social network, type of device, etc. Similarly, the information should serve as more geographical units rather than collect that data on the country level. And finally, I believe that we must take seriously the need to promote transparency and a concrete and common methodology in the collection of data from private organisations which dedicate to cybersecurity, which complements and serve 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 self-reporting: it is true that there are some studies in which they did and they didn't find statistically significant differences between cyber victimisation during the pandemic. However, we must be cautious when assessing the meaning of these results, and especially given that both groups were asked about victimisation in the last year and not in the *Pre-Covid* and *Post-Covid period*. But we need more self-reporting, maybe at a European level.

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

Ilina Taneva. Thank you, Fernando. It was very interesting, and a lot of questions could be asked on your presentation, but the question and answer session is at the end of the meeting today. So,now I have the pleasure to give the floor to ***Michael Levi*** from the University of Cardiff. We are starting ***Session 1 Modernising crime and justice justice statistics***.

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

Llinares, F. M. (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 https://www.raco.cat/index.php/IDP/article/download/373815/473802/

Session 1 - Modernising crime & justice statistics

The International Effort in the Modernization of Crime Statistics

Michael Levi

University of Cardiff, United Kingdom[2]

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, eco and wildlife crimes. And make the point that every one of these, except maybe fraud, have come for financial online components, that is quite important to keep that in mind. And when I say ransom, 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 have 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 the 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, was not designed for routine

[2] Additional material: the author's visual presentation is available here: https://rm.coe.int/presentation-michael-levi-reforming-crime-statistics-coe-2020/1680a033b1

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. SoI am aware of the shift. And what do we and 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's one reason we do not have time series that include fraud or other cybercrimes. And there is a multiple victimisation 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 well enough developed 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 different time between the crime happening and the time of our awareness. And generally, 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 to divide them into the US -they always have to come first. There was a National Academy of Science 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, then the difference may not matter so much.

Let us turn to non-US reform efforts. I am not going to go through every country. We have national representatives. The European Sourcebook, the last published version, says almost all countries provided data on fraud. There are only a few of them could adopt the standard definition. And that is quite a big range between countries. Eurostat crime data: largely absent cybercrime. The UK we are not going to cover that in detail because we have a speaker tomorrow who's 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 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 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. The ICVS, which, well, we have spoken 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's 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, British Airways, etc., 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, 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

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 https://www.aic.gov.au/publications/rr/rr19

The Budapest Convention and the classification of cybercrime for statistical purposes: some observations

Alexander Seger

Council of Europe[3]

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 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, why do we need statistics or data on cybercrime? It is to 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

[3] Additional material: the author’s visual presentation is available here: https://rm.coe.int/presentation-alexander-seger/1680a0339b

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. One point four million requests in 17 EU member states that 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 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 a 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.

At Covid-19-related cybercrime, because this was also mentioned, is one of the topics of this conference, but it 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.

OK, so we can pick a new type of offence in a way that cybercrime matches in many cases with the offences of the Budapest Convention of 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 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, and its situation report concludes that there is about 82 million Euros damage by the one hundred thousand cybercrimes that they recorded and registered in their system. And that probably they also investigate, but if you listen to German Industry Association, they concluded that the damage of cybercrime to German industry is 100 billion Euros in a year. You see there is a slight difference and that is a problem.

Most cybercrime and most damage 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, by the people who were supposed to know because they were in high-level positions. They are saying that any major cybercrime against industry, against the sector of industry, against institutions, is considered as a national security issue, 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 ask that because the majority of people of private sector entities think that criminal justice is useless, that criminal justice system cannot offer a response to crime, there is no follow-up, no remedy and attacks against anything larger than an individual in many cases are considered a matter of national security. Companies do self-defence, they fear their reputational damage in particular of cybercrime: i.e. affects a bank and, in many cases, insurance pays, we all experience that. We do not even have to go to the police anymore if we are defrauded 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, etc., all sorts of cyber violence. Law enforcement would not know how to 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% that is reported and recorded by criminal justice authorities, it seems that less than 1% is actually leading to a criminal justice outcome. So, from 10,000 crimes, you make it one to ten convictions, a very important problem.

And one important point I wanted 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: in 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, a rape case person may have groomed the victim on the Internet, the location data may prove that the offenders were at a certain point 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 experience when it comes to terrorism. And that is the criminal justice's response may become more and more residual. In that sense also worrying when you look at some court decisions that national security states are given the margin of appreciation, that is not the case when it comes to criminal justice response. And I would be worried about a recent decision, again, of the Court of Justice in Luxembourg, where governments go there and ask: *what shall we* *do about access to data?* and they respond to the question: "The problem is related to the way the courts decide is based on national security, access to data, and therefore they put some obstacles there but *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 systems 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 other challenges 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 cybercrime, but as the most serious offence. And then there is the issue of transnational nature of cybercrime and 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 Trick-Bot "Take Down" ("Take Down" in Inverted commas, because it was only partially taken down and then moved to other servers), which involved different offenses, 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 infected with this trick bot with 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 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 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, carried out evaluations in the criminal justice area. And all of the evaluation reports recommended keeping of 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*, which is promoting a more strategic approach to this. The link was shared with you this morning. Hopefully that this 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.

Cybercrime Statistics: National Experiences. Estonia.

Andri Ahven and Mari-Liis Sööt

Estonian Ministry of Justice[4]

Mari-Liis Sööt

My name is Mari-Liis Sööt, from Estonia and working for the Ministry of Justice and me and my colleague Andri, whom you cannot see right now, but who is sitting here next to me, will explain to you a little bit in detail about how we collect criminal or statistics about cybercrime. And first of all, I would like to thank all the organisers of this conference and bringing up this very important and interesting topic. And I would also like to thank previous speakers, *Fernando Miró*, *Michael Levi* and *Alexander Seger* for their very interesting presentations and issues that they raised that me myself could sign all of the presentations you gave. So, the aim of the discussion is actually to find ways to better grasp the cybercrime extent 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 mis-usage 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 or 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

[4] Additional material: the author's visual presentation is available here: https://create.piktochart.com/output/50198798-cybercrime-stat

computer systems in order to steal someone's money is an example of such case, which could fall on both categories.

So, before our look into our official statistics, let me say from the soft or surveys side (Table 1) that in Estonia we asked people about their personal experiences, about offences that they most probably face. And according to the annual victimisation survey, we get to know that 30-40% 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.

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 as victims of sexual harassment and so on 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 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. Why I also decided to show you the survey results is also to stress that these kinds of surveys actually allow for international comparisons pretty well once agreed on the methodology.

So,now coming closer to the topic that we are supposed to talk about, it only is when we 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 better know 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 collect (see Figure 1 and Table 1), and I will show you why. The total number of computer-related crimes in Estonia is a very small number, 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 over 20,000 crimes altogether are registered in Estonia. Just put it into the context.

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

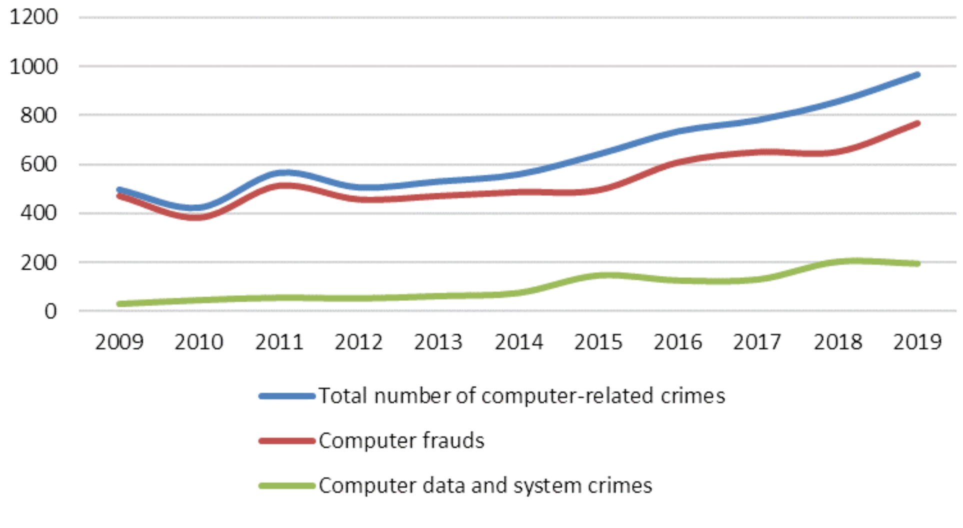


Table 2. Computer-related crimes: registered offences 2009–2019

	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
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? The number contains computer-related fraud. It contains the provision of the Penal Code in Estonia, which is precisely computer-related fraud and it does not contain the offences recorded as other types of frauds, such as so-called *ordinary fraud, investment fraud, insurance fraud,* etc. Why is this? It is not because they are not committed via the electronic means (most of them are), but this 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. Let us say, tomorrow we hope to have more automatic analyses which would help to filter out cases related to a computer in other types of fraud too. This needs development of various IT systems and this problem and solution also relates to other content related to cybercrimes. Let it be child pornography or any other. So, we need IT solutions for that to investigators 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 of 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. I found a lot of examples, of course, about cybercrimes, but only a few of them I present here. 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 in different types of crimes according to the Penal Code. And one of the most typical things I think know concerning frauds and also computer-related frauds is 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 ordering goods. And it appeared what 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: concerning child pornography. According to the section of the Penal Code we may find both offline offences and online offences, first up, for example, if you prepare pornographic material, you are using cameras and you do not need any electronic means, additionally, you will make storage of pictures or videos. We might be saying such kinds of offences may take offline and, of course, online offending has increased, and as I understand it, they got a majority of such offences, of course, downloading pictures and videos from the Internet and uploading pictures or videos are quite common offences.

Mari-Liis Sööt

The point what we are trying to make is when the country sends information about a computer-related fraud, and 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.

And the second problem is that we still try to put a lot of effort to filtering 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, which cause bigger harm, which includes commitment in groups, etc. So, in reality, these contain only a small number in the official statistics, let us say 5% in the last year in Estonia while it makes a lot of effort and it 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 the highly influential computer offence, the majority of those offences is actually in Estonia made up *of digital family violence*. We call it *digital family violence* because it includes mostly changing, capturing the passwords of social media, 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 mass 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 is stolen and so on. The most serious and highly influential cybercrime, 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 so on.

Before giving the floor again to *Andri*, who will bring an example to illustrate the point for international comparison, it clearly suggests first taking small bites, namely comparing only what is comparable. Let us take the 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 can have a final word to bring. 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, illegal obtaining access to a computer system, and if we look at descriptions of crimes, we may find very different crimes. 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 then clients' database was stolen and one of the most serious cases, which is still in investigation, is where it was evaluated more than 10 million Euros, and it was committed when installing spyware and Bitcoin were bought during several months. Those types of crimes are relatively rare, but may cause huge damage. But in the same section of the Penal Code, the absolute number of crimes is much higher concerning digital stalking and so on. For example, surveillance of social media called as 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. Again, that is up to that number. So, I think what we are approaching our time limit, and we are happy to listen next presentation. Thank you everybody for your attention.

Cybercrime Statistics: National Experiences. Spain.

Francisco Sánchez Jiménez

Spanish Ministry of Interior[5]

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 of 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 Center for the Protection of Critical Infrastructures. By being together different units with statistical and cybercrime-related responsibilities, we believe that it 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 how the situation is in my country. In Spain, we have detected a significant increase in cybercrimes, which is common with other tendencies in several countries around us. In fact, within the first six months of the present year, with their special conditions related to the pandemic and the lockdown, we have reached

[5] Additional material: the author's visual presentation is available here: https://rm.coe.int/presentation-francisco-sanchez-jimenez/1680a0339e

the 15.6% in relation to the criminality in general. Together the evident risk for every victim of these crimes, we have to place severe prejudices to the national economy. In my country, 50.8% corresponds 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 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 point 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 know how 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 mindsets. 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 seeks 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 Center against Cybercrime. It should be necessary the creation of an innovation laboratory that it 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, due to the fact that only with a better knowledge of things we will 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-Report Delinquency Surveys & Cybercrime: The State-of-the-art

Lieven J.R. Pauwels

Director of the Institute of International Research on Criminal Policy, Department of Criminology, Criminal Law and Social Law, Ghent University, Belgium[6]

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 you 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, it is also important to understand why and to understand the mechanisms behind this phenomenon. And this is s 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

[6] Additional material: the author's visual presentation is available here: https://rm.coe.int/pauwels-council-europe2020-cybercrime-final/1680a033c8

online and offline offending and victimization. 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, 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 brackets, 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, the same as 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 into 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 we still do not know about and there is 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. So, 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*, etc. So, 'what kinds 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 brackets- "traditional offenders", 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 increases or decreases in different kinds of offences.S so self-reports can play a role. When you look at the literature of self-report 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, routine activity, theories, but if you try to count them, the overall majority comes from forms of "social learning theory", 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 (and 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, you can see I can distinguish seven periods:

1) *Exploration and discovery of hidden crime* not known to the police, which was already known in the 1940s and 50s.
2) The golden years of *theory testing in the 60s* when people started to understand that the methods of self-report 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, norms are also related to individual differences in crime involvement.
3) *The area of nationwide representative* studied between since the 1970s.
4) I call it the *hyper optimistic period*, the 1980s, at least the first part of it. People were very optimistic about the use of self-reported delinquency studies because they at that time 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? What 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 answers in a socially desirable way, there are people 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 cybercrme / digital offending.

6) *Starting period of the internationalisation*, meaning that many schools start to implement the method os elf-reported delinquency studiesin different countries. And one of the key examples here is the *ISRD* (International Self-Reported Delinquency Study). Publication are available on three waves and a forth 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 regards 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 everybody who has become a victim of cybercrime or who commits these cybercrimes are always online. However, I am not going to say I am overly pessimistic or too optimistic, rather, in between (i.e. realistic) because it seems that many of the traditional findings are being replicated using an online survey. This is a very important thing; it is good news. Bad news is that we might need to

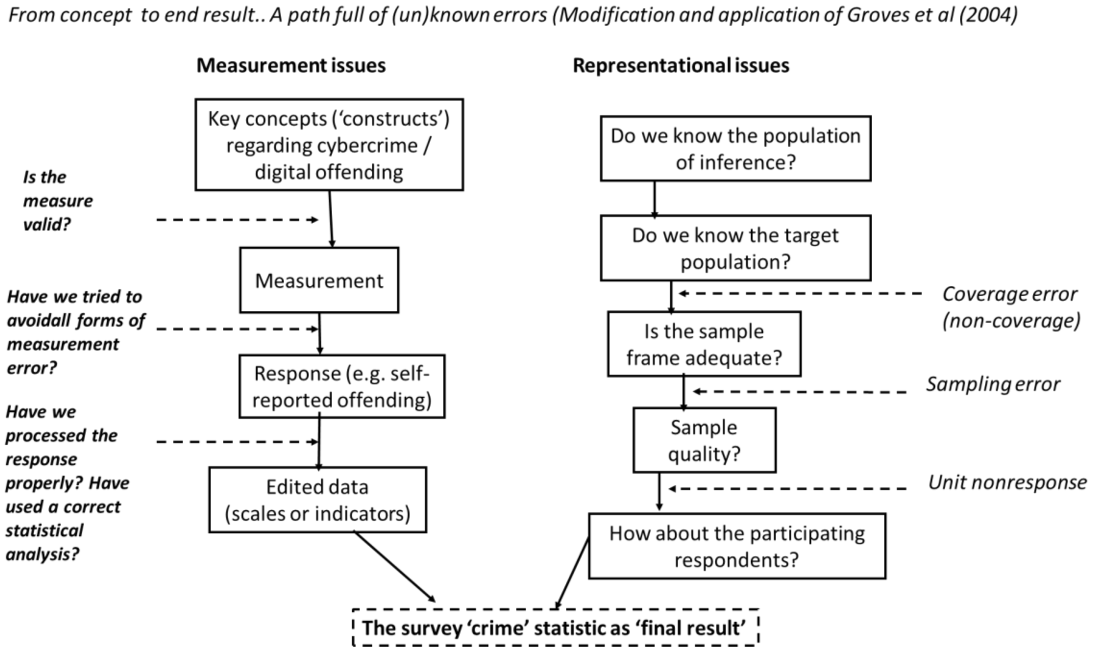
refine concepts and measures but speaking as a methodologist, this might be not too bad because we learn by improving measures and trying to solve methodological problems is a way of making a living (for methodologists like me, just meant as a joke).

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 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 phew number of eople were already recognising the problems of lack of data on perpetrators. For example, one of the first PhD studies on online offending was a study published by Rodgers in 2001, there is the study of Skinner and Free 1997. So, these were the very first published self-reported delinquency studies and if you look at these studies, 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) respondent or (3) questionnaire

Figure 1. Total Survey Error components linked to steps in the measurement and representational inference process (adapted from Groves et al., 2004)


From concept to end result.. A path full of (un)known errors (Modification and application of Groves et al (2004)
Measurement issues
Representational issues
Key concepts ('constructs') regarding cybercrime / digital offending
Is the measure valid?
Measurement
Have we tried to avoidall forms of measurement error?
Response (e.g. self-reported offending)
Have we processed the response properly? Have used a correct statistical analysis?
Edited data (scales or indicators)
Do we know the population of inference?
Do we know the target population?
Coverage error (non-coverage)
Is the sample frame adequate?
Sampling error
Sample quality?
Unit nonresponse
How about the participating respondents?
The survey 'crime' statistic as 'final result'

When conducting research, we obtain results, but our results are affected by both a combination of reliability problems and systematic errors (see the figure above, borrowed from Groves et al, see the PowerPoint presentation as well). 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. Next, 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, to study online of learning. 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, e move to the *measurement instrument* -

the questionnaire item that we have a response of the respondent and respondent also needs to understand the question.Tthe results of the survey statistic 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 means the questions to be understood. It has been done in the field of traditional crimes and it should be done much more 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 influence. 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 can be seen from life course criminology, but it goes with some significant challenges because. Are adults, less willing to report crimes compared to 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 much 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 presented framework (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 like trying to steal passwords, deleting files from ones computer to online threatening. Fewer studies deal with online hate crime radicalisation, which I think are also important issues nowadays, and it is possible to study these phenomena to a certain extent. We should really try to, move on... traditional self-report 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.

We have following challenges from my point of view: violent extremism, hate crimes, sexting, child pornography and also the issue of measuring of 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, digital piracy. And they refer to acts which are being committed in the past 12 months or the past six 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 surveys) .There may be some alternative ways of using self-report instruments to understand digital crime. And this is the randomised scenario study (also called randomized 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 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 examples to be able to know to what extent we can apply this methodology to the different kinds of cybercrime, also the types of cybercrime committed by adults.

I also said that measuring exposure is important. Exposure is about the opportunity structure. People, and especially 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 you 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 activities that they expose themselves to becoming a victim or may be, for example, targeted in the field of violent extremism (i.e. facing the risk of being recruited online).Tthere are plenty of examples people are harassed in chatrooms. So, we really need to find out better ways to measure exposure to criminogenic settings. And one way, I think 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 and with whom are spending their time online, what kind of social network sites they use, …. 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, maybe 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, violent extremism? We know that people are exposed and in one study we conducted a couple of years ago (in the context of to the Sharia for the Belgian case), 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 that this study showed 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 been 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 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 (Wester 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, I think, personal data, and this is nowadays, I think, a very huge challenge because of the GDPR 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, (some of which are related to GDPR).

I have said a lot in a short time. I hope I am still within my limits. Short conclusion: as my colleagues said: *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, so traits and (online) experiences. 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'? Nor 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 is the key to a better prevention.

So,my final word would be: stop the endless testing of seemingly competing theories, which was a typical problem of old self-report studies, because I think we live in the age of integration.

I would like to end by saying: "one plus one, equals three, not two", meaning that by integrating our ideas we have a lot more will 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

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., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Research note: An investigation of reporting behavior among cybercrime victims. *European Journal of Crime, Criminal Law and Criminal Justice.* Accepted for publication.

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 https://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

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

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 http://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, (2013), 24. Available at https://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 http://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. (2010). Criminological theory in the digital age: The case of social learning theory and digital piracy. *Journal of Criminal Justice*, *38*(4), 470-480.

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

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 https://www.cybercrimejournal.com/RokvenetalVol12Issue1IJCC2018.pdf

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 https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/rogers_01.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 http://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).

Q&A Session 1

Ilina Taneva: Thank you very much. We are reaching, we have two more minutes until the end of the meeting. Unfortunately, there is virtually no time for questions, but you can always send them by way of messaging to everybody. You have the possibility to send a question either privately or to everybody by using the chat function of the KUDU system, either today or tomorrow. Keep the questions for tomorrow. Unfortunately, we will not have the last speaker with us tomorrow to be able to answer them. But you can always send in the questions also to him directly on his email. You have the PowerPoint presentation among the documents uploaded. So, unless there is something that ***Marcelo Aebi*** or ***Stefano Caneppele*** would like to say, I would like to close the session and we will see each other tomorrow at nine twenty.

Marcelo Aebi: Thank you very much, Ilina. If we want to say something, it will take long. So,tomorrow we have to wrap up sessions. It will be, we have enough time to discuss at that time, even if *Lieven Pauwels* cannot be there. But we will find a way of communicating at one moment or another. So, I would like to thank all the persons that accepted the invitation to participate. And looking forward to seeing you again tomorrow.

Ilina Taneva: Bye, everybody. See you tomorrow. There is someone who wrote something, uh, Lieven Pauwels said that he will be there in the afternoon tomorrow so he can answer questions tomorrow afternoon for those that would wish to ask him questions. Thank you, everybody. Have a nice evening and see you tomorrow.

Session 2 - Modernising victimisation survey

Stefano Caneppele: So, I can take this mean just to introduce the session today. Welcome back, my name is *Stefano Caneppele*, I am a professor of criminology at the University of Lausanne and with the *Marcelo Aebi*, *Michael Levi* and *Fernando Miró-Llinares*, we are part of the committee of experts that set up this conference. The goal of the conference was to put together a different dimension 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 an opinion and view about the issue of modernising victimisation surveys that we have seen yesterday that crime and criminal justice statistics is not at the moment able to grasp all the different variety of cybercrime. And some of criminal justice experts suggest that victimisation surveys may do part of this story. And this is the reason why we dedicated this session to the discussion of how we can modernise victimisation survey. And that is why we will start with Professor *Marianne Junger* from the University of Twente. She did a very nice and interesting article on the state of the art on cybercrime surveys. And this is the reason why we wanted to open this session of today.

So,just to complete the presentation of the session, so we have Professor Junger that will open the to the discussion around the Modernisation of Victimisation survey, then we will have three national experience Finland, Netherlands and England and then we will conclude the session with a wrap-up discussion about the inputs that we get from these presentations. I recommend to every speaker to respect the time. So, 20 minutes each. And now I again say thanks to Professor Junger to have accepted the invitation and I leave the floor to her just to start a presentation.

Crime Survey & Cybercrime: The State-of-the-art

Marianne Junger and Pieter Hartel

University of Twente, Netherlands

University of Twente, Delft University of Technology, Singapore University of Technology and Design[7]

Thank you very much, Professor Caneppele. Very happy to be able to present some of our work. I just would like to emphasise that I did not do this on my own and we mention that we collaborated with Rick Verkade, who now works at the Security & Privacy department at the Province of Overijssel (the Netherlands). And in case you speak French, if you prefer to speak French, I can speak French as well. So, if you prefer to ask 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.

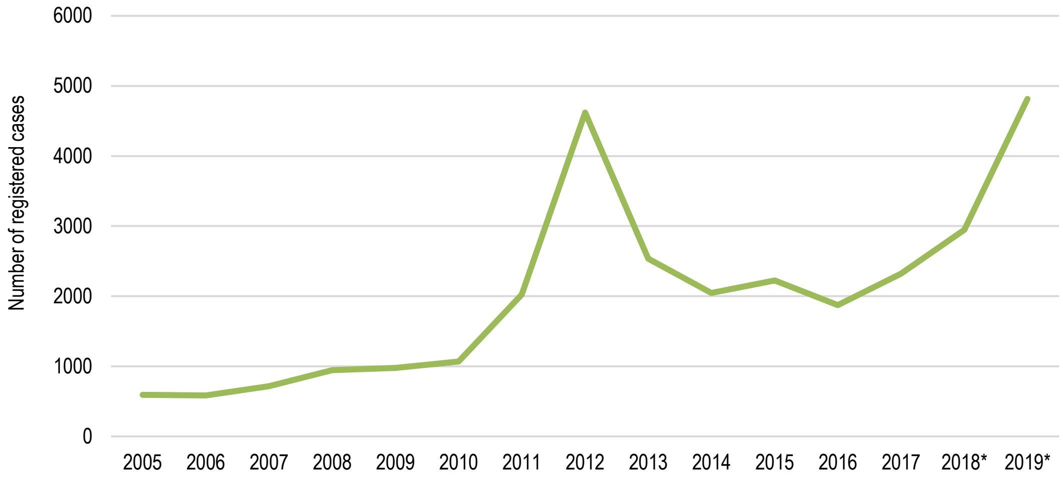
1. Registered police reports

At first, I will present a few data on registered crime. I think someone also showed figures on registered online crime yesterday. Let's start with some concepts. As a whole, cybercrime has been described as a vague concept and even more specific crimes can be 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 (figure 1) that

[7] Additional material: the author's visual presentation is available here: https://rm.coe.int/presentation-marianne-junger/1680a033ae

there is a gradual increase in 'computer intrusions' with a bit of an odd peak in 2012. But overall, the figures are relatively low and suggest a low level of 'cybercrime', as measured by 'computer intrusions', and registered by the Dutch police.

Figure 1: Number of officially registered reports of computer intrusions, yearly counts, in the Netherlands [a]



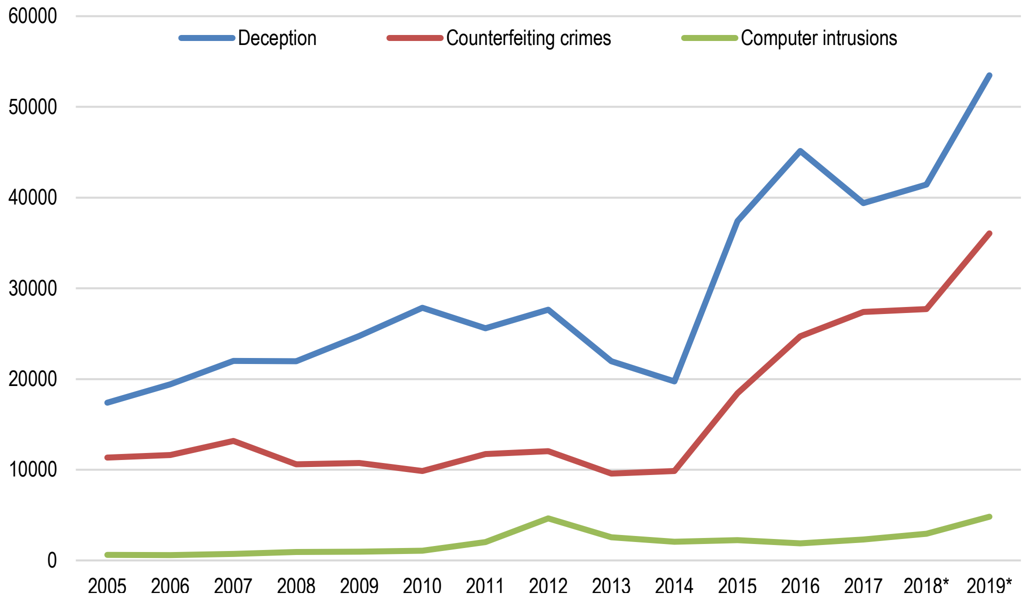
[a] Sources: 2005-2014 CBS statline, 2015 Nationale Politie BVH Stuurkubus. Combined with: https://opendata-cbs-nl.ezproxy2.utwente.nl/statline/#/CBS/nl/dataset/83648NED/table?ts=1603353000816; Hesseling, R. (2016). Wat weten we niet? Paper presented at the Seminar Veiliger in Nederland? Feiten, trends 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' increased by a factor 2.4, 'extortion' by 1.8 and 'computer intrusions' by 3.9 [Statistics Netherlands, 2018 #15885;Statistics Netherlands, 2018 #15884]. Across the world, fraud statistics show an alarming increase with new reached heights in the US (Finklea, 2014; Javelin, 2017), and in the UK (Financial Fraud

Action, 2017), in Spain (Kemp, Miró-Llinares, & Moneva, 2020) and in 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 by the green line. Figure 2 suggests that a lot of cybercrime, 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 were ICT-related and 40% of all frauds were 'ICT-related', meaning that somewhere in the process, ICT was used to commit the threat or fraud (Montoya, Junger, & Hartel, 2013).

Figure 2: Registered crime, fraud and cybercrime[a]



[a]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 with the legal categories of offline crime.

2. Victimisation surveys

I would like to continue with a brief discussion of 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 the crime victimisation surveys have been described by the National Academy of Science, as the most appropriate mode of measuring crime (Aebi, Killias, & Tavares, 2002; Cantor & Lynch, 2000; Gottfredson, 1986; National Academies of Sciences, 2018). Victim surveys have a number of advantages:

- Victimisation data are independent from the 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, like, 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 was mentioned above, it proves quite difficult to operationalise the concept of 'cybercrime'. And one of the reasons, among others, is that cybercrime is often a more complex crime, 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/her. I would like to present a brief visualisation of the crime script of phishing from a Microsoft report (Microsoft, 2020)(figure 3). (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/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 ATM's. If you somehow receive money in a cryptocurrency, in the end you probably want to exchange it into dollars or Euro's. Basically, in the end, the cashing out system is the bottleneck of the entire system (Florencio & Herley, 2012).

The important conclusion here, is that we, 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 so, what can you ask them? And if the money is gone from their bank account, how can they understand what actually happened, where their personal identifiable information came from, how their money disappeared? 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 an 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 until 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 cyber bullying and threats, and for online shopping fraud: when these incidents were described in respondents' own words, the descriptions of online harassment matched what was meant with '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 is 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 onto into 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'll start with Identity-fraud.

Identity-fraud

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

Phishing. Among the 14 respondents who said that they were the victim of identity fraud, in six 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 the 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 (MJ: unspecified what 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 banks 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 that we were unable to categorise the incident as this concerned 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 three were, in our opinion, truly identity fraud; six incidents could be best explained as phishing 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, I would like to give examples of two cases that were actually phishing in our opinion. 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 coming from 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:

- Abuse of an email account sending spam to the contacts of the respondent.
- Someone tried to login from Estonia on the account of the respondents' brother who happened to be in India. However, using 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 to a third party for marketing purposes.

Hacking. One incident was really 'hacking': so-called friends of the respondents' sister were trying to get the 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 be have been counted by Statistics Netherlands', as their questionnaire focusses on victimization 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 kept both incidents with '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 the victim's answers it appears that very often the description of the incident was confusing and incomplete. Also, many victims were at a loss to explain what it was that they saw happening. Therefore, for the authors it was also often difficult to understand the explanation that respondents provided.

The results basically are that, for identity fraud and hacking, of the 27 incidents that were reported half were phishing, and further, mostly identity fraud and skimming. Table 1 summarizes 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**
Cyber-bullying/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 conclusion, to measure cybercrime victimisation, as a research community, we 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, the speaker from Estonia mentioned that he and his colleagues have a question about phishing.

We also suggest researchers have '*an offender bias*": we ask questions about what 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 3500 surveyed respondents (employees from 7 countries: US, Australia, France, Germany, Japan, Spain and the UK) are not sure what the term phishing means. The older generation (55+) knew this better than the younger generation (18-22).

Furthermore, it is difficult to ask questions from the point of view of the law, it easily leads to lengthy and complicated questions. This certainly happened with some of the questions of Statistics Netherlands (above). In their effort to kind of copy legal categories that 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 for a dimensional approach. I think 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. On the one hand of the dimension crime is completely physical, on the other end of the dimension crime is completely digital. A lot of crime has 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.

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 propose is that we experiment more to learn better how we can improve our measures of cybercrime. So, for instance, we could experiment with other questions, broader questions, more precise questions and ask things like 'what happened to you, can you describe this?'. We have tried in the past to help people with their IT problems, and ask them about their ICT-related behaviour, like 'Okay, can you tell us 'how do you deal with your PC in practice?', and then, also check in their PC if one could find evidence 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, also ask about fraud victimisation, and then ask about eventually the online and offline aspect.

Multi-disciplinarity. And then perhaps we can improve by working more with other disciplines, by including, for instance, computer scientists. This would help us in trying to understand what happens in the technical sense, what is happening on the computer system. Use alternative measures, like 'can we see or measure how much phishing emails are coming in?'

And so, let us well, in conclusion, pay renewed attention to measurement issues, it matters for policy as well as for prevention, I think a stayed within my time limit. So, thank you very much. And perhaps someone has questions.

If anyone is interested in more information, they are welcome to send me an email.

Stefano Caneppele: Thank you very much, Professor Junger. I suggest that will put the question to the end of the session. So, it is very good link that you are doing with the next presenters, which will discuss the national experience in the Netherlands. One instance on the concept of audit. So, I ask *Johan Van Wilsem* to join the floor.

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. Avalaible 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 Retrieved from https://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. Avalaible at https://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. *Criminal Justice and Behavior*(4), 85-138.

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.*

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 https://www.usenix.org/conference/enigma2019/presentation/lusthaus

Microsoft. (2020). *Microsoft digital defense report, september 2020*. Retrieved from https://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. https://ieeexplore.ieee.org/abstract/document/6657122

National Academies of Sciences, E., 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. Retrieved from 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

Netherlands: National Experiences in Cybercrime Surveys: Challenges and Lessons Learned

Johan Van Wilsem
Court of Audit, Netherlands[8]

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 pieces 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. So, over a 10-year period, including overall six waves, each time approximately 6,000 respondents. And as a panel study, we tried to include as many as the same respondents as possible. On this study, I published all kinds of articles and chapters. 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 myself from these studies. *Lesson number 1* is that it is very valuable to conduct panel studies; victimisation studies overall are based on a cross-sectional design. So, one measurement in time, either a representative sample or not, but it sticks to one-time only measurement. In a panel study, we have the same respondents, but we have multiple measurements over time from these same respondents. This allows for new things in comparison to cross-sectional studies because it

[8] Additional material: the author's visual presentation is available here: https://rm.coe.int/presentation-johan-van-wilsem/1680a0339f

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 so-called *super targets*. Additionally, apart from this career perspective, panel studies 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 policy-makers are actually effective in reducing victimisation risk? To name an example in a cross-sectional study in which we ask for victimisation as well as the security measures target to take to protect themselves against cybercrime. For instance, a firewall or having wireless a secured wireless Internet connection. In a cross-sectional design, 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. So, that technical protection measures, not so much are the resultant of less victimisation, but the victimisation is actually the cause of increased protection measures.

In order to identify some more about the career perspective for the data that we collected in six waves, I took a comparison of two types of where we can look at that data (Table 1). The left column, you see all the data that was collected in this 10-year period, which results in approximately 13,000 respondents that participated at least once. In the right column, you see a selection of those people that participated each of the six times we asked them to participate in the LISS panel. Most respondents are not willing to participate six times. So, that's a much smaller group of thousand people. For both groups, when you look at the left or the right column, either way we are able to follow most respondents for a longer period of time. And so, in regular cross-sectional studies when we ask about victimisation over the past year, we see for various cybercrimes a few percentage points. But when we are able to follow people over time, and in this case a 10-year period, it is a quarter of the people. So, if you either look at all the data that was collected or if you look at the people that participated each six times, it is a much larger number of people that say: "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

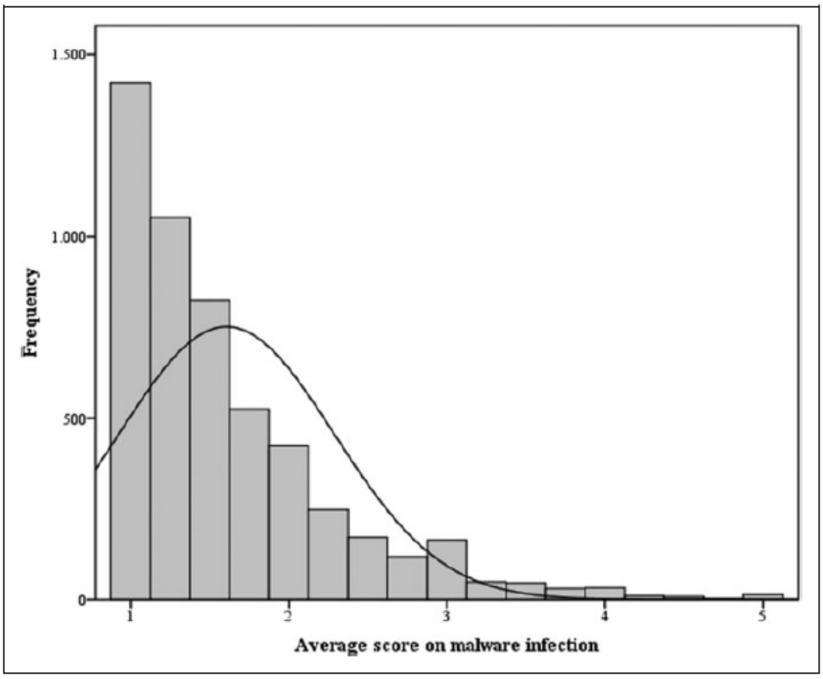
	All respondents, participating at least once	**Respondents participating all 6 waves**
N	13,430	1,072
Cyber victim 2008-2018	24%	38%
Victimized 1-2x, among victims	75%	72%
Victimized ≥ 10x, among victims	3%	3%
Share of incidents experienced by super targets	16%	13%

When we look at the group of victims, which is either a 24% or 38% depending on the selection, if we look at those victims, the most people are saying "I have over this 10-year period of time being 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 when you collected over these six waves, the amount of people, the number of victims that say "I have been victimised 10 times or even more", is approximately 3%. That small group is involved in approximately one in six victimization incidents. So, a large concentration of victimisation in that group.

The second lesson I learned from these studies is likewise, as *Marianne Junger* said, 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 knowledge how that came about, or a new program about appeared on. Each of these computer problems may not be a definite sign, but at least it is indicative of malware infection and it is an alternative way, instead of asking people if they have been the victim of a malware infection. Most responders will have a hard time to recognise malware infection occurring to them. So, the answer to such victimization questions would probably yield are less reliable than questions about things that people are much more able to indicate, and that is computer problems. These malware infection indications may actually accompany cyber victimisation at a later point in time, such as being hacked. Therefore, possibly if we are able to identify if people have certain computer problems, 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 being a victim of a computer crime.

What we did in this next slide is asking a range of four types of computer problems in the examples that I showed you, ask people how many times they experience this on a (1) to (5) scale. One means "This hardly or ever happens to me"; five 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, if we average out these scores for respondents in a panel study, most of the respondents luckily say that they are 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 that 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 three: it is worthwhile to ask questions among victims about the actions they undertook and also the outcomes that these actions led to. This is not a new lesson because, as you all know, being familiar with victimisation surveys, it is quite familiar to ask victims if 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 if the victims actually were successful in getting their money back. So, if they were being reimbursed by their bank, what were 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 over an eight-year period we started asking questions about banking fraud in 2010 in the LISS panel, was to ask 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, so the amount of cash that was withdrawn illegally from the bank account was varying between victims. Ten percent of the victims say this was about an amount of Euros that was 1000 or more; also, a group of people said: "well, it was relatively not so harsh", this quarter said it was 50 Euros or less (Table 2). When we look at the *eventual* loss, we see that the reimbursement policies in the Netherlands seem to be quite generous. So, 80% of these victims eventually did not have anything to lose. So, it was completely reimbursed, which left the group of approximately 20% with additional financial losses. And most of the time, not too large amounts. But sometimes these were considerable amounts of for instance, up to 250 Euros or more. This was a minority but, nonetheless here as well we can see can we relate these outcomes to the actions that people undertake and the characteristics that they have (e.g., age, educational level, self-control).

Table 2: Amount of financial loss after banking fraud (N=636), Data from 2010-2018

	Initial loss	**Eventual 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
€ 1000 or more	10.1	0.9
Unknown	18.4	1.9
Maximum loss	€35,000	€10,500

And I want to go to the next slide and share the last lesson with you, and that is that 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 proven to be a prime predictor of the issues 1, 2 and 3 that I just talked about. This means as much as 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 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 low self-control people, considering the fact that they are less inclined to contact the banks after the victimisation, which in consequence leads to less often receiving a reimbursement from their bank after banking fraud. So, the portion of 20% that are left with eventual loss, we see a concentration among the group with low self-control. And that means if we look at efforts for prevention of victimisation, it yields the largest benefits if we are able to do this successfully among the group with low self-control. This is simultaneously a very hard task because successful prevention is difficult for people with a 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 are among which we see that the risks are concentrated.

Thank you for the attention. I understood that we have questions at the bottom end of the session. So, once again, thanks for the attention.

Stefano Caneppele: Thank you very much, Johan, for your presentation. Very interesting. And many inputs that I am sure that will be discussed later on. I ask you just to come to *Matti Näsi* from the University of Helsinki to join the floor right now. As I said, the question will come later. I will ask later to all the speakers to join the floor again for the questions. But right now, it is time for Matti Näsi to present the exercise that Finland did about victimisation surveys.

Finland: National Experiences in Cybercrime Surveys: Challenges and Lessons Learned

Matti Näsi

University of Helsinki, Finland[9]

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 in 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 of national level threats and sort of 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 cybercrime and cybercrime victimisation as well.

From a criminological perspective, I do not think that we have established a very good picture or laid very good foundation in terms of understanding what our situation currently is, especially in terms of the hidden crime aspect, in terms of the victimisation experiences of those that do not come to the attention of police and official statistics. And this is in a way kind of surprising because Finland is a very tech-savvy country, has been for decades the big IT sector, the industry that does have a big influence on the society in general. But despite this, we have very little information or relatively little information regarding criminological perspective or cybercrime perspective on

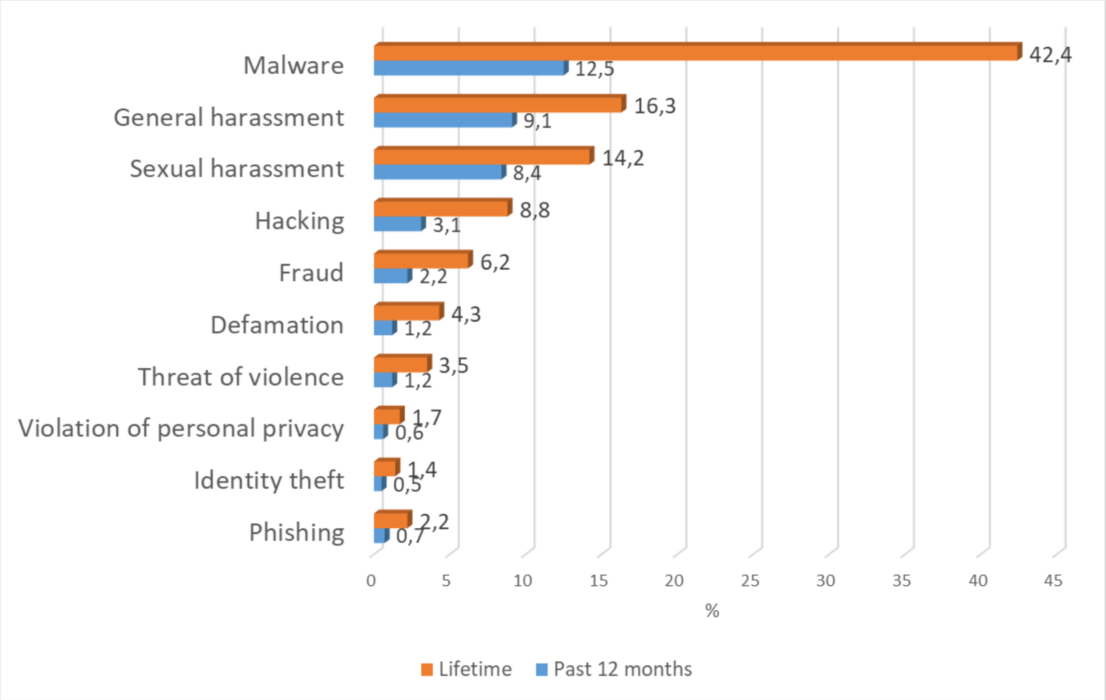
[9] Additional material: the author's visual presentation is available here: https://rm.coe.int/presentation-matti-nasi/1680a033af

this matter. So, there is 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 honesty, the problem with official statistics that they tend to tell us relatively little: official police statistics, for instance, in terms of fraud, last year there was 29,000 cases of fraud recorded by the police. However, from the statistics, we cannot really tell whether it was an offline fraud, online fraud or some sort of hybrid fraud. So, we do not really have means to establish whether that incident took place or what environment took place. We have seen a steady increase in fraud crime statistics, and we speculate that this is to do with because of increased online offending. But the statistics itself, it is not yet a good tool that it could be in terms of revealing the details in many of the offences. This is an example of hacking cases where we do see a great division between years on how many cases are reported to the police. So, there is a lot of instabilities in terms of how good the information is and how reliable, 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 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 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, 2009, and it was about 40,000 participants and it was representative of 15-70 four years old. And in it there was a question regarding cybercrime victimisation. However, the question was very vague or very general, and it was just the respondents being a victim of crime via the Internet. So, that does not really give a very detailed information about the phenomenon in general. So, there was a lack of detail, population-level information regarding cybercrime, victimisation prior 2018. Our aim was to try to fill this void a little bit in 2018 National Crime Victim Surveys that we collect every year in its current form, it has been collected since 2012, but the earlier version has been established already in the 1980s. So, it is a very established measure, very established tools of collecting victim surveys. It usually focuses on traditional crime victimisation: property and violence. But in the 2018, we decided to include a cyber module in it. And the aim is hopefully to include this cyber module in every four years so that we have information on a continuous basis. So, hopefully we can make that happen. But this survey is collected by our institute at the university. So, it is not the statistics centre in Finland, but it is in our institute. A little bit about the description, because this relates to the challenges we have with this survey, so, of course, it involves the basic background information, age, gender, education, financial situation, etc., and the questions about offline traditional crime victimisation. In the cyber module, we also have items, not just the victimisation items, which were 10 different types of cyber offences, but also questions regarding the behaviour, online behaviour of the respondents, so their online behaviour and activities, their online skills, as well as questions on what sort of measures they take in regards to their use of protection, password use, etc. In the 2018 survey, we have a sample of 14,000 and the response rate was about 39% and it was a representative of the 15 to 74-year-old Finns very well.

Now, here are some of the items and sort of the prevalence rates regarding lifetime and past 12 months victimisation: we see that malware and forms of harassment were the most common forms of victimisation. If you compare this to the article that Marianne and her colleagues published a 2018 there, for instance, the prevalence of harassment tends to be much lower in many of the national level surveys. So, this may reflect that our item might be a little bit different from those studies. Here, you also see that we were there was some calls for fishing information, and we have that here. Our Estonian colleagues yesterday had a much higher prevalence rate of fishing and I predict that this is mainly because the item is different. In our survey, we did not ask whether they had received fishing messages or fishing attempts, but we collect the information regarding whether the respondent had given out their username, password or credit card information as a result of a phishing message. So, whether that message or the phishing attempt had been successful, not whether they had actually been tried to be a sort of whether they had received this type of phishing message.

Figure 1. Cybercrime victimization in Finland 2018, lifetime and past 12 months (%)



Another interesting aspect with the victimisation prevalence is that if we look at the 2009 survey ten years ago, and although the item was very general in it, the 2.5% of the respondents reported some form of cybercrime victimisation in the past three years. However, 10 years later, in 2018, we have 55% of respondents have lifetime victimisation experiences, and 35% of the respondents reported some form of cyber victimisation in the past 12 months.

So, in this way, it would seem that the rate of cybercrime victimisation has tenfold it. But it may be due to the study design and the question design that may influence that the prevalence rates because ours was much more detailed information. So, that might influence the prevalence rate in some sense. But I think it is still an interesting finding that there is a big difference in the 2009 survey that 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 regarding victims than offenders. It also dictates that this type of, well, this type of information that we tend to collect, it makes, at least in the case of Finland, it does make the research on crime and cybercrime a bit more than one-dimensional compared to traditional crime. And I say this because many of the types of offences, they are very specific and you need specialist skills on hacking or it may be malware or fishing and that it takes a much more sort of sophisticated approach than, for instance, asking about online harassment, whether someone has been harassing their partner or partner or someone they know. So, from an offender's perspective, it is that research design, you know, it 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 just been focusing on the victim perspective. That has been said in previous presentations, it is an umbrella term. It makes it is very vague. So, what forms of victimisation to actually focus: whether we focus on those more computer aided, computer enabled offences versus malware, phishing, etc., or do we also include items of harassment and defamation and so on, threats of violence, etc.? So, whether there should be a separation in the studies or whether they should be sort of all, you know, be brought together in some form of victimisation surveys, I do not know. One question is also who is the actual intended target, whether the respondent actually have been victims personally or whether they have been a victim in the case of collateral damage, i.e. if your own if your bank is facing a denial of service attack and the bank is down for three days and you cannot buy anything and you cannot use a 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 major hacking incident where a hacker downloaded a patient's records from a company that provides psychological counselling services. It has been a massive breach of information. And the discussion is also, of course, about the victims, but it is also about the level of cyber security. And some of the discussion is about the level of cyber security of these individuals. But in this case, they were not victims because they had a poor password or they were active online and exposed to potential offenders, no, they were victims because they were using a different service that they were using a service provider that has nothing to do with their online behaviour. So, it is just there is so many levels of victimisation here that it is the key to try to establish who's the victim and whether they were primary victims or not.

It is just an abstract, we also have challenges with the survey design in general is about how to ask how to get set up the questions and how to get the sort of relevant information and detailed information that we were actually looking for. If you look at different cybercrime, articles that are being published, there tend to be quite a bit of variation in the measures. So, there is a measure of items on how to ask, how to ask about victimisation experiences. So, there is not really established measures and questions that are in use. So, I think we could use some you could use it with 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 statistics in an international context as well. Questions regarding the background variables such as online behaviour of user protection are even less established. So, in terms of looking at the risk factors and how individual sort of routine activities and behaviour online might influence the risk of victimisation, we need good background information variables, and I think there is even less established measures and questions regarding this type of information in the field in general. Many of the most cited studies that use these sorts of more advanced experimental study designs (and they tend to be American studies), they also use data or samples that are not very good. They usually college-level samples and that 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 they cost a lot of money to collect these population-level studies. I think the emphasis in the future research should be on studies that use a good and representative data rather than always this experimental and small sample data. But in our case, the biggest challenge is the declining response rate in surveys. And I am not joking about it about this. But if the current trend of the rate of decline in responding to these surveys, if it continues as far as past the past five years, in 2030 we do not have any respondents. In the past five years, our rate of response has declined almost 20%. So, it is a massive problem if this same trend continues, we do not get reliable data on this sort of hidden crime aspect. So, it is a big problem.

So, few lessons learned from the survey. Well, cybercrime victimisation, if you look at the victimisation trends in a traditional crime in our survey, violence and property crime, what is also interesting, we asked about what the people were afraid of, certain types of crime victimisation. We asked about cybercrime victimisation as well as violence. And over half of the respondents reported of 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 of being afraid of violence victimisation and cybercrime, victimisation is in a way a big threat or is perceived this as a significant threat in terms of people's responses.

When we talk about the official statistics, the challenge is that the sort of the case of hidden crime seems to be particularly strong in the cybercrime context, because only 2% of the victims have actually reported their incident to the police; so most or majority, vast majority of these types of victimisation experiences are not known to that official statistics. Of course, there were differences between offences; fraud offences were reported more likely to the police than some other forms of victimisation. But in the case of fraud, it was only 10% that 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 better bigger picture in terms of the victimisation in the cybercrime context. And I am keen to sort of international collaborations in terms of developing better study designs and measures and items to have sort of good ways and solid ways of collecting this type of research. Thank you.

Stefano Caneppele: Thank you. Thank you very much, Matti, for your presentation. You work perfectly on time. So, we also appreciate the fact that you respect the schedule. In the meantime, we made available the presentation that you did before, and so you can find in documents, you can download it. And now it is the turn of *Billy Gazard* from the Office for National Statistics, Center for Crime and Justice.

England and Wales: National Experiences in Cybercrime Surveys: Challenges and Lessons Learned

Billy Gazard

Office for National Statistics, Centre for Crime and Justice, England and Wales[10]

Thank you for inviting us to the meeting and to share an update on measuring cybercrime in England and Wales. Next slide, please. So, I just want to give you really a 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 in England and Wales, just to give you some brief information, it is a randomly selected cross-sectional survey, representative in England and Wales. As a whole, is conducted by face-to-face interviews in people's homes using trained interviewers and a structured questionnaire. So, we approximately interview about 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. So, we ask people about their experience of crime in the past 12 months. And we have a long-standing 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 asked about additional topics such as perception of crime, domestic abuse and drug misuse.

In terms of measuring cybercrime in the survey, so in the long-standing time series, we obviously concentrated on more traditional offline crimes. But given the changing context and more people being online and the ability to

[10] Additional material: the author’s visual presentation is available here: https://rm.coe.int/presentation-billy-gazard/1680a0339c

conduct crimes with online help, in 2011 the National Statistician's Independent Review recognised the need for 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 misuse of time classified as national statistics in 2018. And symptoms of the development work, I guess the main kind of challenge was around how we classify these offences and how do we make it in a way that is simple that our users can understand, so that we can classify if an offence has taken place. And we did that by separating our offences into *non-confidence frauds*, where use of personal information has been used for gain and confidence, versus *frauds where deception has been used in use in order for gain*, whether that be financial gain through tricking someone into in terms of online goods, for example.

And so once we actually decided how best to kind of fit our questions so they could be easily understood and would measure fraud, then we were some of the additional challenges that we faced were making sure that our classification closely aligned with Home Office counting rules. So, the national standards for how police record crime as well as far as possible. But obviously there are some differences. So, for example, who is the victim? How many victims? Obviously, the crime survey is a 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, with traditional crimes, we are able to obviously record when an incident took place - with fraud and cybercrime is a lot more difficult, so we move to a recording against when the victim came to know about the fraud rather than when it took place, and also existing victim forms that we had in place before we introduced the fraud and computer misuse questions. And it was important to distinguish whether the crime took place geographically within England, Wales, whereas obviously with computer misuse and cybercrime, we do not always know, given the complex nature of these offences and the global nature of them, we decided not to ask where the incident took place for these incidents of fraud and computer misuse.

And so, kind of what we came up with and what we are able to now produce in our statistics are a range of categories on 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. So, this includes unauthorised access to personal information as well as computer viruses. So, these modules are really formed in a way that could we also measure the online part of this fraud as well. So, we know that we can divide fraud into kind of offline fraud and online and then computer misuse; we have those questions added in 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, how many in some way are related to cybercrime.

In terms of what we know right now, we have been collecting and producing statistics on fraud and computer misuse since the early March 2017. So, we have an obviously a much shorter time series compared to other crimes that 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 crime survey and 53% of these incidents were flagged as cybercrime. And so, you know, a huge volume of incidents of cybercrime, even just when it is just looking at fraud. In addition to that, there were just sort of one million incidents of computer misuse as well. So, 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 like it is 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. So, only 14%, for instance, in that year, which is the case for action fraud. But we do ask questions about the further questions on the nature of fraud, so we do ask questions about whether they have reported banking fraud to the bank, for example. We also have the impact on the victim method, reason for the initial contact with the perpetrator, satisfaction with reporting body responses, as well as questions around the experiences with computer viruses and security measures that people take online. And a lot of this we have reported in our main publication on nature, on fraud and computing, with this latest one being published earlier this year.

So, obviously, we have got this set of screeners in place, but we are constantly trying to make sure that we improve the questions, we are so that we can find out more about the nature of these offences and how they take place so that we can help policy makers in government. The most recent round of questioning development took place last year, and it focused on how we can identify for the offences that are facilitated by a computer misuse offence. So, for example, when someone's personal details are hacked and information is gained by fraudsters to enable 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 are. So, these were due to go into the questionnaire in April 2021, but obviously this has all been affected by the coronavirus pandemic. So, 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. And 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 really make some operational adjustments to 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. So, it took us nine weeks from the date of the suspension to go and live back into the field. We had obviously quite a big challenge 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 *recontacting 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 recontacted and in order to make sure that we had enough sample that we could continue to measure crime until we estimated that face-to-face interviews might again become a possibility. We set this up as a panel design and we set up as three waves. So, we are going back to respondents every three months to ask them about the previous three months experience of crime. And this was 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, it is very, very similar to the face-to-face question that has been running since 1981, and so we have the same screening module, same victim forms, so we can continue to measure crime, have our crime estimates for crime and also for fraud and cybercrime and all other modules. We did not have space for 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. As well as making sure that we collect up to date demographic and social economic indicators. We managed to publish our first estimates from the newly set up a 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 to 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 survey mode. But this 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 in on how it has impacted on crime levels. So, we have produced our statistics in a way that we can look at the instance and what particular time period they took place in within that 12-month reporting period, and what we are able to do is to look at the change in crime between the January to March 2020 period with the April to June 2020 period when we have had the lockdown, restrictions had the most impact on people's lives and on crime trends. And what we found was there was no significant change in fraud and computer misuse during this time. But this needs to be taken into the context that we have at the moment smaller sample size. We have only been in the field since the end of May. And also, we are only looking at the instance within a quarter rather than a whole 12 months as well. So, that has an impact on the sample size uncertainty around those estimates. So, we will need more data really to see how the impact of the pandemic will be and what the impact has been on fraud and computer misuse offences.

Some of the challenges that we face during the pandemic in terms of measuring crime and this includes cybercrime, as I alluded to just before, the facts. So, the impact of moving to a telephone interview on estimates and comparability over time and uncertainty, so the smaller sample size accounting for the services on, say, having more complex waits 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 around recall bias. So, the possibility of more instances being reported in more recent quarters than the causes 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 addressing the user need and making sure that we are flexible in our data collection and the way able to add in questions to the survey and 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 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 very well may be future updates to how the Home Office counting rules for reporting crime. And we need to match where possible while also balancing the time series as well, and continue to work with our partners to make sure that now we have the current situation where we have maybe a little gap in the data: that 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 also, we have done some development work recently around child cybercrime, and we have added a module to the 10 to 15-year-old survey. And the first results of this are going to be published in February 2021, where we are looking at estimates of the prevalence and nature of online activity among children, including speaking strangers, sending receiving images and online security, using data from the 10 to 15-year-olds.

And so, for those who are interested, there are some recent publications up on our website, and so our most recent publication on the 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.

Q&A Session 2

Stefano Caneppele: Thank you, Billy, so we can turn off the presentation, I may ask to all the presenters of the morning session to join the flow. I think that the architecture the infrastructure should support the multiple speakers on the floor. So, is it possible to invite all the. No, no, it is not possible. So sorry. OK, if it is not possible, many very interesting input so we can ask to talk to the participant to address some question to our speakers. I can live some minutes. Maybe someone wants to think about the question you or she wants to address to our speaker. I think the generally what we found from this morning session is that we cannot measure everything even through a survey. And the victim survey has some limitations in terms of what we could measure, because our, let us say, people that should be interviewed should not be aware of what is going on or they are only one part of the puzzle. And so that probably the most important question is what we should measure. We have seen that most of the measurements are focusing on fraud, which is a little bit awkward compared to the older victimisation survey, because it was generally said that we cannot measure fraud through the traditional victim surveys, since people are not really aware of fraud in many cases, but now it seems the best indicators to measure compatibility through this using victim survey, which means that even the issue of measurement is changing. And there are other issues related to how we could monitor the evolution. Very interesting, the input from the idea of the adoption, the final stages from the Netherlands, and also the fact that the other issue which was being raised by Finland, is that the declining response rate may be an issue for next year. And finally, again, the different from England and Wales. Just to show how the issue of measurement of what we should really measure again is the big question we should answer for next year. Of course, there is already something very well established, but now probably if there is someone who wants to ask a question… Maybe my question is what kind of cybercrime should we measure through victim crime survey -

to all the participants-? And what do you think whether we should extend to some other forms that have not been monitored yet? Or we should just try to focus and to try to make more consistent and comparable figures across different countries?

Billy Gazard: I think you I guess something that is coming in, so England and Wales, I guess, from some of our policy-makers and some of our users, and particularly of the current period, there have been a lot of questions about how the pandemic has impacted 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 asking if that is the case. I think the telephone survey data that we have enabled us to answer that question. I think we probably do not quite have enough data yet. The sample size is to really answer that question. As I said, we did not see any kind of significant change in fraud and misuse of pre-pandemic and kind of during the current time, April to June period. But we did see, although they are not significant, we did see a slight rise in those offences using the survey. But we need a bit more data first to see if that does end up being significant when we have a larger sample size. Also, we have the issue of recall bias. So, people possibly reporting more fraud in the most recent quarter than preceding quarters. So, for me, I think it is going to be a very important question to 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 what the method of that fraud is and knowing the nature of the circumstances of that which 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 that the landscape of cybercrime and in particular fraud online has changed during this 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, as Matti stressed the fact that there was a trend of declining response rates to the survey, so are you and come from the same issue in England and Wales? So, are people more reluctant to participate in the survey or to your experience?

*Billy Gazard***:** Yes. So, I mean, I would not say we have had; we have not really had that issue with 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. So, a lot of the other national surveys have seen a decline in response rate for some reason. We know we have definitely thought about why is this; and we have managed to keep a higher response rate; and we were thinking maybe it is because people, you know, with interest to talk about their experience of crime are more willing to share that. But given your experience in Finland, maybe there is something else going on in terms of how we interact with respondents, how we do recruitment. I am not sure; we have seen a small drop off in recent years. So, we were always above 70% in recent years. We had a year recently where we dip down to 69% and this year obviously was slightly lower. But that was really impacted by losing two weeks of fieldwork. So, we are not too worried about it. But it is a trend that we have seen across other surveys, but not in crime. But having said that, in the current circumstances, if we were to go back to randomly selected households and going back into the field, this is obviously going to be completely impacted by the mode: I think it is much easier to recruit people when we are knocking on people's 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 if that is the case.

Stefano Caneppele: Thank you, Billy. It is Matti Nasi, then Michael Levi and Johan van Wilsem asked to take the floor. So, we start with Matty.

Matti Näsi: I think one of the basic issues here is that in Finland, it is a postal survey. So, since 2012, it has been a postal survey. Before that, it was a household interview or phone interview. So, that's, of course, changes that the playing field a bit. But within the eight years time that it has been postal survey, we have seen almost 20%. So, that might in part explain that the change in the response rate. But why so steep? I do not know. Of course, what it is interesting when we compare our older surveys that were used or collected in telephone surveys, we saw a difference in terms of reporting, for instance, domestic violence, because if you do the phone interview, you might have the other person within the room. So, it is difficult to collect information regarding domestic violence if the other person is in the room. So, we have seen that in terms of violence, we have seen a difference in terms of response or the prevalence rates when the measure of collection was actually changed. But I do not know if this decline in other countries is also to do with what the postal service and whether it is that people just do not respond in a paper survey, although they can do to actually fill a questionnaire online as well. They have to link that in the mail. But I do not know. This may be that it is better to keep the prevalent response rate higher when you do that in-person interviews or telephone interviews.

Stefano Caneppele: OK, thank you. Thank you, Matty. So, now it is Michael Levi.

Michel Levi: Fine, very interesting presentations. Thank you, everybody, this morning. Maybe a point of information: first of all, of the unusual features of the British crime data is that the we also add information coming from the banks. And from CIFAS, not for profit body, so those data are added to the crime survey data to constitute our crime statistics. That is a very uncommon feature. But reliability tests had to be done before that was done. The other feature, if I can just add to the presentation, which was excellent, was that the National Cybersecurity Center has instituted a new direct reporting system report for reporting of phishing attacks. Now there is an issue of demarcation between that and Fraud action. Fraud has come to a lot of criticisms, but it is a very clunky system. But the national cybersecurity system is very easy. If you get something, you suspect of being a phishing email, you just forward it to the phishing address and they do whatever they do with it, but that they are not there is any expected criminal justice outcome. From that, and there is no compensation, you know, there is not really an economic a direct harm that is anticipated. So, when we start adding these different sources and trying to avoid duplication and overlap, then we can build a better picture. And I suspect that National Cybersecurity Center, which tries to intervene on the basis of the volume and nature of fishing to take down websites, etc., that produces a better rounded portrait if we add that to the very important crime survey data. And it was fascinating to hear the adaptation. So, I just thought I would say that is really a point of information for us to be thinking about going forward. Now, there are not any parallel organisations to Cifas in any other European country. There is a more limited version in the Netherlands, but there is one in. But the banks, the European card producers could easily do that through the system. If you were thinking about that and the final edition, I want to make is that I had just done a study. It is going to be published by the Australians soon with the Australian Institute of Criminology, looking at what we know about trends in fraud and that since the Spanish flu. So, of the last hundred years, looking at fraud pandemics and economic crises and I have a small grant, 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 in mostly in Europe since 1850. So, that's a longer thing. We cannot reinterview people in 1850 for the recall survey, but that might eventually be useful. So, there is a bit of academic work going on in this space. Thank you.

Stefano Caneppele: Thank you, Michael. It is true that there are a variety of institutions that are collecting different types of data on cyber incidents or not really some cyber fraud linked to their institutional goals. Of course, we can see that the information is a dispersed and it is getting a bit outside of the criminal justice field since many people are aware that the criminal justice cannot do much on, let us say, dealing with this kind of issue. So, the point here is that should we set up a sort of partnership between a different connection between the countries and institutions to provide this a more complex picture of cybercrime. But now there is Johan who asked for taking the floor. So, the floor is yours, Johan.

Johan van Wilsem: Yes, thanks. Just a short contribution. And going back to your original question, I believe, is are there additional crime types that we can measure via crime surveys? And I am not pretty sure about that. And I think the main work for this moment is trying to figure out what the best ways are for the current crime types that we include in surveys and how to measure them. And if we actually need to stick to traditional victimisation surveys or in terms of as valid answers as possible, taking detours. Because the question is, when it comes to computer issues and we call it *issues*, I am not sure that everybody perfectly is able to assess what victimisation experiences he or she has gone through. So, that's why the computer problems are just an experimental way to a certain, if it has any, bearing on real victimisation experiences. And I think we need to do more work on that, more work on the experimental field, how to actually give our questions to respondents and if they need to be 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, so making work additional questions on could you give us more detail on what actually happened, how much money you lost? You can do that in a quantitative way, but also, I think qualitative work is very important in which people just tell their stories. So, in order to be more able to understand what the crime actually is, because the field is, in my view, lacking that point.

Stefano Caneppele: Thank you Johan. I have two more questions for you. The question was about what Lieven Pauwels was saying yesterday regarding the difficulties: difficulty to carry out a panel survey due to GDPR. I have seen that you started in 2008 with this panel survey: is this GSPR affecting your capacity to continue on? which you say under which condition you are allowed to continue with the panel survey?

Johan van Wilsem: So, I see you mean continuation of this panel?

Stefano Caneppele: Yes. In terms of this GDP is limiting your capacity in carrying out this kind of survey?

Johan van Wilsem: Well, actually, it is for the past year, we got funding on all kinds of sources, including from the Ministry of Justice and Security, but we are looking right now for additional funding. And it is actually quite a hard task, which is surprising to me because I think long-term victimisation panel studies are rare and we can learn quite a lot from them. So, yes, this is an issue.

Marcelo Aebi: Stefano, I think that there is a misunderstanding because we are using these abbreviations all the time, GDPR and this...Stefano is talking about these regulations of the European Union on the protection of personal data. Now, when you go to any website, you have this information, "When you put cookies, you accept it" and so it complicates for some person, I am not sure because you are losing a panel, but for other persons, the control of privacy is creating problems. I think the question was that one. Is that the case?

Johan van Wilsem: I see, I am sorry for the misunderstanding. We have not looked, we are doing this panel study by the research agency centre data.

So, they are the research agency and I do not think they have any serious issues with this. So, my answer to that question would be no. To be short.

Stefano Caneppele: OK, so that's interesting. So, probably from an academic perspective, this could be an issue, not for a public institution, of course. The other question was related to your findings that you got regarding the fact that there was a huge concentration in terms of serious repeated victims. And you are saying that their best predictor was a lack of self-control as the most convincing and consistent dimension that you found in your research, but this opened the issue in the debate about how we can prevent, as you said, the main change, this persistent rate, which is difficult to change with some awareness campaign and so on. And so, did you consider, did you set up any special programs? And we are just, as I say, connected to the next session. But is there any special program in place to work on reducing or increasing self-control in cybercrime victims or to your knowledge, in the Netherlands?

Johan van Wilsem: No, it is not that I am aware of that. If you think about how to 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 is, is there an alternative to that? And I think it would be viable to investigate if all kinds of messaging warnings which are focusing on short-term outcomes: if you click this button, then maybe this will happen, might be an effective strategy for people who have trouble in seeing long-term consequences of their actions. So, that means in socio-psychological terms that you need to have reminders regularly in order to warn people: "This may cause harm in one way or the other," but that is part as well. But maybe the more feasible way than really changing one's level of self-control, because, again, I think that would be very hard to change that other than by aging.

Stefano Caneppele: OK, thank you.

Marcelo Aebi: Yes, this is a general comment, as probably all of you know, we are publishing on the new edition of the European Sourcebook of Crime and Criminal Justice Statistics. At the end of this edition, we have a chapter on Victimisation Surveys and we are going to have it also in the new one, the one that will come out probably in January. So, I was wondering for the persons who were present… I mean, what we are trying to measure there is also the issue of cybercrime, and so we are asking, which is the question that you are formulating, so, this allows some comparisons across countries. And I was wondering if you would be fine for you if we send you the chapter six, which is already finished, but we learned new things today with you, so maybe you can take a look and give us your feedback and add some specific information on your countries. Would that be OK for you? This is an open access publication that is distributed that it will be available online, that is used mainly by researchers -as the name indicates, is a sourcebook, so it is the place where you go to get this information on how crime is measured in different countries. So, it would be really useful not only for the scientific community, but also for policy-makers that may want to take a look at this issue. And it is a way of putting all of this information together.

Stefano Caneppele: In the chat, they said OK to me.

Marcelo Aebi: You will receive a message from me and from Lorena Molnar, who is following also the conference - probably Monday at the latest, because we want to act immediately. Thank you very much.

Stefano Caneppele: Thank you, Marcelo. I had a question for Marianne, but Marianne she had to leave in advance. So, I think that we are finished, if there is nobody else wants you to make some comments.

Marcelo Aebi: Yes, maybe I have one final thing, especially for Billy, because you were getting these very high response rates because you were going door to door. And I do not know, I was wondering, do you send them, for example, a letter first to announce that the house has been selected for the survey, and then: do you think it will mean you will go back after the pandemic? Because my impression seeing what happened in other countries is that is the way in you conduct this survey. For example, the Catalan survey, and now it is by telephone and their response rate, even if they usually they do not publish really very long longitudinal series because it also exists in the 1980s. But the response rate varies a lot and has changed a lot with the telephone calls. So, my question is to Billy: do you think this is the key issue?

Billy Gazard: I think it is a good question. So, yes. It is a randomly selected household survey using a postal address. So, a letter will go out to potential participants, letting them know about the survey and that someone will be knocking on their door soon to ask them about the survey said that that is kind of how we recruit the sample. Will we go back to face-to-face? I think when the pandemic was first happening, I think our first thought was that this will be a break in the series: we set up a telephone interview and then the idea would be that we would then go back to face-to-face. However, the longer the pandemic is going on and, you know, 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 there is an increased possibility of moving permanently to a different mode. And the definitive answer to that is still, 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 that impacts on our response rates. I think if we were to move to a different survey mode permanently, whether that was via telephone or online, we would really need to think about how we managed to keep those response rates up. So, if it is you know, if we did go on with those modes, do we still continue to knock on people's doors to get them to try and get them to participate, even if it is over the phone or online by kind of going up and going to remind them to do it?

Marcelo Aebi: Yes, and who is the interviewers are part of your institution or this is an external company that goes door by door?

Billy Gazard: Yes. So, the with the crime survey, we work with a partner agency every five years. We tend to out the survey for companies to compete to do it. We have been with Counter Public for the majority of that time. So, they are our current partners, so they have interviewers on our behalf, recruit for the survey.

Marcelo Aebi: Thank you very much. And now for the telephone, did you change company or is the same company that provides? Because the qualities of the individuals are quite different from one kind of interview to the other.

Billy Gazard: No, we are still working with the same contractor. And also, so we thought about this issue, about the quality of the interviewers and actually the face-to-face interviews you know, the crime is separate from that telephone unit that does telephone interviews. We actually transferred a lot of face-to-face interviewers to doing to go to the telephone unit, to do the telephone interviews. So, in most cases, we have kept the same pool of interviewers to conduct the interviews.

Marcelo Aebi: Thank you very much.

Stefano Caneppele: OK, thank you, Marcelo, thank you, Billy. So, if nobody else wants to take the floor, I think we have completed the session about the *Modernising Crime Victimisation Survey*. And in the afternoon, we will discuss about the issue if we put in place, some might say, some initiative to think about how to deflect and to deter cyber offenders. And then Marcelo will arrange and will chair the session in the afternoon, and we will start at 1h Central European time. So, in one hour we will be back. So, thank you, everybody. Thank you for all speakers. Thanks to Ilina and to the Council of Europe staff for supporting the conference and providing the cyberspace floor for this meeting. And let us see you back in one hour of for the last session of this conference. Thank you very much.

Session 3 - Rethinking victims assistance & deterrence models

The Internet Organised Crime Threat Assessment

Nicole Samantha van der Meulen

Europol[11]

Excellent. Thank you very much. All right. 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 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. So, 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, 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? So, for the last six years, we have send out surveys to the member states and third-party countries asking them about developments over the last 12 months in different areas of cybercrime. So, 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

[11] Additional material: the author's visual presentation is available here: https://rm.coe.int/presentation-nicole-samantha-van-der-meulen-europol/1680a033b3

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. It is accessible on our website, 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.

So, 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 of 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, 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. So, 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 that 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, is that – which I am sure you have spoken about – and there is also the title of this conference: *how criminals took advantage of Covid-19?* I think it was very important to mention there is that Covid-19 did not necessarily introduce new forms of cybercrime. Rather, it exacerbated existing problems in the way that there were many forms of cybercrime 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. So, they may not have been as well prepared for 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 that, 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. So many of the threats that you will hear about today or that you will read about in the IOCTA also featured in this from 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. So, 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. So, there are those at the top-end that 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 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 like phishing, business email compromise (BEC), CEO fraud, but it can also be a prepatory 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 registered 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 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 in the future.

The cyber-dependent crime indicated 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, i.e. victims that are more likely to pay and 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, 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 what 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, which 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, 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.

The person who went before me, already spoke about it, really an area of concern, especially when it comes to developments with regard to Covid-19, obviously we receive a lot of referrals about materials of child sexual material, including self-generated material, of course, and there is really more referrals than law enforcement can cope with. But we see from the offender communities, obviously, they are cooperating a lot to make sure they stay under the radar or out of reach of law enforcement. And another large concern was that the live-streaming 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 live-streaming 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 live-streaming in Europe.

In the area of non-cash means of payment fraud, there were a lot of things continuing, but a lot of new things were introduced in the document that we received a lot of reports on. The steep rise in the area of what we call SIM swapping is an example. So, the criminals basically approaching the telecommunication providers in order to get a new SIM card in the name of the victim 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 here, 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 – 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's really an area where prevention and awareness has 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, diamonds, so they there is advertisements of investment opportunities and subsequently, obviously people give their money and lose everything. Card fraud is something that continues to increase also because there is 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 onto its own.

Those are the key findings in the different areas. This is a bit more detailed and in depth. 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 the 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 criminal and one from a native speaker. So, even for less "popular languages." And I have covered ransomware now. Also worth noting is 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, perhaps. 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.

So, in the area of recommendations, we have put them into a number of categories that we usually focus on that was also emphasised: cooperation is key. And that is especially 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. But 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 that there is trust and acceptance. So, not naming and shaming, especially if, for example, an organisation has fallen victim to cybercrime, it is important they feel comfortable sharing that because that facilitates learning and it also helps other organisations be better prepared for a subsequent attack. Prevention and awareness, it was mentioned by my colleague who spoke before me on the Portuguese side, really important. We try to do what we can. We have a number of campaigns. I have not listed them here, but of course, happy to follow up with anyone who might want more information. It is also readily 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 thirty-six 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 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.

Marcelo Aebi: First of all, thank you very much. If you cannot stay, maybe if someone has a question, this will be the right moment to ask it.

Stefano Caneppele: I have a question regarding the coordination with all the European partners. My question is, have you already discussed regarding the standardisation of reporting system in terms of cybercrime typology? Because I am aware that this is not the main goal of Europol to focus on statistics. But the problem is, as you said, that if we do not have the idea 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 European Union?

Nicole Samantha van der Meulen: So, when you say across the European Union, do you mean in terms of like across the member states then? Yes, as far as I know, there has been an attempt in terms of trying to put it on the agenda, I am not aware of anyone trying to sort of move further along because of the feedback, what people said during the interviews for the IOCTA. I am thinking of 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 straight to say how can we standardise it? So, I actually want to maybe, but this is very preliminary, sort of look into a couple of countries to see how they are doing it. And to see what are different models before sort of moving on. Like this will be quite a long process and I think I might follow up with some countries who have specifically mentioned that they are looking into it themselves, because then you can sort of I do not want to say piggyback, but go along with their developments. But as far as I know, no serious progress has been made in this area, and I think it is because it is a bit of a, well, it is a very challenging issue, and I think the way to approach it is maybe not to expect too much in the beginning, but to see how you can at least get some insight into how these systems work in the different countries.

Stefano Caneppele: Thanks.

Marcelo Aebi: Thank you very much. Are there any other questions? OK, it seems that that is not the case, so well, thank you very much for the call.

Deterrence, Diversion and Desistance of Cybercriminals

Michael Levi

University of Cardiff, United Kingdom[12]

Marcelo Aebi: And so we arrived last presentation before the wrap-up session, and this is by Michael Levi from the University of Cardiff that you know perfectly well already. Does not need a formal presentation.

Michael Levi: ***Marcelo Aebi***: And so we arrived last presentation before the wrap-up session, and this is by Michael Levi from the University of Cardiff that you know perfectly well already. Does not need a formal presentation.

Michael Levi: Well, thank you. So, first, I am going to take you through a number of different areas in the understanding that normally in this committee we deal with. Criminal justice processes, but I am going to go a little bit beyond that. So, first point I am going to make is that very often what happens when we look at online crime is that they are not just my government, but other governments really are trying to do counterterrorism control models. And my aim here is to re-examine public policing and public private partnership.

To see if the world satisfices may be strange, the term to satisfice by balancing different interests: cybercrime reduction and harm 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 crimes. 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

[12] Additional material: the author's visual presentation is available here: https://rm.coe.int/presentation-michael-levi-truly-final-coe-cyber-evidence-beyond-cjs/1680a033b2

important here and trying to bring people along onside is part of what a modern government needs to do. And to summarise, key features of deterrence, diversion, assistance 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, 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, unprosecuted offending because of attrition rate. *Alexander Seger*, for example, said what a tiny percentage of cybercrime ever get dealt with in the justice system, plus a particular problem of the cross-border dimensions. In other words, you know, if the offenders are in China or in Russia or in Romania, taking two out of three are member states of the Council of Europe, what is the realistic chance of getting being brought to justice, either extradited or prosecuted in their home state? And this is a controversial area.

In my opinion, we need to take account of civil and administrative sanctions if we are going to think about what happens to offenders, because we cannot just rely on criminal convictions sentences. We need to look at other methods of "dealing with crime". And I am not going to expand on this very much, the counterterrorist model my government has been working on and which it 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, 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 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 *Cybercrime EU Eurobarometer* data gives us some data on people who experience 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 preventative activity going on, a lot of it is developed 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 in which services are better or worse in prevention services 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 are: 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. We take this seriously. It means 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 and advertise to try and get people to stop 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, and 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 impacts of deterrence. When you see companies, you know, 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, I have added this really the risk 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. Very low prosecution rates for all online offences. 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, is an important area to sanction. And online hate and other cyber offences and national security threats, they tend to get most of the attention of most cyber security units. This is the report of a survey that the English Sentencing Council did when they asked people what they thought were the most aggravating features of online crimes. The Sentencing Council has yet to finalise any recommended sentences for this, but these are important things 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 mentor, on different ways of dealing with offences, but in cybercrimes we do not because little is known about the offender profiles of cyber-offenders. But what we know is that different from other forms of delinquency, people can often do very big crimes when they are very young, which is rare, but we do not know whether they mature out. Europol and Interpol say and there are some examples of this, that people turn to making money from 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, not in Europe, of course. So, they are mentoring presents, different challenges from mentoring for other offenders, and we do not know whether getting them to work with past cyber offenders we believe have gone straight is really a good thing or not. I will come to that as we talk.

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 they 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 the behaviour rather than the person. That is a lot of research about the legitimacy of interventions. And those are what we understand not just for cybercrime, but 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 you some UK examples, which you can read over at your leisure. In one, people were arrested, received a visit from a police officer. 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, Europol, etc., have been learning from these experiences. There was a database for the *Lizard Stresser Booter Service*, and people got a home visit from the National Crime Agency. If they were not believed to have actually carried out an attack and were told the stuff is in red, it is illegal, they can prevent individuals from accessing vital online services. And they were told that committing cybercrime can result in severe restrictions. So, these are the kinds of messages that were put out by the National Crime Agency who believe that this is quite effective. And the truth is 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. 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. But we know that the likelihood of detection matters to a lot of cyber criminals. So, warnings highlight that low-level offenders are not so anonymous as they think online. And warning has to be given because personally administered warnings about behaviour seen to be legitimate might actually generate defiance and more delinquency. It could be counterproductive if we are not careful.

Positive interventions, diversion: evidence is weak for cybercrimes. We might try like to say, well, you could be rich like Banksy if you engage inlegal 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 cyber criminals have become consultants, but there are security clearance issues and security risks 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 doesn't 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 government, police and for judges, that is people who want to nudge to change our behaviour is 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 in the round, we got some models for action. Trouble is, 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 they 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 for I mean, it may be OK for big business, but it is unrealistic. And we need to, as Europol and member states try and do, we need to look at takedowns of websites, bot nets and 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.

Q&A Session 3

Marcelo Aebi: Thank you very much. OK, so we now have some time for questions and reflections on what we heard. These were three very different presentations covering different ways of looking at the phenomenon from the victim to the deterrence of the offender. So, we covered a lot of topics. Remember that Nicole is no longer there. So, we should concentrate the questions on Riccardo and Mike. OK, so I would start with a question for Ricardo about the profile of fewer of the people that ask for help. Do you have statistics on that or just the general idea of who is mainly required…is there is this trend about gender or I am also thinking about the ethnic minorities that you may have your differences are they overrepresented or underrepresented?

Riccardo Strella: Sorry, yes, we have some statistics from last year, so every week, every year, we try to deliver the annual statistics regarding the context to our helpline and hotline, mainly the content, the in terms of the age gap of people that contact us. And we the vast majority are grownups. So, young adults from 25 to 50 years old is the vast majority of people that contact since and mainly males in terms of what we were seeing since. I think it is an important topic or something to highlight is that we had since the pandemic, we had lots of reports regarding sextortion cases, but mainly regarding those sextortion emails. I do not know if you I think that you are all aware of those sextortion emails. Basically, that can come from data breaches and people ask us if the threat on the on those emails is real or not. And we have lots of calls regarding that and picking up on the, the cyber-resilience theme we are seeing in terms of awareness for, for example, cybersecurity measures that all of us should implement. What we saw is that we are seeing in Portugal that a lot of people, for example, simple things like changing their passwords are not implementing. So, those sextortions that come from those data breaches, the passwords that appear, even though that that people tell us that are passwords that are very old, people do not change them. And so, they lose access to, for example, their Gmail accounts and so on, because we see that those cyber-criminals try to gain access immediately to better known applications that that we use. And we see that in Portugal, there is a lot to do regarding our cybersecurity measures and that we could all take.

Marcelo Aebi: OK, thank you. Well, perhaps this majority of males reflects the fact that they are more often connected or is or do you think it is the campaigns that you are making that do not reach women? You think it is a real distribution or it reflects...?

Riccardo Strella: No, no, I do not think it reflects the reality and for example, we do we see that we have a lot of dark figures in between adolescents and infants that do not reach out to us. And so, we also have this year a campaign in schools because we know a lot of situations that happened regarding cyberbullying, non-consensual image sharing among adolescents. And they do not reach out to us because a lot of the victim blaming so specifically on these cases of non-consensual image sharing. There is still the idea that victims are to blame. And so, they feel very ashamed to come out and to and to ask for help. And most of the cases that we know or that we have directly talked with victims always come first for someone, for some peer that knows about the situation and reaches out to us, to them to ask for information, to help a friend. And then we can reach to the victim. But yes, there is a lot to do and also to change minds regarding this situation.

Stefano Caneppele: I have a question for Ricardo. My question is more on the European perspective. So, is there any European network of NGO dealing with victim assistance of cybercrime? And did you have the opportunity to share and to make some say and comparison in terms of what is the most recurrent profile of people that have access to your hotlines or your platforms? Or is it any safe place in which at European level you can compare experiences and exchange practices?

Riccardo Strella: Yes, I am. I cannot tell you now which are the things that the trends... But one thing I can tell you, the organisation that we are apart from Insaaf, and then I can share the link of the website, we as a network for three and three months have to send all the information regarding the contacts that that we received on the helpline and also on the helpline and the hotline. So, they are two different entities, but they then do they retrieve the data from all the European countries that are part of the Insaaf network and they usually have annual entry reports regarding the profile of the victims or the persons that contact. But because I have to say that our helplines do not deal only with the with cybercrime, we deal with other things, like I said, for example, online addiction and so on. But there you have compiled all the information. I am not a specialist. My speciality is not statistics. But one thing I can say is that when we send those numbers, let us say we all have to follow the same categories. So, in that sense, it is all uniform, let us say. And so you can have you can receive some that from the Insaaf reports.

Marcelo Aebi: OK, thank you very much. Thank you. So, let me check if there is a question on the chart, I do not think so. OK, so maybe now I will have a question for Mike. So, you had a very difficult task because the deterrence, diversion, this is the sort of cybercrime. I mean, if we had problems defining what is cybercrime, we also have a wide diversity of cyber criminals. So, I was thinking like, this is one of the profiles would be a hacker. And usually when you stop smoking, for example, when you are trying to lose weight, they tell you to put away, to not to have cigarettes at home, not to have a lot of food in your fridge. But for a hacker, let us say the actual world nowadays will live online constantly. And so, just thinking of this concretely, if it is funny for any bad habit, it is extremely difficult to quit when you are exposed to the risk. How do you see this?

Michael Levi: Yes, I mean that is a very good question. Yes, that maybe it is the only thing I can think of directly to this yet when we look at research on child abuse, for example, physical abuse, one of the differences between parents who beat their little children, for the under two is that they have distorted perceptions of the babies and what you can expect 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. Yes, mentally, they thought of their favourite Elvis Presley song, their favourite Freddie Mercury number, their favourite Bach cantata, and as a way of diverting themselves mentally from the stress that the baby was given, and this is one of the findings that some cognitive psychologists have looked at. So, learning to divert, you know, you can keep that packet of cigarettes, Marcelo, but just do not. Yes, as Nancy Reagan used to say about drugs: Just *say no* but divert yourself mentally by thinking of some positive thing, a holiday that you had, how innocent the baby is, it is not their fault. And so, there are those sorts of techniques of mental diversion 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, the *ubiquity*, I mean, some offenders as part of the sanction are told, you know, you are not allowed to have a computer at home. But, yes, you can maybe do that like Kevin Mitnick was. 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. Would be one kind of thing to do.

Marcelo Aebi: Yes, it is very interesting what you say, because there is research conducted at the University of Lausanne, among others, they use precisely that is a way of dealing, for example, with that say, to simplify types of post-traumatic stress. And they associate, for example, I remember they made a presentation for the alumni, the former students of the university, and he was playing the case of, he had seen his brother fall from a tree and he was severely injured. And since that day, every time he would see someone on a tree, especially his kids, it was a problem. And they worked on associating this with Spiderman, and so just mixing the idea. This is exactly what the psychologists are doing. But they are doing it in a way that neuroscientists can see which are the parts of the brain that are connected. And in the long run, then, of course, he's not that he's completely out of this as a souvenir, but when he sees something like that, the two images come, and it is less important. But it is very interesting because this is something that eventually will go the way I will remember.

Michael Levi: I think cognitive behavioural modification, mindfulness of different kinds. Of course, Spiderman was dealing with web crime, so it is very relevant to online. But yes, I think that needs to be more creativity in this process. And, you know, given, of course, we might have to have different models for different I mean, you know, in your example, they were dealing with it as a victim. But you also need to deal with your… Oscar Wilde once wrote, *I can resist anything except temptation* and say, yes, so we need to move away from that in dealing with offenders. Otherwise, it becomes like science fiction episodes. But we need a lot more creativity. But yes, this is such an important phenomenon for our times. And I am not being too depressed about the criminal justice system, but it is Yes, 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 in a way and approach the messaging from prosecutions and from sentencing in a much more creative and systematic way than we usually do.

Marcelo Aebi: My impression, I think that you said creativity because otherwise I think we have. People keep saying: "Yes, education, yes, we should prevent", but nothing concrete, and here at least I have seen something concrete in what you were saying and something that they say does not know where he stands. There is never a good wind. So, this could be one idea. And I think it is really creative. And of course, I my impression of these days of this, I should say maybe in the next session, but I could already mention it is so there are a lot of things that are being done. Maybe they are not well known. So, we keep saying we do not know it. But at the same time, for example, this is something that maybe Matti could answer because I was surprised when he said in the morning that they are going to use this cybercrime every four years. So, every four years is like the World Cup. I would prefer to have it only or five years. Yes, that would be worth. But my opinion, I mean, this is so important and it is so difficult to currently, to divide the digital world from the physical world, you know, apart from these people that say that maybe through that adolescents can no longer make the difference. But in fact, it is very difficult. I mean, being realistic and they are interrelated all the time, we are jumping from one world to the other. And so, it was not biggest surprise. That is only every four years is like…

Michael Levi: And it may be about money. Yes. It is the cost of doing the surveys.

Matti Näsi: Just respond to that. One of the issues is that we used to survey the national survey. So, ask the two basic items, basic models, which is the violence and the and the property crime. But the challenge is that the third one is a module that is usually different every four years, every year. So, one year we might have cybercrime. Next year we might have a model that focuses on domestic violence. So, it has been so far that we have 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 about money that we cannot really do a separate population-level crime survey because it has cost so much money. So, we have to adjust and try to do it and hope that we could do it at least every three years. But I think it might be that that would be ideal every two years. But we usually have a different theme or research project within the institute that might, might or could use that third alternative module and have a different theme in the survey. So, we have to balance it with that, with money we have in news and with the themes that we have been in research. So, that's the challenge why we cannot really do it every year.

Marcelo Aebi: Well, thank you. I see the point. But just as a general reflection, this also has consequences on what we know about crime. If you look at the debate on the crime drop, the real crime drop was in the United States. But of course, it seems that we follow what they do. And then, of course, in the UK and mainly in Anglo-Saxon countries, it was not so clear in other countries. But without mentioning that, the problem is that nobody was measuring cybercrime. So, I remember in the first article with Antonia Linde in 2010, we already mentioned that crime changed to cybercrime. But when you want to look at trends is very difficult. With the Stefano, we were very lucky to find data on the losses of credit cards. And then you can see since 1992, also accepted at a time when crime, traditional crime started decreasing. You see that there is an increase. We are not seeing that this is the explanation. Of course, *the security hypothesis* remains realistic, but there has been a change in the lifestyles. And these are very difficult to show it. And of course, in the debate, many people took positions, very strong positions. But, you know, four years is a lot of time and I see the problem. But my impression is that it is not so easy currently to separate property crimes from property crimes that take place on the web. You know, so you may see a decrease of pickpocketing or a robbery, but it does not mean that property crime is going down because it may be taking place somewhere else. So, but I see what you say, but it shows that we are always delayed we then the researchers and the institutions that do research because we have still not, we can still change our mind. Our mindset should be nowadays things happen like today. I mean, I have been in front of the computer since 9AM, but I went back to the world for one hour to have lunch and then come back. And it seems that we did not realise that. And so, someone must say: "one moment, probably OK, we must include some questions on cybercrime in the module, on a property and in the model of violence, because these are new forms of violence"; at least is why I how I see it. And I know that you cannot do it alone. But perhaps one of the things we could do with this one with the proceedings of this conference is if we want to have some impact on policy-makers, which is one of the goals of the Council of Europe with all these projects, maybe it is something that we still need to work on to change the mindset of the persons.

Matti Näsi: I agree with that. And it is. It is a problem that we would collect in such a sort of extended period of time, except every four years, it does not really give up because it is a rapidly changing type of crime. It is also so if you want to be on top of it in some forms, then you really do need to have an active following on it. And I think we might think about options in terms of whether we could have some type of yearly annual items and annual sort of questions that we could use in terms of having a tracking cybercrime and then have every four years. We have an extensive model with background factors and so on, that could give us, you know, if you want to do more advanced statistical analysis, that you have those tools available in every four years or so on. But I think this is a collaboration in any form would be it would be highly, highly encouraged. But what was interesting to note is that if you were not at Eurocrim in Ghent, a couple of years ago, unfortunately, we could not do that in person this year. But there you could see already in the sessions that the cybercrime is getting more and more attention. And I think that was that really a year with you when you saw a lot more cybercrime-related papers and lots more cybercrime-related research. Some of them are very specific topics, very specific type of crime. But I can certainly see the change in terms of how researchers approach crime. And it is not used to be much more focused on traditional forms of crime. But I can see the change now.

Marcelo Aebi: Yes, yes. I totally agree with you, we have seen this change. The interesting thing for the debate is that one of the key arguments in the drop of crime debate was people are more sensitive to violence. So, they go in more often to the police in case of a minor thing and this increases non-lethal violence. But indeed, what we have seen in all these presentations is that people seldom go to the police when they are victims of offences committed on the Web. So, this part of the debate, the fact that, yes, we know very little about the frauds and we see the increasing difference, but we know that it is a minority. These changes completely the way in which the world is really working. And I think that our perception in the academic world specifically, it is a little bit far away. We are now working with Stefano on an article with inside this debate and, was very interesting to hear the presentations today because you gave me and, I also suppose there are different new ideas to finish that paper because I have the impression that we are debating out of nothing at all, forgetting what the real debate is, it is kind of an analogic debate, it is like watching crime in black and white, let us say, or in a classic TV without 3-D. But this will see we will see what we can do about that, about that in the future. Thank you very much.

Stefano Caneppele: I have a question for Michael, actually, because it comes out from what you presented today that there is a rhetorical saying that cybercrime is a priority, both in terms of resources. There is a feeling that the public has been delegated to the private sector, are part of the policing of the worldwide web of cyberspace, because there is a sort of untold story that probably countries are not able to dealing with this kind of issue because it is something on transnational and the best thing to do is just to announce a public private partnership. What is your opinion about it?

Michael Levi: I think that is 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 the money on extra public resources for cybercrime or fraud, whether online or offline or mixed, and come back to Marcelo's point earlier, we have to really remember that a lot of it is mixed. And 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 we 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, they do delegate quite a lot, as they do with credit cards, etc., and that bit of the system works quite well. It is where the harms are not just against it, is where 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 the private sector should be dealing with it. It is 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.

Matti Näsi: A couple of comments in terms of first 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 and less were actually afraid of physical violence. So, we see what you see as the in there in terms of how crime and the perception of crime are changing. But the other point is that I want to sort of perhaps bring to the table and it is a huge thing. But I was in that event with the cybercrime event in Finland and there was a prosecutor from one of the courts in Finland and saying that the problem with the prosecution process is that the judges do not have the knowledge of cyber-related issues, that sometimes the sessions can be very, very slow. When do you have to explain to the judge what is IP address, for instance? We start from the very, very basics of the process in the court system is slow because there are not skill levels, that people are skilled that can then 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 in that in the online spaces and whether they have the expertise to help them to come to the police? If we think about police training, we think about traditional crime. Yes, so you have the different ways of use of force, etc. 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 that can actually implement and sort of operate within the context of online or whether it is hybrid offending or complete online? So, at this moment, we rely a lot on the private sector in terms of providing us tools to secure our business. And what but that is private sector investment, private sector knowledge. What about the public context?

Marcelo Aebi: You know, we invited the private sector also to participate in the 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. What you said about the levels of fear of crime is really impressive and people are more worried about cybercrime, but nobody is discussing about this. You know, in some cases I understand it for a credit card company, it is not good publicity. If you say every day around the world, one million credit cards are stolen. I mean, if the newspaper said tomorrow, this is a huge issue, so nobody's paying attention. But you see this disconnection, as I was saying, between the reality and the way in which politicians are looking at data on criminal policy-makers. Maybe, as you said, there is not only that the judges, the lawyers, but maybe everyone, because traditionally in the Old World, the wise men and the wise men, the *counsel of the wise* in other languages like Spanish, were *wise*. That does have the same meaning is *the counsel of the old*. And so, the idea was that you become older and you become wiser and then you know more. But nowadays the world has changed and, of course, you always have many things, but you do not have the ability to work with that technique. And this is changing the relation, even the relationships inside the families are changing because that is the key advice to help the parents. So, that is a major change in the way our society works. And maybe is that worse than we are really realising? Yes, and I think you said that Fernando wanted to say something, that.

Stefano Caneppele: Yes, Fernando was commenting about the fact that we were not considering that long, one of one part of cybercrime is about social networking. There is interest for another one to jump in, kind of a different one.

Fernando Miró-Llinares: Only related to what Marcelo was saying and with Mike and 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 is one of the keys on cybercrime because there are an important percentage of cyber hacking, so social networks, they have a lot of information. I was saying that for some crimes are the ones who decide, so are the ones who have the information. They have the information of how many tweets of hate and the evolution of the amount of this information that happened during Covid-19 that we do not have the information. They have all that information there. They have the information of the evolution and in some kinds of fraud, they also have the information of that kind of spam that happened in social networks.

So, I believe that for once, in one thing related to, what Mike was saying about deterrence and change in psychology, I think we have to focus also on social networks related to measurement of cybercrime. We have to focus on social networks and relate to change the perspective of whom is that relationship between government and individual. I think now the government is not the problem. The new government of cyberspace are social networks, and we have to put them and we are not thinking too much on them. I see a lot of studies about politics, about sociology, but not a lot of criminology attending to the power of social networks, attending of all of those topics. I do not know if it is totally related with where you would say, but I think it is important.

Marcelo Aebi: Yes. I mean, we had I think we need to change our framework the way in which we see the world. And now, of course, we are not going to find the solution this afternoon. But I mean, I am going out of this discussion more worried than I was before because I have seen all these connections. If they are hearing Mike ring a bell, then Matty says something while it rings another bell. And there is like a line that goes over these different topics, and the line is we are starting the word as if it was flat and now is round, you know, maybe I mean, it worries me a little bit for us, not only our society, but also us as a community of scientists. So, Yes, but it is not so easy to change this because when you come with them mean I have seen your exchanges also, Fernando, about this issue of the crime drop. It is very difficult to say clearly the things you have to say when you are going through a process of peer review in and the process of peer review and is controlled by the ones who are having another position. So,there were still a little bit more to say about that until.

Riccardo Strella: 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, it regards the for example, *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 we find that a victim, for example, perceives as offensive, and that would constitute hate speech under our legal framework, we also have to deal with those on platforms, definitions of hate speech that are not the same. And then they have the power to remove it, and if it complies with their own community standards, they will remove it. If not, we even can say that "but according to Portuguese law, it is a crime to say that", they would not comply with that. And we have to play by their own rules if we want the maintain our main goal that is to help the person that reaches out to us and to have the content removed.

Wrap-up session

Marcelo Aebi: I would like to start by saying that I really enjoyed the discussions, the presentations too, but the discussions were really interesting, it is not always the case, maybe because when we go to a conference, the time for discussion is very short. We made an effort here when organising the conference to leave some time, some extra time at the end. I do not know if we were completely sure about that. But in any case, we have the time to discuss, to say openly whether we want it. And I am happy about the fact that the everyone that participated in them. Nobody came with the ideological preconceptions and we could talk openly and this is really not so easy that it happens, and so it is like the intellectual having been happy intellectually and, you know, it is what this philosopher from Catalonia said "el gozo intelectual", "le plaisir intellectuel", "the intellectual pleasure" – the feeling that you have a nice discussion that we went through different things. And so, I am really happy about all this.

What happened today? And I am still under the influence of these discussions and then about the future. So, I think that a lot of things that were said today were extremely interesting and the Council of Europe has used to have a tradition for many years of organising criminological conferences. It was the main place of the meeting place for criminology from Eastern and Western Europe for many decades, I would say. And somehow, without even realising this, we have to say thanks to Ilina because she mentioned these conferences. Maybe somehow, we are relaunching a long tradition. And finally, the fact that we are obliged to make them online allowed some more people to participate. Perhaps in the future, the model would be a hybrid model like cybercrime, as we said that cybercrime is working now. Of course, the good thing is that now we would close the session and then go out together and sit around the table and drink a beer and discuss quietly. And of course, this cannot be done, but some people that could not attend perhaps could do it in the future online so, because this finally we have like 30 people participating in the conference. We would like to do that, to bring this to them to a larger public. And we are fully aware that it is impossible to ask people to write another article with all the time that we have the discounted. But as we recorded the audio, what we are proposing is that we will do a transcription at the University of Lausanne with Stefano and Lorena Molnar, who will join us for this project. And then we will send you what we have. And of course, you can do whatever you like to adapt it. But at least there is something and this is it is the proceedings of the conference. So, we do not have to apply the rigid standards of peer review article. Of course, the fact that we are discussing, also introduce a kind of peer review in that because the discussions will surely help the final papers, but we will send it to you. And of course, you can decide whatever you want. And I think it is important to send this message.

And we will now have to find a way of summarising also the discussions that we have, because I think it was really it was very interesting. And so, of course, this would be something that will be available and in open access and a way of reaching the wider community and bringing out one kind of reflection about the current situation. So,that would be my message. I do not know, Stefano, if you want to add something. We have two minutes now,

Stefano Caneppele: I think you said everything we needed to say. So,I want to just thanks again to all the participants and all the speakers. I think we got very good insight and inputs about the issue. I also would like to thank again in all the staff of the Council of Europe that were able to set up this conference despite this difficult time. Thanks to the interpreters and the technician also on behalf of everybody.

Marcelo Aebi: Yes. So, OK, thank you very much for attending, as I mentioned, I really enjoyed this conference. And I hope to see you again soon. We will be in touch and take care. And let us hope to meet also to be all together in Strasbourg soon. Again, thank you very much for attending this conference.