UNIVERSITEIT TWENTE.

CRIME VICTIMISATION SURVEYS MEASURING CYBERCRIME

MARIANNE JUNGER (University of Twente M.JUNGER@UTWENTE.NL)

PIETER HARTEL (University of Twente, Delft, University of Technology, Singapore University of Technology and Design)

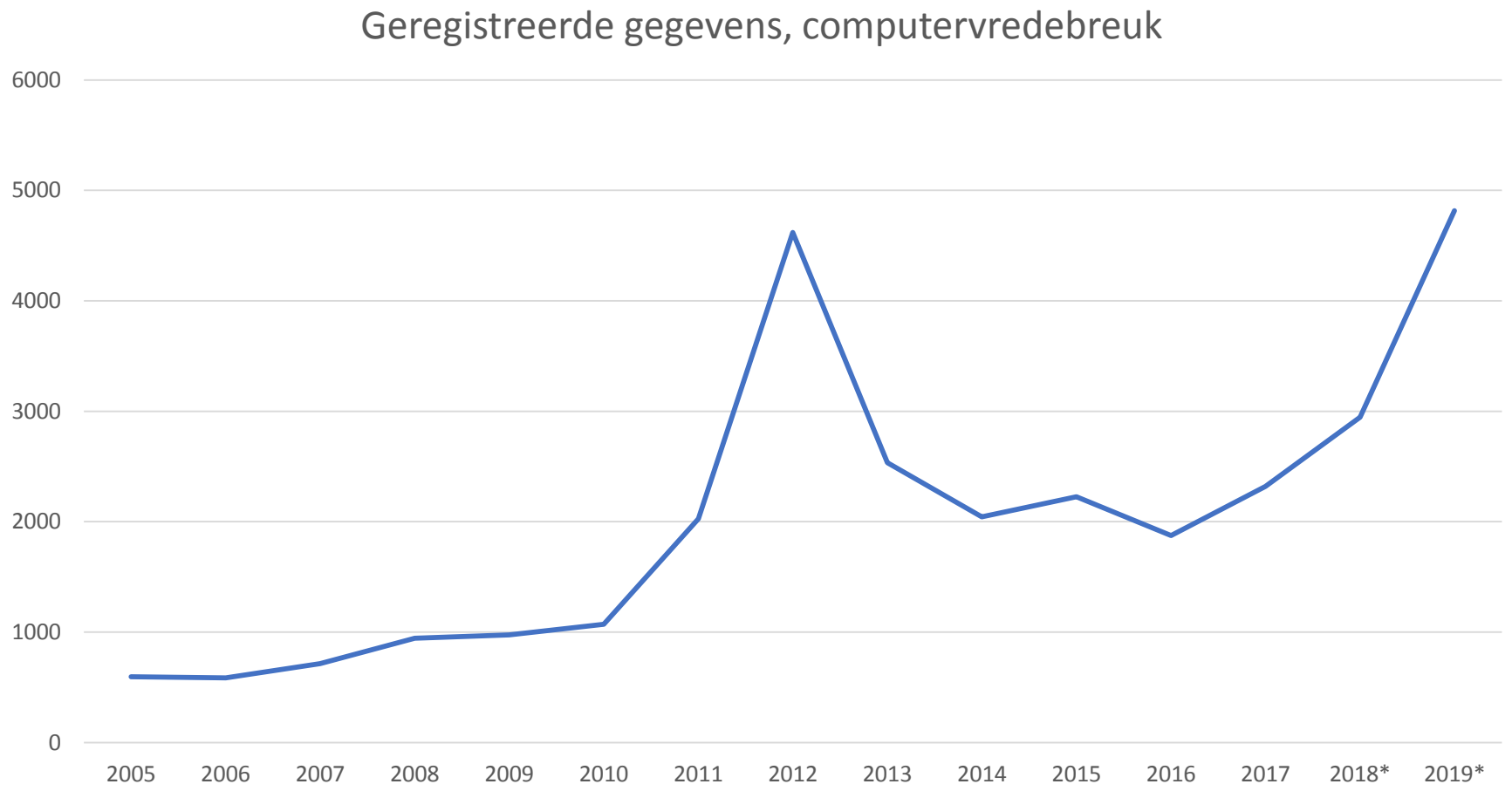
Conference: Measuring cybercrime in the time of covid-19: the role of crime and criminal justice statistics"

organised by the European Union and the Council of Europe, Strasbourg (online meeting)

Vous avez une question?

Je parle français – au cas où préférer poser votre question dans cette langue

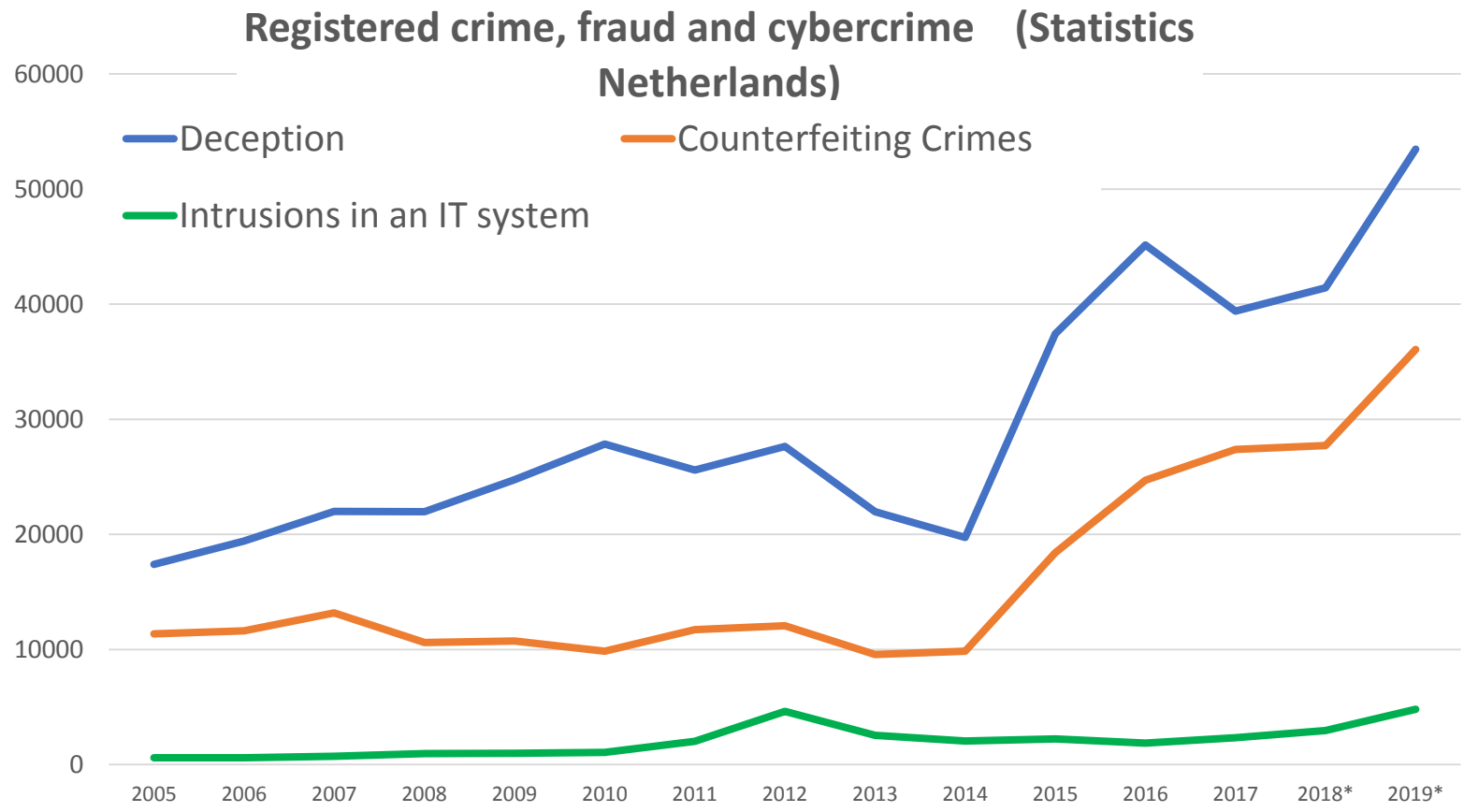
Increase in ‘computer intrusions’



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

Is cybercrime hidden in other crime categories

e.g., in 2012 ICT-related: threats: 16%, fraud 40%*?

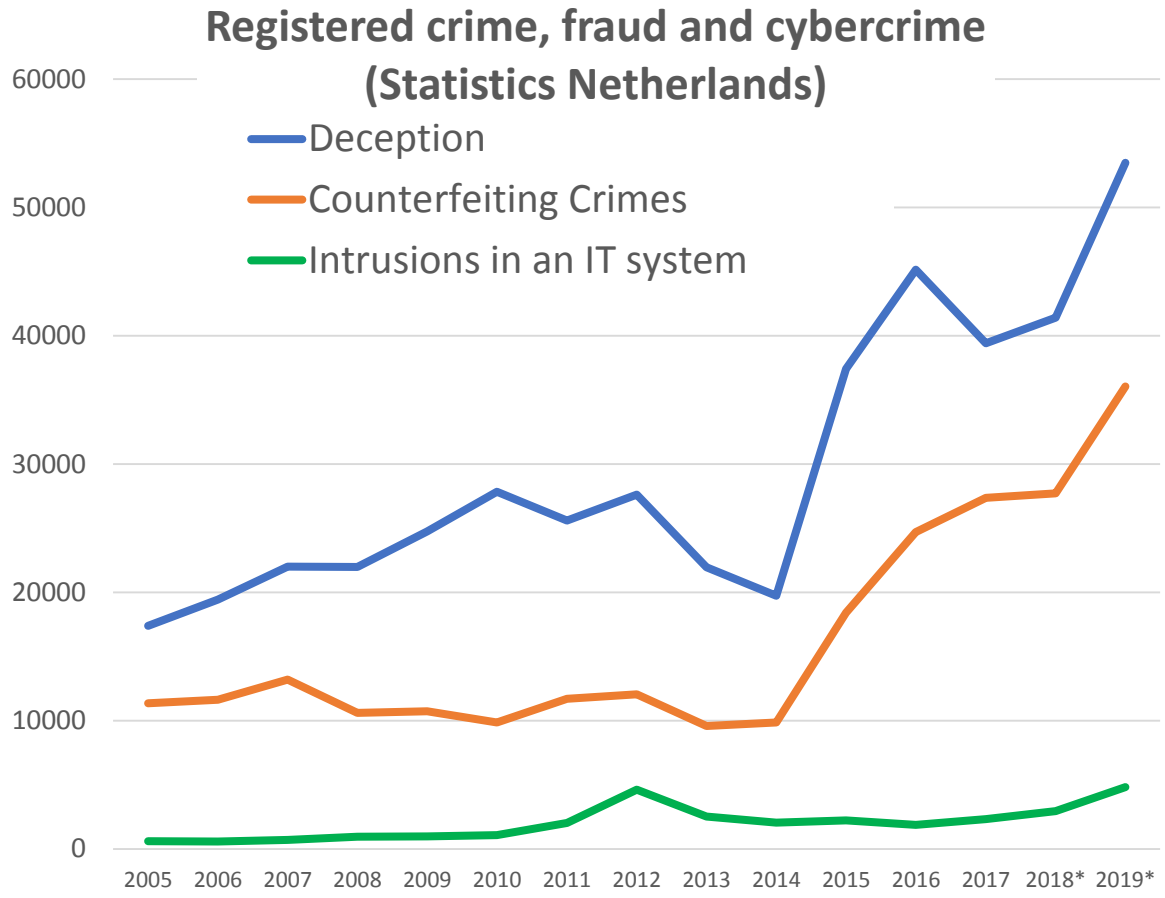


* Montoya, L., Junger, M., & Hartel, P. (2013). How 'Digital' is Traditional Crime? European Intelligence and Security Informatics Conference (EISIC) 2013, 31-37. Retrieved from https://ieeexplore.ieee.org/abstract/document/6657122

Is cybercrime hidden in other crime categories
e.g., in 2012 ICT-related: threats: 16%, fraud 40%*?

Steep increase in fraud**

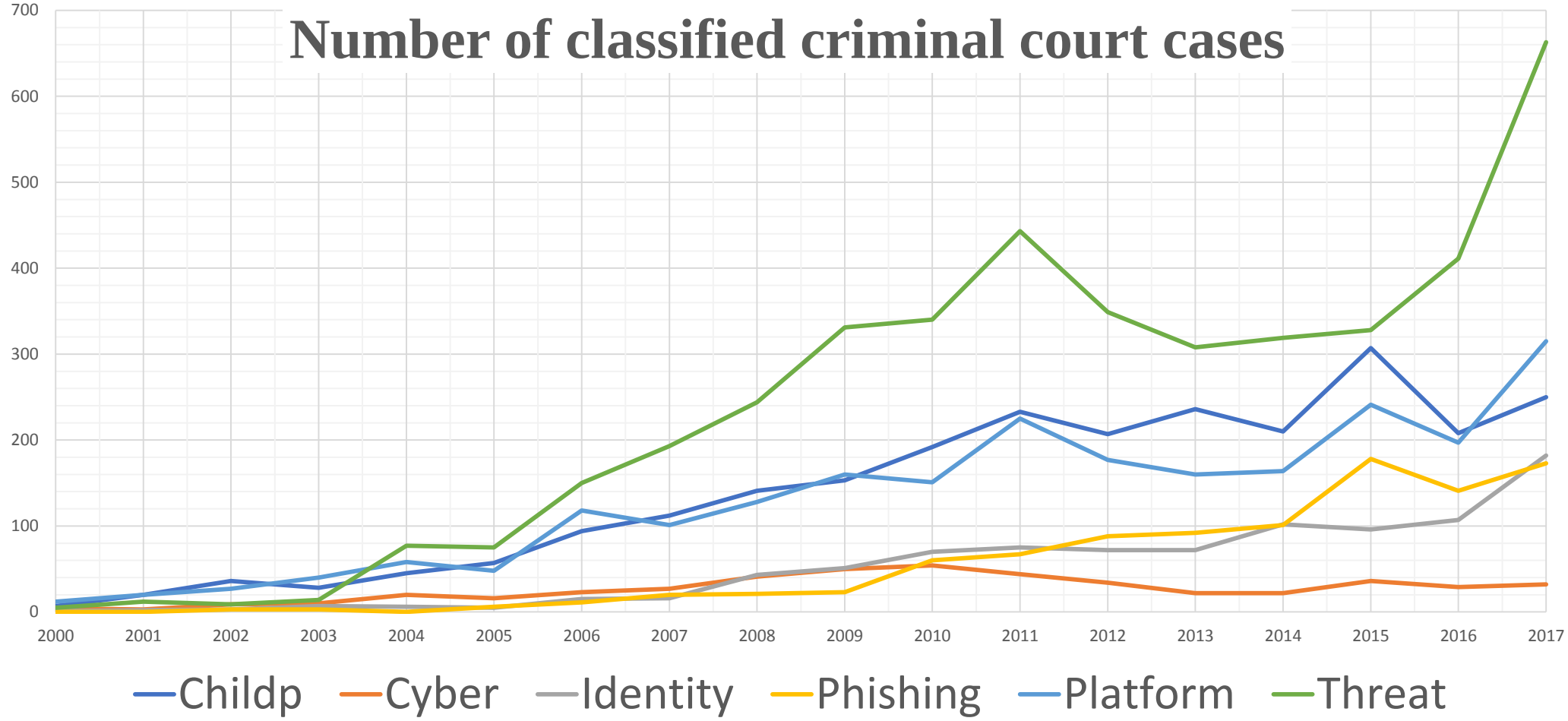
- US (Finklea, 2014; Javelin, 2017)
- UK (Financial Fraud Action, 2017)
- Spain {Kemp, 2020 #17721}
- Australia (ABS, 2015)



* Montoya, L., Junger, M., & Hartel, P. (2013). How 'Digital' is Traditional Crime? European Intelligence and Security Informatics Conference (EISIC) 2013, 31-37. Retrieved from https://ieeexplore.ieee.org/abstract/document/6657122

** In: Junger, M., Wang, V., & Schlomer, M. (2020). Fraud against businesses both online and offline - Crime scripts, business characteristics, efforts, and benefits. *Crime Science, 9. doi:https://doi-org.ezproxy2.utwente.nl/10.1186/s40163-020-00119-4*

ICT aspects, hidden in court cases,
done via machine learning



- Sessink, D. (2018). Using Machine Learning to Detect ICT in Criminal Court Cases. (Bachelor), University of Twente, Enschede, Nl.
- See also 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.

Plan

1. Crime victimization surveys

2. Cybercrime: how to define and how to measure?

3. Measuring cybercrime through Crime Victimization Surveys (CVS): results pilot

CVS 'most appropriate mode of measurement'

National Academies of Sciences (2018, p. 43)

1. Independent of police statistics

2. Representative samples -> national % of victims & incidents

3. New classifications, e.g., 'stranger to stranger crime'

4. Instrumental for
   - Theory development, e.g., Routine Activity Theory (RAT)
   - Impact of victimisation
   - International comparisons

- 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.*
- Cantor, D., & Lynch, J. P. (2000). Self-report surveys as measures of crime and criminal victimization. *Criminal Justice and Behavior(4), 85-138.*
- *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). Chicago, Ill.: The University of Chicago Press.*

How to measure cybercrime (CC) in CVS?

Council of Europe, 23/11/2001 -> legal description

- as means
- as a target
- as content

- Council of Europe. (23/11/2001). Convention on cybercrime. (CETS No.185). Budapest Retrieved from http://www.coe.int/nl/web/conventions/full-list/-/conventions/treaty/185.
- Koops, B.-J. (2010). The internet and its opportunities for cybercrime. In M. Herzog-Evans (Ed.), Transnational criminology manual (Vol. 1, pp. 735-754). Nijmegen: Wolf Legal Publishers (WLP).
- Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Cambridge, UK: Polity press.

Cybercrime (CC) ‘as a vague concept’

Various specific cybercrimes also ‘broad and imprecise’*

Reasons, e.g.,

- Cyber crime is more complex – longer crime scripts
- CC is ‘invisible’

* UNODC Intergovernmental expert group on cybercrime. (2013). *Comprehensive study on cybercrime. Draft - February 2013. Retrieved from Vienna, Austria: Retrieved from: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf*

Phishing: crime script

Microsoft. (2020). *Microsoft Digital Defense Report, September 2020. Retrieved from* https://www.microsoft.com/en-us/download/details.aspx?id=101738 *p. 15*

Defining and operationalizing CC

Can victims know?

When money is gone from your bank account, what happened?

Council of Europe. (23/11/2001). Convention on cybercrime. (CETS No.185). Budapest Retrieved from http://www.coe.int/nl/web/conventions/full-list/-/conventions/treaty/185.
Koops, B.-J. (2010). The internet and its opportunities for cybercrime. In M. Herzog-Evans (Ed.), Transnational criminology manual (Vol. 1, pp. 735-754). Nijmegen: Wolf Legal Publishers (WLP).
Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Cambridge, UK: Polity press.

Comparison of population CVS

1. Six crimes were comparable over 9 European CVS's
    1. Online shopping fraud
    2. Online banking/payment fraud (with or without loss)
    3. Other fraud
    4. Cyberthreats/harassment
    5. Malware
    6. Unauthorised access to personal information (including hacking, excluding offences that led to banking/payment fraud)

Reep-van den Bergh and Junger *Crime Sci (2018) 7:5*
https://doi.org/10.1186/s40163-018-0079-3

Crime Science

RESEARCH Open Access

Victims of cybercrime in Europe: a review of victim surveys

Carin M. M. Reep-van den Bergh[1] and Marianne Junger[2*]

Abstract

Objectives: Review the evidence provided by victim surveys in order to provide a rough estimate of the personal crime prevalence of the main types of cybercrime.

Methods: We performed a search in databases, searched online, and contacted several Offices for National Statistics in Europe and selected surveys that provided information about individual victims of crime which were representative for a general population. Six types of cybercrime have been distinguished, namely online shopping fraud, online fraud banking/payment, other cyber fraud (such as advanced fee fraud), cyber threats/harassment, malware, and hacking. For every survey the questions on cybercrime are presented and the crime prevalence estimates are compared.

Results: Nine surveys were included. Annual crime prevalence rates ranged from 1 to 3% for online shopping fraud, from less than 1 to 2% for online banking/payment fraud. Less than 1% of the population is a victim of other types of fraud and a maximum of 3% of the population experiences some sort of online bullying such as stalking (1%) or threatening (1%). 1–6% is a victim of hacking. The estimates for being a victim of malware range from 2 to 15%. For all offences it cannot be estimated how much of the differences are due to variation in methods and questioning

Focus now: Pilot study at University of Twente

CVS Statistics Netherlands

1. Cyber bullying/ threats
2. Online shopping fraud
3. Hacking
4. Identity theft

Pilot study

1. Convenience sample of 225 respondents

2. Aim: check questions of Statistics Netherlands on content

   - Do the answers match with the questions
   - *‘Describe what happened, please? ‘*

Results

1. Okay for ‘cyberbullying & threats’ and ‘online shopping fraud’

2. Not so good for ‘hacking’ & ‘identity theft’

Two specific concepts are analysed

1. **Identity theft**: *Here, someone's personal data is used without permission for financial gain, e.g. to withdraw or transfer money, to take out loans or to request official documents. Perpetrators may have obtained personal data in various ways, for example by intercepting the mail, copying bank card data at an ATM or via the internet.*

1. Hacking: *In the past 12 MONTHS, has it ever happened that someone has maliciously broken into or logged into a computer, email account, website or profile site (eg Facebook, Twitter) belonging to yourself or someone else in your household?*

Results: 'ID-fraud' is mainly 'phishing'

	ID-fraud
Phishing	**6**
ID-fraud	**3**
Skimming	**3**
Cyber-bullying	**1**
Malware	
Hacking	
Threat/cyber-bullying	
Unknown	**1**
Total	14

Coded as phishing by MJ & PH

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

Problem: This e-mail, is this: a) "real email from google" or b) a "fake mail from google"?

(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.'

Results: ‘hacking’ is **mainly** ‘phishing’

	Hacking
Phishing	**9**
ID-fraud	
Skimming	
Cyber-bullying	
Malware	**2**
Hacking	**1**
Threat/cyber-bullying	**1**
Unknown	**1**
Total	14

Coded as phishing by MJ & PH

(1) ‘Partner received emails from his own account with advertising ads.’

Problem: it probably only looks like it comes from your own account.

(2) *‘I got a pop-up asking for my credit card information because I had earned extra flight points and she wanted to add them.’*

Results: phishing is most important issue

	ID-fraud	Hacking	Total	Proportion
Phishing	**6**	**9**	15	0.5
ID-fraud	**3**		3	0.1
Skimming	**3**		3	0.1
Cyber-bullying	**1**		1	0.04
Malware		**2**	2	0.1
Hacking		**1**	1	0.04
Threat/cyber-bullying		**1**	1	0.04
Unknown	**1**	**1**	2	0.1
Total	14	14	28	1

Conclusion: It's hard to measure cybercrime through CVS

1. Half of incidents are **phishing** (for ID-fraud & hacking)

2. Next: **ID-fraud** & **malware** (no more skimming in NL)

3. ISSUE: no one (almost) asks for phishing

Conclusion: It’s hard to measure cybercrimes

1. ‘Offender bias’?
    - Questions ask about what offender meant to do, rather than what victim experienced
2. Link to COE Budapest Convention
    - do victims need to know the convention before answering questions?

Conclusion: problems

1. Conceive offline versus online as a dimension

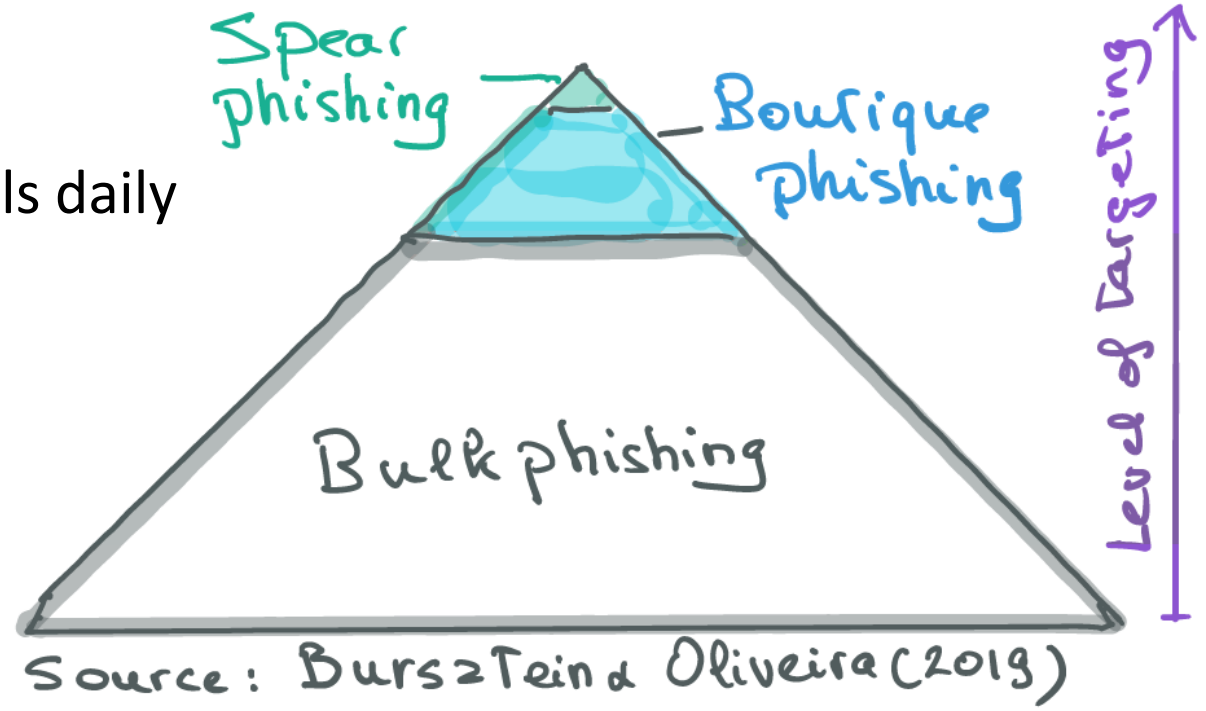
2.Pay attention to modus operandi more generally

3.Is this a cohort/age problem?

- Jardine, E. (2015). A Continuum of Internet-Based Crime: How the Effectiveness of Cybersecurity Policies Varies across Cybercrime Types. *Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, Northampton, MA, Forthcoming.*
- Montoya, L., Junger, M., & Hartel, P. (2013). How 'Digital' is Traditional Crime? *European Intelligence and Security Informatics Conference (EISIC) 2013, 31-37. Retrieved from https://ieeexplore.ieee.org/abstract/document/6657122*
- Tcherni-Buzzeo, M., Davis, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? Justice Quarterly, 33(5), 890-911. doi:10.1080/07418825.2014.994658

Alternative measures: e.g., phishing

- Microsoft block about 13 billion malicious emails
- Google blocks about
- 100 million phishing emails daily



Microsoft. (2020). *Microsoft Digital Defense Report, September 2020. Retrieved from https://www.microsoft.com/en-us/download/details.aspx?id=101738*
Bursztein, E., & Oliveira, D. (2019). *Deconstructing the phishing campaigns that target Gmail users. Paper presented at the Black Hat USA 2019, Las*

CVS: experiments to learn how this could work

1. Experiment with other questions – broad or more precise
    - Ask “what happened to you?”
2. Help people with their IT problems (*in a computer shop?*)
3. Integrate CC with measures of fraud victimisation
    - and ask ‘Online versus offline?’ & ‘How has this probably happened?’
4. Multi-disciplinarity: include computer scientists

Lets’ pay renewed attention to measurement issues

It matters for policy and prevention

Thank you!

Comparison of population CVS

1. Six crimes were comparable over 9 European CVS's
    1. Online shopping fraud
    2. Online banking/payment fraud (with or without loss)
    3. Other fraud
    4. Cyberthreats/harassment
    5. Malware
    6. Unauthorised access to personal information (including hacking, excluding offences that led to banking/payment fraud)

- CVS Statistics Netherlands*

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. doi:10.1186/s40163-018-0079-3