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 between the studies or real differences between countries or change over time.

Conclusions: As yet there have been very few well performed randomised sampled studies on cybercrime amongst the general population. Cybercrime prevalence (and its trend) can only be well measured if the questions are frequently updated and adequately address new aspects of cybercrime. To adequately monitor cybercrime in the future it is advisable to develop some fairly abstract main categories that are of durable validity, whilst allowing for up-to-date illustrations. Furthermore, ideally the questioning in the ongoing surveys in the different countries should be standardised and there should be a uniform categorisation of the different cyber offences. A screening question in order to permit more accurate dating is essential to reduce telescoping bias. Surveys should ask about the impact on or damage to the victims.

Keywords: Cybercrime, Citizens, Surveys

Background

The world is online, and this also applies to criminals. With the growth of the internet, new crimes emerged that have been labelled cybercrime (Bregant and Bregant 2014; Jang-Jaccard and Nepal 2014; Jewkes and Yar 2010; Newman 2009; Reyns et al. 2014; UNODC Intergovernmental expert group on cybercrime 2013; Wall 2007). Knowing that half of the world population nowadays is online (Internet World Stats 2017), we know that half of the world population is at risk of becoming a victim of a personal cyber offence. What we do not clearly know is what fraction of the population has actually been a victim of this type of crime.

'Cybercrime has climbed to the top tier in the National Security Strategy of many EU states.' (Armin et al. 2015, p. 135). Armin et al. (2015) *also state that 'Governments need reliable data on crime in order to both devise adequate policies, and allocate the correct revenues'* (Armin et al. 2015, p. 135). But at present official statistics on

*Correspondence: m.junger@utwente.nl
[2] University of Twente, Enschede, The Netherlands
Full list of author information is available at the end of the article
The views expressed in this paper are those of the author(s) and do not necessarily reflect the policies of Statistics Netherlands

cybercrime suffer from important problems. Anderson et al. (2013) conclude that '*There are over 100 different sources of data on cybercrime, yet the available statistics are still insufficient and fragmented; they suffer from under- and over-reporting, depending on who collected them, and the errors may be both intentional (e.g., vendors and security agencies playing up threats) and unintentional (e.g., response effects or sampling bias).*

Cybercrime is a broad and imprecise concept (UNODC Intergovernmental expert group on cybercrime 2013). Often three broad categories of cybercrimes are distinguished (Wall 2005). First, *crimes against computers* imply the unauthorized access of the boundaries of computer systems such as cyber-trespassing or hacking/cracking, where the computers are the focus of the attack. Examples include computer viruses, denial-of-service attacks, and malware (malicious code). Second, *crimes using computers, often referred to as 'cyber-enabled crime',* are crimes that use Information and Communication Technology (ICT) to commit a crime, such as identity theft, phishing scams and the fraudulent use of credit cards online. Third, *crimes 'in' computers*, where criminal content is the crime. Examples of main content-related cybercrimes are pornography, threats of violence and terrorism (Wall 2007). In practice, this distinction can be imprecise: a phishing mail can be used to seduce users to click on a link to steal information, which is ICT as a modus operandi, but also installing malware, which is a computer integrity offense. At present there is no universal agreement on a classification of types of cybercrime (Gordon and Ford 2006; Reyns et al. 2014; Stol 2012).

Although there is no universal conceptualisation of the different forms of cybercrime, we first describe briefly a number of major forms of cybercrime that have been measured by some victim surveys.

Online shopping fraud

Online shopping is characterized by the inability to inspect merchandise before purchase, and/or a lack of direct contact between the parties involved in the sale (Moons 2013; van Wilsem 2013a). Accordingly, consumers are at higher risk of fraud than in face-to-face transactions. When ordering merchandise online, the item may not be delivered, the item may not work or it might not be the same item as in the online photo. Merchants also risk fraudulent purchases if customers are using stolen credit cards (Enisa 2010; Moons 2013; van Wilsem 2013a).

Online banking fraud and payment

Online banking fraud occurs when the fraudster gains access to, and transfers funds from, an individual's online bank account. In some cases, an individual may be duped by a criminal into making a fraudulent money transfer themselves (FFA 2016). Online banking fraud can start with a phishing mail that directs users to a fraudulent website where he has to fill in login information or that installs malware on a computer which then steals login information (Brody et al. 2007; Milletary and Center 2005).

Other cyber fraud

This comprises for instance advanced fee fraud and identity fraud (Enisa 2010). The scam typically involves promising the victim a significant share of a large sum of money, in return for a small up-front payment, which the fraudster requires in order to obtain the large sum (Enisa 2010).

Identity theft is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name and to the other person's disadvantage or loss (Enisa 2010; Harrell and Langton 2013; Tuli and Juneja 2015). Identity theft occurs when someone uses another's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The person whose identity has been used may suffer adverse financial and/or emotional consequences if they are held responsible for the perpetrator's actions (ITRC 2014).

Cyber threats/bullying

Cyberbullying is bullying that takes place using electronic technology (Kowalski et al. 2014; Nansel et al. 2003; Wachs et al. 2017). Children who are being cyberbullied are often bullied in person as well (Wachs et al. 2017). Additionally, kids who are cyberbullied have a harder time getting away from the behaviour. Cyberbullying is different from traditional bullying is a number of ways. First, cyberbullying can happen 24 h a day, 7 days a week. Second, cyberbullying messages and images are often posted anonymously and they can be distributed quickly to a very wide audience. Third, deleting inappropriate or harassing messages, texts, and pictures is extremely difficult after they have been posted or sent (Stopbullying.gov 2017).

Malware

Malware (short for malicious software), is an umbrella term used to refer to a variety of forms of hostile or intrusive software, (1) including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software (Aycock 2006).

Hacking or computer intrusion

A security hacker is someone who seeks to breach defences and exploit weaknesses in a computer system or network in order to get into the system. Hackers may be motivated by a multitude of reasons, such as profit, protest, information gathering, challenge, recreation, or to evaluate system weaknesses to assist in formulating defences against potential hackers (Bachmann 2010; Conteh and Royer 2016).

At present reliable statistics about victims of cybercrime are rare (Cliff and Desilets 2014; Leukfeldt 2017; Lynch 2006), although crime statistics are important for policymakers. A commission of the UK government (Smith 2006) listed several reasons why a nation needs crime statistics at a national level:

1. to provide reliable quantitative measurements of criminal activity and trends that enable the parliament to fulfil its democratic function of holding the government of the day accountable for this aspect of the state of the nation;
2. to keep the public, media, academics and relevant special interest groups informed about the state of crime in the country and to provide (access to) data that inform wider debate and non-governmental research agendas;
3. to inform relevant aspects of short-term resource allocation, both within government and also for external related bodies—e.g. for policing and victim support;
4. to inform performance management and accountability at the national level of agencies such as the police;
5. to provide an evidence base for longer-term government strategic and policy developments.
6. We would add the importance in applying pressure on the designers and operators of ICT systems, software applications, etc. to design and manage their products in such a way as to reduce opportunities and provocations for crime; and in providing reliable and valid data which can be used in time series analysis and impact evaluations of preventive efforts.

The two main sources of statistics about victim prevalence are self-report victim surveys and police registrations. The present study focuses on victim surveys. Victim surveys have been of increasing importance for crime statistics since their development in the nineteen-seventies (Hough et al. 2007; Rand 2007). They have profoundly affected knowledge and theories about crime (Cantor and Lynch 2000; Hough and Maxfield 2007). Victim surveys provide information on the amount of crime and on the trends in crime, independent of the reporting behaviour of victims and recording practices by the police, and this was the main motive for developing them (Cantor and Lynch 2000; Hough et al. 2007; Lynch 2014; Rand 2007). Police recorded figures cannot assess historical changes as the willingness to report a crime by the victims and the methods of recording by the police differ over time (Lynch 2014; Wittebrood and Junger 2002). Victim surveys have been important to the study of crime in other ways as well: they led to the creation of new ways of classifying crimes, they were important in the research into opportunity and routine activities approaches (Cohen and Felson 1979; Wortley and Mazerolle 2008), they provided new information on contact crimes and they provided information on the consequences of becoming a victim (Cantor and Lynch 2000; Gottfredson 1986; Lynch 2014). Finally, victim surveys are the best method for international comparisons of crime rates (Aebi et al. 2002; Dijk 2007; Messner and Zimmerman 2014).

Of course victim surveys also have their limitations.

1. Because becoming a victim of crime is relatively rare, large samples are needed and this makes victim surveys labour intensive and relatively expensive (Maxfield et al. 2007; Rand 2007).
2. This cost aspect is exacerbated by the fact that response rates have been declining, whether they are conducted face-to-face, by telephone or online (Maxfield et al. 2007; Rand 2007).
3. Sampling frames can be a problem. Most surveys focus on 'households', and, accordingly, they miss certain categories of people, e.g., the homeless and people in institutions. In some countries these categories became an increasing part of the population, for instance in the UK (Maxfield et al. 2007).
4. In previous research, several methodological choices and survey characteristics have been shown to be related to the estimates of crime prevalence (Addington 2008; Eckberg 2015; Powers 2015; Schneider 1981; Skogan 1986; Tourangeau and McNeeley 2003):

- The wording of the questions is important. The wording has to be clear and easily understood, and not open to different interpretations. The questions should measure very precisely what the survey wants to know. A very important aspect in these is the correct dating of the offences. In order to prevent telescoping bias a survey should include a kind of 'screening' question that asks about crime prevalence in a longer period, preceding the actual question that asks about the period of investigation. Victims can tell their story even if the crime happened

outside the required timeframe. Recent research showed that the exclusion of such a screening question led to high telescoping (Reep 2013a, 2014). Telescoping results in an overestimation of crime prevalence.

- It has been proven that the mode(s) that have been chosen to collect the data influence the results (Schouten et al. 2013). Interviewer-guided questionnaires can go into more detail and interviewers can clarify questions if needed. However, victims might be reluctant to share their story with an interviewer as well, since they may feel ashamed or the perpetrator might be close by. Self-administered questionnaires are cheaper and allow access to more respondents, but there is little control of how questions are interpreted.

5. Another important topic is any possible self-selection bias. It is likely that people that have affinity to the subject of a questionnaire, for instance because they have been a victim of crime, respond to a victim study more readily than those who have not. An over-representation of victims in a victim survey will result in an overestimation of crime prevalence, unless this is corrected for by weighting the data. Recent research (Reep 2014) showed that victims of online shopping fraud who reported the offence to the police responded more often to the victim survey than those who have not been a victim. This was not the case for victims of other computer crime (in this case mainly hacking) (Reep 2014). Other research showed that victims of cybercrime participate earlier during the fieldwork (faster or need less reminders) than those who were not victims (Reep 2013b). An intensive reminding process that results in a higher response rate will reduce the self-selection bias and increase the validity of the estimates.
6. The types of the crimes included in most victim surveys is limited. Surveys should be suitably brief in order to keep people willing to respond. This however results in a limitation to the detail in questioning about the crimes.
7. Finally, with the increasing digitalization, the nature of crime has been changing and cybercrime has been included only recently in a number of national victim surveys (Armin et al. 2016; Kanich et al. 2011; Maxfield et al. 2007). Victim surveys necessarily tend to be stable over time. The nature of cybercrime however has been rapidly evolving. There has not been much experience on how to formulate questions for the most common types of cybercrime(s). This makes it hard to get accurate figures that are comparable over time and over countries.

The present study's goal is to present the prevalence of cybercrime in Europe. To that end our aim was to select victim surveys of general populations that measured cybercrime. Accordingly, we provide a qualitative and quantitative comparison of how cybercrime has been measured in Europe and give an overview of the main prevalence rates.

Methods

Study selection and inclusion criteria

To select relevant victim studies for the present review the following set of inclusion criteria have been used.

First, the methodology of the study had to be clearly described, and insight in the questionnaire had to be given so that the results could be properly evaluated.

Second, the survey had to be based on a large statistically random selection of (people living in) private households, in order to produce results representative for a country.

Third, a weighting procedure had to be performed in order to produce representative results.

Fourth, the study needed to present crime prevalence rates over a clearly defined period so that *annual* crime prevalence rates could be calculated.

Fifth, figures had to represent the period since 2010. This year was chosen for practical reasons and to increase the likelihood that surveys would provide figures over the same time period that would allow comparisons of trends, as most surveys were of relatively recent date.

As the use of the internet has grown in the last 20 years this will influence the prevalence rates for cybercrime. For example, ten years ago online shopping was less common than it is today which results in less victims of online shopping fraud.

Sixth, at least one specific type of cybercrime is explicitly measured, not 'cybercrime' as a global concept.

We already knew about the existence of three surveys that have measured aspects of cybercrime in the Netherlands and about the crime survey for England and Wales. To find other victim surveys we first searched through library databases of Twente University[1] and in Scopus. The following search keywords were used: 'victimization' and 'cybercrime' and 'survey'. This provided 35 hits. None of these however could be considered to be a crime survey on representative samples in Europe and did fit our criteria on adequate measurement layout above.[2]

[1] Including: ACM Digital Library, AMS Journals, BioOne, Directory of Open Access Journals, IEEE Publications Database, Informa Healthcare e-Journals, MEDLINE, ScienceDirect, SPIE Digital Library, SpringerLink, Staten-Generaal Digitaal: Dutch Parliamentary Papers, Wiley Online Library, WorldCat.org.

[2] An overview of these 35 studies can be obtained from the authors.

In a next step we searched with internet search engines to find surveys. This resulted in a few articles about the prevalence of cybercrime, only one of which fulfilled our inclusion criteria. We knew that large population surveys are generally executed by governmental institutes that usually publish only on the governmental websites in their own language.

This led to us searching for grey literature. We contacted statistical institutes (hereafter 'institutes') which were known to have executed victim surveys and asked them directly what they have measured in the field of cybercrime. We contacted institutes in Sweden, Germany, Luxembourg, France, Norway, Belgium, Austria, Latvia, Portugal, Finland and Poland. Some institutes did not conduct victim surveys at all anymore, some did not include cybercrime and some provided extra figures for this survey. From other European countries, to the best of our knowledge, we knew that there were no population victim surveys. It is possible that we overlooked some surveys.

Classifying cybercrime and estimating its prevalence

There is no existing clear classification, stable over time that captures all possible old, new and possible future types of cybercrime. In this survey the following six types of cybercrime are distinguished. These types of cybercrime are operationalised by the questions as they were presented to the respondents.

- *Online shopping fraud* All questions mention that online shopping fraud refers to fraud as a result of buying or selling goods online. Only the Swedish questionnaire is different. In the Swedish study the question runs: 'cheated out of money or other valuables' online. If this occurred by the use of 'bank card or a bank account' this was classified as 'online banking fraud', otherwise, it was considered to be 'online purchase fraud'.
- *Online fraud banking/payment* All questions on online fraud banking/payment refer to money disappearing from bank accounts. However, the CSEW (United Kingdom) does not explicitly mention this description but asks whether the respondent noticed that '*personal information or account details (had) been used to obtain money, or buy goods or services without your permission or knowledge*'(Office for National Statistics (ONS) 2015, p. 26) which is less explicit.
- *Other cyber fraud (such as advanced fee fraud and other identity frauds)* Fraud is a very broad category(National Fraud and Cyber Reporting Centre 2016). The CSEW (United Kingdom) asks questions about identity theft (for instance: the use of a victim's personal details to make an application, e.g. for a mortgage), fake investments, or sending money to someone 'who turned out to be not who they said they were?'. A similar approach was used in the ODW (The Netherlands).
- *Cyber threats/harassment* Most questions refer to receiving threatening messages. However, the ODW (The Netherlands) asks about stalking with the explicit reference to 'repeated harassment'.
- *Malware* All questions on malware explicitly mention having a 'virus on your computer', with the exception of the WISIND (Germany) question, which is more general and asks if one's devices have 'been infected with malicious software'.
- *Hacking* The questions on hacking are formulated in several ways. In the CSEW (United Kingdom) it consists of 'stolen information from your device'. The VM (The Netherlands) asks if 'someone—with malicious intent—broke into or logged on a computer, e-mail account, website or profile site?', The ODW (The Netherlands) asks about altering web-content, stealing or altering data on a device, breaking into your email account. Surveys specifically exclude answers in the case hacking was the modus operandi for financial fraud or cyber threats/harassment. Thereby, in principle, they avoid possible double counts with other types of fraud. Similarly, surveys ask about incidents that 'were not mentioned previously', also to avoid double counts.

Ideally there should be an indication about the severity for every offence type, for example a division into whether or not the incidents resulted in any harm or loss or distress. This review provides information if the surveys include any such measurements, but do not break down the figures in amount of harm.

The estimates in this review on the prevalences are given for all categories of cybercrime. The published estimates are presented in Additional file 2: Appendix S2. If the survey only provides estimates for the online population, the estimates are adjusted to cover the whole population by multiplying the estimate with the fraction that uses the internet. If the study period exceeds 12 months, the prevalence is adjusted to cover only 12 months. And if only total figures for a crime type are published with the fraction that is cyber related, the cyber related estimate is calculated. The resulting prevalences are presented in 6 figures, one for each crime category. All prevalences relate to the total non-institutionalized population.

Given that this study is based solely on secondary data, we did not need the approval of an ethical committee.

Table 1 Survey characteristics

Survey	Country	Mode data collection	Year first data collection on cybercrime[a]	Periodicity data collection on cybercrime	Percentage response rate[b]	Number of respondents for cybercrime (in thousands)	Age group studied
NTU	Sweden	By telephone[c]	2006	Every year	60–76	12–15	16–79
CSEW	UK	Face-to-face	2016	Every year	72	18	16+
VM	The Netherlands	Online and on paper	2012	Every year	37–41	80–145	15+
ODW	The Netherlands	Online and on paper	2011	One-off	47	10	15+
ITN	The Netherlands	Online and by telephone	2015	One-off	41	5	12+
WISIND	Germany	By telephone	2014	One-off	21	12	16+
DV	Germany	By telephone	2012	First time, second one in 2017	22	32	16+
CVS	France	Face-to-face	2010	Every year		15	14+
ES	Luxembourg	By telephone	2013	First time, second one in 2017	30	3	16+

[a] Most often the 12 months preceding the survey are investigated

[b] For telephone surveys measured as percentage of the eligible numbers, for study 3,4,5 measured as the percentage of the total bruto sample

[c] Approx 12% responded online or on paper, these respondents don't get the questions if a crime happened online

Results

The institutes in Norway, Belgium, Austria, Latvia, Portugal, Finland and Poland did not have usable information for us. The following nine surveys meet our strict inclusion criteria and are included in this review:

1. NTU—Nationella trygghetsundersökningen, conducted by The Swedish National Council for Crime Prevention (Brå) (Brå 2016).
2. CSEW—Crime Survey for England and Wales, conducted by the Office for National Statistics (Office for National Statistics (ONS) 2017).
3. VM—Veiligheidsmonitor, conducted by Statistics Netherlands (CBS 2017; Statistics Netherlands 2013, 2017).
4. ODW—(on)veiligheid in de digitale wereld, a one-off (Domenie et al. 2013) (ODW is not an official abbreviation).
5. ITN—ICT gebruik van huishoudens en personen, a one-off (CBS 2015; Eurostat 2016) (ITN is not an official abbreviation).
6. WISIND Projects, a one off (Rieckmann and Kraus 2015).
7. DV—Der Deutsche Viktimisierungssurvey, conducted by the Max-Planck-Instituts für ausländisches und Internationales Strafrecht (Birkel et al. 2014) (DV is not an official abbreviation).
8. CVS—Cadre de Vie et Sécurité, conducted by the Institut National de la Statistique et des Études Économiques (INSEE) in France (ADISP 2015).
9. ES—Enquête sur la Sécurité 2013, conducted by the National Institute for statistics and economic studies of the Grand Duchy of Luxembourg (STATEC 2015) (ES is not an official abbreviation).

As the estimates probably rely more on the methods of data collection than on the country we choose not to refer to the surveys by name of the country in which they are conducted. In this review the surveys are referred to by their abbreviation as given above.

Main characteristics per survey

The main design features of each selected study are presented in Table 1. All surveys are based on a large random selection of (residents in) private households. Most surveys are led by an interviewer, 4 by telephone and two face-to-face. Three surveys, all of them from The Netherlands, use a mixed mode design in which one of the modes is online. The response rates of the NTU and CSEW are very high, but we do not know exactly how this is measured, for instance, we do not know if framing errors such as 'wrong address' are excluded as being non-response. The response rates of the WISIND and DV are relatively low which implies that these surveys might suffer from selection bias. Most surveys only include the population of around 15 years and older. The NTU was the first that included any questions on a cyber component to the offence in the questionnaire, in 2006. Finally, the reference period in all surveys was 12 months, with

Table 2 Types of cybercrime that are covered in the questionnaires

Study	Questions about crime prevalence over a period of 12 months of												
	Online shopping fraud		Online banking and payment fraud		Other fraud				Cyberbullying/ threats/sexual offence		Malware		Hacking
					Advanced fee/ dating fraud		ID fraud other than banking						
	Victim	Damage	Victim	Damage	Victim	Damage	Victim	Damage	Victim	Damage	Victim	Damage	Victim
NTU	y	f	y	f					y	e			
CSEW	y	fet	y	fet	y	fet	y	fet			y	fet	y
VM	y		y						y				y
ODW	y	f	y	f	y	fe	y	fe	y	fe	y	f	y
ITN											y	f	
WISIND	y	f	y	f							y	f	
DV	y	fet[a]											
CVS			y	f									
ES	y	e	y	e									

y: questioned

f: includes questions on financial loss

e: includes questions on emotial impact

t: includes questions on time loss

[a] There is a 4 point scale question on the seriousness of the incident, this implicitly includes finance, emotion and/or time

the exception of the WISIND survey (Rieckmann and Kraus 2015) where it is 30 months.

Table 2 shows for each study the cyber offences that are covered. As we think it is important to include information on harm of any kind with statistics on cybercrime, this table also shows whether or not the study addresses any loss involved with the incident; financial, time or emotional. Only ODW, which was a one-off, asked questions about all seven types of cybercrime. Only the VM has included many types for a few years in a row. Most studies only ask about one or two cyber offences. Nearly all studies ask something about the loss or harm that was incurred by the crime. Most surveys measure the financial loss, only the ES survey also measured the emotional impact of every crime.

Additional file 1: Appendix S1 presents an overview of the questions by survey and type of cybercrime, questions in native languages have been translated into English. The crime prevalence estimates are based on these questions. As the measures on loss or harm are very diverse, only the questions where the respondent is asked if he or she is a victim of crime are presented. The NTU, the VM and the CVS have measured cybercrime for a few years now and kept the questions unchanged. The CSEW is conducted face-to-face and uses a very intensive approach. This makes it difficult to make a detailed analysis of the questioning. In addition some open questions are used to categorise offences. This is why the questions as provided in Additional file 1: Appendix S1 do not cover exactly all questions/information that are used to classify someone as a victim of the type of offence concerned.

As mentioned before the measurement of (cyber) offences closely depends on the wording of the questions. As shown in Additional file 1: Appendix S1, for online shopping fraud, banking fraud and malware most surveys use similar wording, however they are not exactly the same.

A correct dating of the incident is also important for a precise estimate of the prevalence in the reference period. The former mentioned screening question that covers crime prevalence over a long period is included by ODW, DV, ES and the CVS. The surveys that have been carried out repeatedly over a few years have kept the wording of the questions identical which normally gives a greater chance of providing correct trends.

The prevalence estimates as published or provided in the available reports or by respective researchers are presented in Additional file 2: Appendix S2. Some studies only presented figures for the online population, some covered a longer time frame and others only present the percentages of the overall crimes that are cyber related (see notes under Additional file 2: Appendix S2). Confidence intervals were only provided by the VM, ODW, DV and the ES. Additional file 3: Appendix S3 presents the figures as published/provided after adjustment for comparability (see method section) and so represent the estimated 12 months prevalence for the total

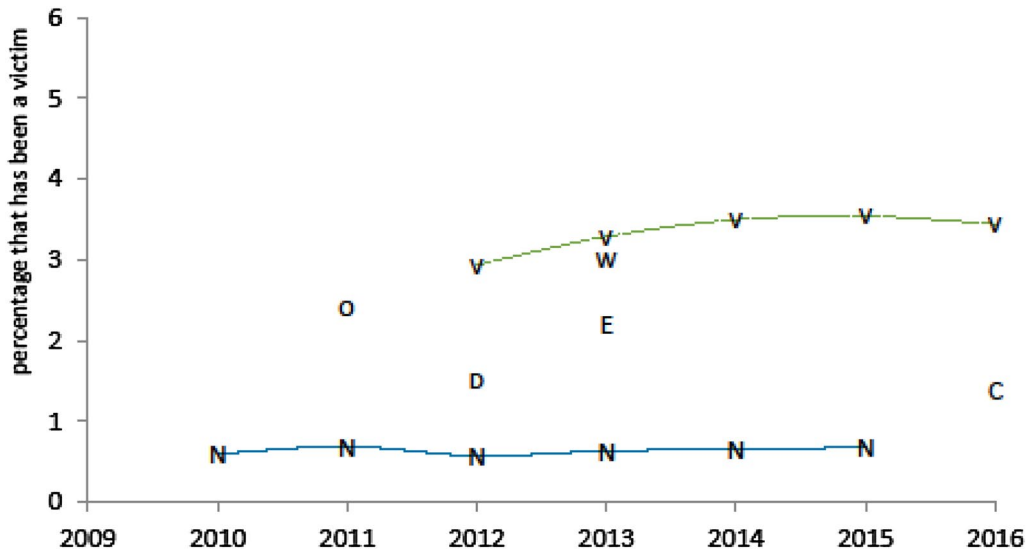

Fig. 1 Self-reported crime prevalence for online shopping fraud. N = NTU, C = CSEW, V = VM, O = ODW, I = ITN, W = WISIND, D = DV, Cv = CVS, E = ES

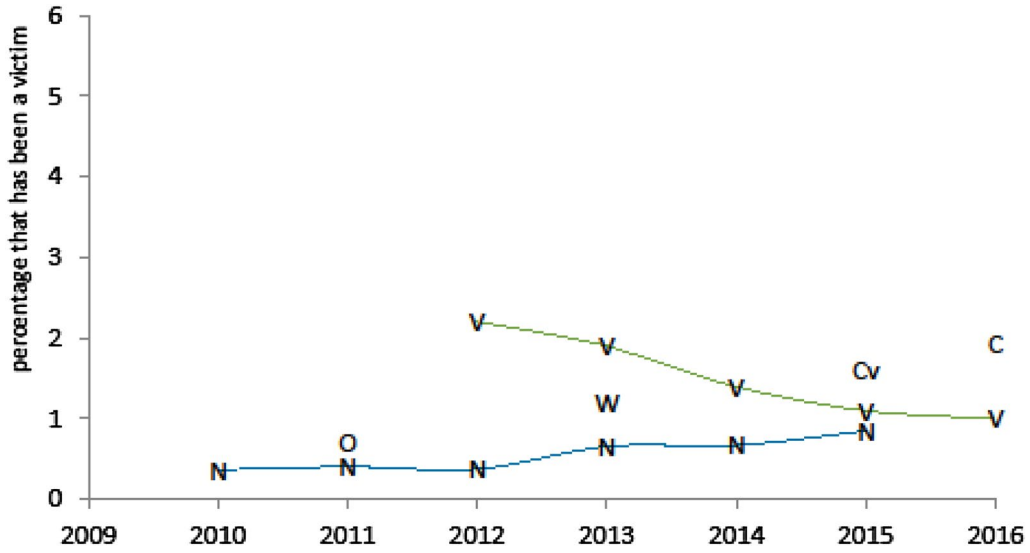

Fig. 2 Self-reported crime prevalence for fraud online banking. N = NTU, C = CSEW, V = VM, O = ODW, I = ITN, W = WISIND, D = DV, Cv = CVS, E = ES

non-institutionalised population. These figures are presented in Figs. 1, 2, 3, 4, 5 and 6 and in text below.

Online shopping fraud

0.6–3.5% of the population reported having been a victim of online shopping fraud every year. Most of the offences, approximately 90%, concern the purchasing of goods or services (paid but not received). The DV and ES only measure online purchasing fraud. The crime prevalence rate increased a little between 2012 and 2013 according to the VM, but has stabilised since. The NTU shows a stable pattern over the period 2010–2015.

Online banking fraud and payment

The prevalence rates for online banking fraud and other online payment methods generally are lower than for online shopping. The prevalence rates range from 0.4 to 2.2% per year. According to the VM, bank fraud has decreased since 2012 while the NTU shows a slight increase since 2010.

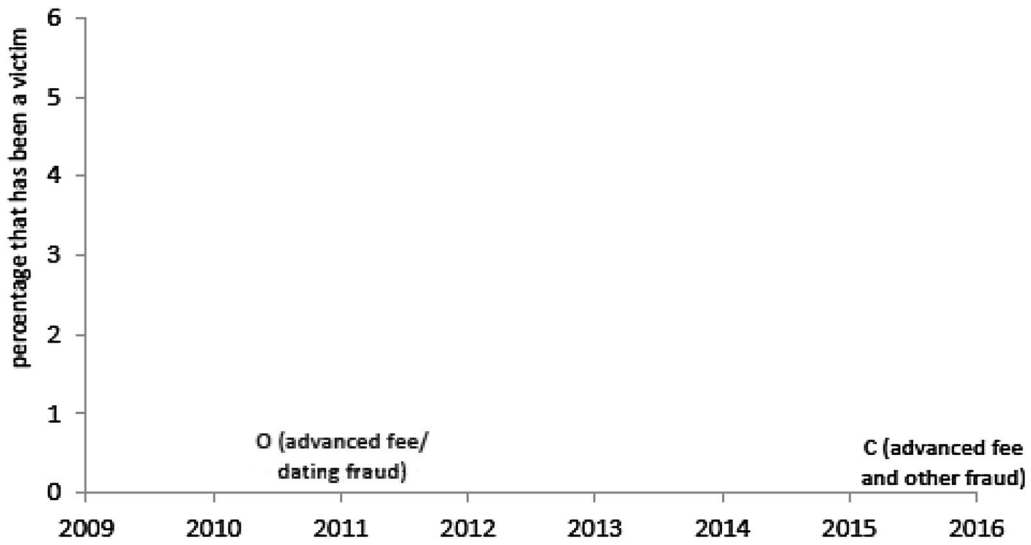

Fig. 3 Self-reported crime prevalence for other cyber fraud. N = NTU, C = CSEW, V = VM, O = ODW, I = ITN, W = WISIND, D = DV, Cv = CVS, E = ES

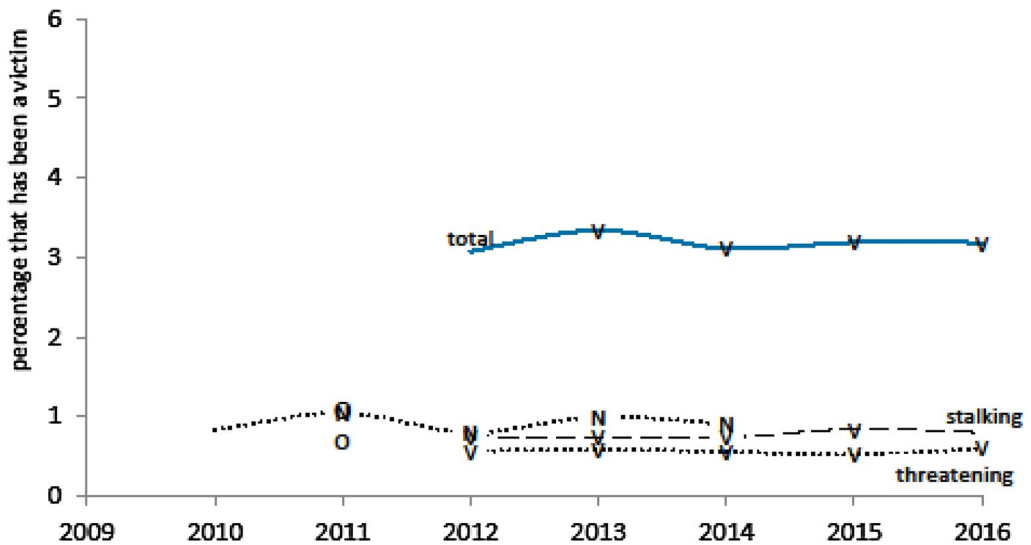

Fig. 4 Self-reported crime prevalence for cyberbullying. N = NTU, C = CSEW, V = VM, O = ODW, I = ITN, W = WISIND, D = DV, Cv = CVS, E = ES

Other cyber fraud

There are many examples of online fraud that do not involve online shopping or online banking. These other types of cyber fraud are mainly referred to as identity theft and include types like advanced fee fraud, impersonation of a well-known shop or brand, or identity fraud to obtain medical help or commit a crime. Many surveys ask about identity fraud/theft, but few make a distinction between online and traditional ways of committing this type of fraud, which is why they were not included in the present review. The scarce figures on this are shown in Fig. 3 and illustrate the absence of figures on these offences. According to the ODW 0.2% became a victim of advanced fee or dating fraud in the year 2011. The CSEW published it as 'other fraud', which includes non-banking ID-fraud as well. This study gives for 2016 a crime prevalence estimate of 0.4%.

Cyberbullying

Only the NTU, ODW and the VM measure some aspects of cyberbullying that is not only focused at youth. According to the VM, every year around 3% of the

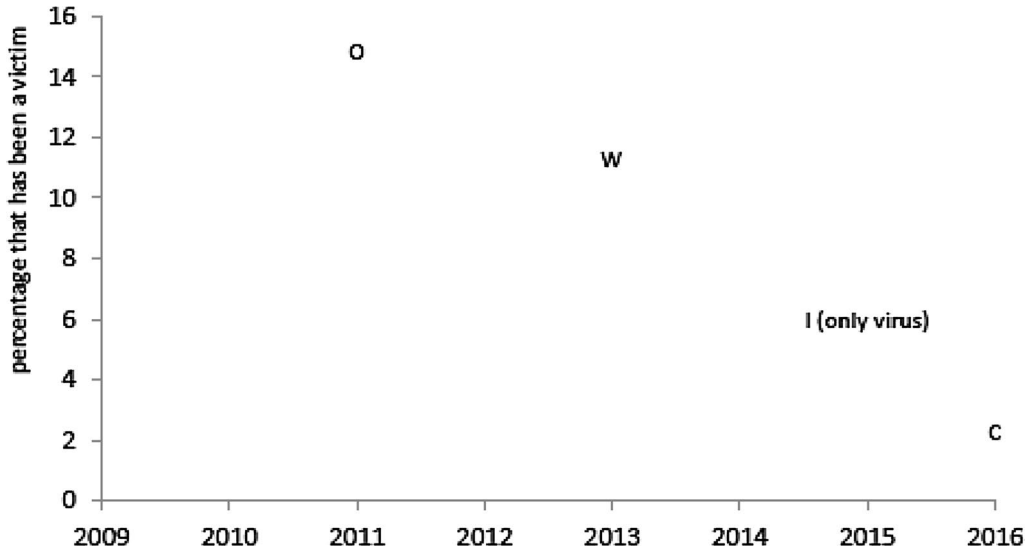

Fig. 5 Self-reported crime prevalence for malware. N = NTU, C = CSEW, V = VM, O = ODW, I = ITN, W = WISIND, D = DV, Cv = CVS, E = ES

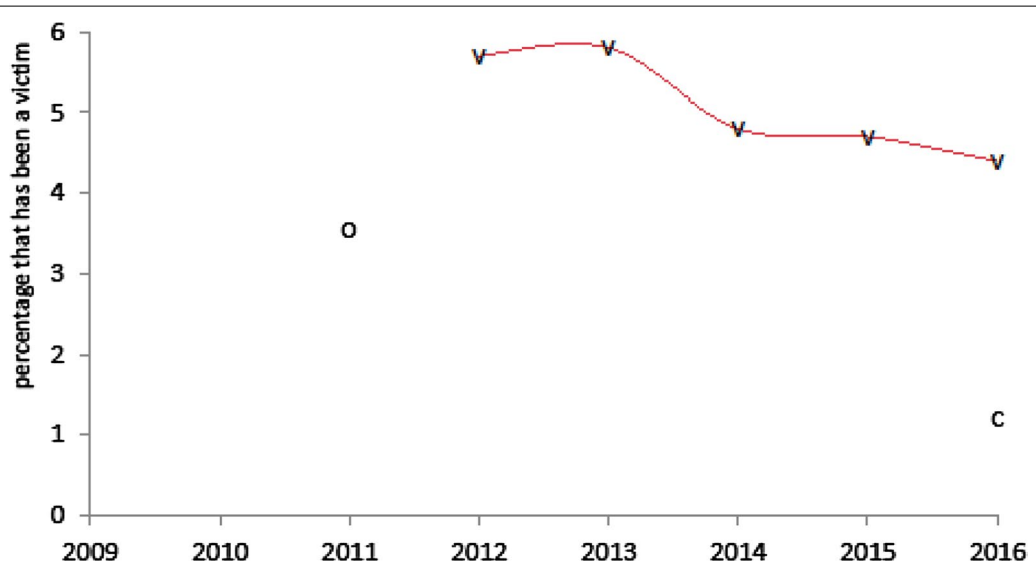

Fig. 6 Self-reported crime prevalence for hacking. N = NTU, C = CSEW, V = VM, O = ODW, I = ITN, W = WISIND, D = DV, Cv = CVS, E = ES

population has been bullied online. This has remained the same since 2010. These 3% can be divided into stalking, threatening, blackmail, slander and other types of criminal behaviour. Only stalking and threatening have been measured by other surveys. Every year, between 0.6 and 1.0% of the population reports having been threatened. Stalking happens to a similar proportion of 0.7–1.1%. Note that in these figures the emotional impact on the victims is not accounted for, so relatively minor incidents may be included.

Malware

The crime prevalence estimates for malware are quite diverse and range from 15% in 2011 (as measured by the ODW) to 2% in 2016 (measured by the CSEW).

Hacking

Every year, 1.2–5.8% of the population is a victim of hacking. As in all preceding offences, the VM shows a higher rate than the ODW. The VM shows a clear downward trend for hacking.

Discussion and conclusions

The current review presents the estimated prevalence of six types of cybercrime in Europe since 2010. The surveys included in the analysis were judged to be very well conducted and should therefore lead to good estimates. Still these estimates are based on a mix of different questions, different interviewing modes, country differences and period changes and possibly suffer from different selection biases. These factors are so intertwined that, with this number of surveys, they cannot be separated into their differential effect on the crime prevalence estimates. Another important aspect that has to be kept in mind when interpreting the results is that the internet penetration and the intensity of internet usage might differ between the populations that have been studied. A higher internet usage gives a higher risk of becoming a victim of cybercrime, as several studies showed (Choi 2008; Holt and Bossler 2008; Junger et al. 2017; Pratt et al. 2010; Reyns and Henson 2015; van Wilsem 2013a, b).[3] For nearly all countries that are included in this survey the percentage of the population that uses the internet slightly increased during our study period (Eurostat 2016). All these Western countries have a high internet penetration. But just like the methodological issues that influence the crime prevalence estimates, the estimates about internet penetration will depend on the methods of the data collection.

Despite all the methodological factors that influence the crime prevalence estimates, and despite the fact that we will not be able to unravel these, this review can provide ranges of crime prevalence rates. Annual prevalence rates for online shopping fraud range from 0.6 to 4%. The operationalisation of this type of crime is quite straightforward. The (VM) estimate of 4% is too high because of measurement errors (Reep 2017). We do not have information about the quality of the other surveys. We believe, based on the present review that the prevalence of online shopping fraud ranges from 1 to 3%. From the surveys that could provide trends, it is not clear if the overall prevalence has increased since 2010. The VM shows an increase, the NTU shows a stable pattern.

Fraud with online banking/payment seems to happen less frequently. Estimates range from less than 1 to 2%. This rate seems to have decreased according to the VM, and slightly increased according to the NTU. Again we cannot conclude that these changes resemble a real change in the countries concerned, as the nature of online financial fraud might have changed, but the questions about it have not. Note that there are substantial differences between the questions that have been used in the VM and the NTU. These might cause the conflicting trends. It is interesting to note though that the Dutch banking association published a strong decrease in banking fraud since 2011 (Dutch Banking Association 2017). This decline has been attributed to several preventive measures taken by the banks, namely geo-blocking, protecting ATMs physically against skimming, transaction monitoring and cooperation with the police (Dutch Banking Association 2017). However, in Sweden banks have taken the same measures (Westerberg 2017), which is why we had also expected a downward trend here.

Less than 1% of the population are victims of other types of cyber fraud such as advanced fee- or other types of identity fraud. These frauds are very rare, but if they happen they often have a large emotional and financial effect on its victims. Online dating fraud first became apparent about 10 years ago. Whitty and Buchanan (2012) found that 0.5% of British adults had at some point been a victim of an 'Online Romance Scam' by the year 2011. This review shows that there is a lack of information on the annual prevalence of this type of cybercrime. We found two studies that addressed these frauds. According to the ODW 0.2% became a victim of advanced fee or online dating fraud in the year 2011. The CSEW published it as 'other fraud', which includes non-banking identity fraud as well. This study gives for 2016 a prevalence estimate of 0.4%.

Another type of crime that is distinguished in this review is cyber bullying. This has the potential of being one of the most serious online crimes as far as individuals are concerned. News items about a teenager that commits suicide as a consequence of being bullied online are becoming painfully common. (Cyber)bullying mainly happens to teenagers (CBS 2017), and there are many large surveys that measure cyberbullying of youth [for instance (Brå 2016; Jones et al. 2013; Kerstens and Veenstra 2015; Näsi et al. 2016; Office for National Statistics (ONS) 2017)]. These surveys based on adolescents cannot however be generalized to the whole population so are not included in this review. Only the NTU, ODW and the VM measure some aspects of cyberbullying that are not focussed only on youth. According to these surveys a maximum of 3% of the population experiences some sort of online bullying such as stalking (1%) or threatening (1%). Note that being or feeling bullied has sometimes a subjective aspect and that is one of the reasons that make it difficult to operationalise this concept. In order to avoid the inclusion of every minor form of harassment, questions should investigate the emotional impact on victims. This is done by the NTU and the ODW.

[3] Please note that not all studies found that indicators of routine online activities are related to becoming a victim (Holt and Bossler 2013; Ngo and Paternoster 2011).

According to our surveys every year, 1–6% of the population is a victim of hacking. As the highest estimate is based on questions that do not include a screening question, we suggest a prevalence of hacking between 1 and 4%. Only the VM provides a trend for this type of crime. The survey shows a decreasing trend since 2012. This might be because the examples in the questionnaire have not been changed since 2012, and accordingly new forms of hacking might be missed like the hacking of cars.

The estimates of crime prevalence by malware range from 2 to 15%. Malware is a rather broad category and it is arguable if it should be distinguished as a cybercrime. Accordingly the various surveys operationalise it in very different ways. Seemingly, as everyone receives malware, we advise to only include the victims that really have suffered from it. But we do not yet have a good suggestion to measure this.

A discussion point that we have not yet addressed in this review is the measurement of unknown crime. Not every victim knows about the offence. For instance, if someone receives a fraudulent bill via e-mail, that person might just pay it. This might happen quite often but, of course, we cannot gain information on this from the ignorant victim.

Another observation is that all included surveys were from Northern/Western Europe. Surveys are expensive to conduct. It seems possible that the governments of East-European countries have less money to spend on crime research. Also, as internet usage is lower in many East-European countries (Eurostat 2016), this implies that surveys cannot be executed online easily and alternatives (like face-to-face interviews) are usually more expensive.

This review provides the questions that have been asked on personal cybercrime prevalence in European surveys up to now. It would be interesting to see if and how much the amount of cybercrime differs between countries. Several authors discussed the problems and benefits of cross-cultural comparisons, specifically in the study of crime (Gartner 1993; Karstedt 2001). For instance, according to Karstedt (2001, p. 288) there are three main aims of cross-cultural research: (1) transport of criminological theories to other cultures and test of their limits and potential of generalization; (2) exploration and discovery of variations of crime and forms of social control; and (3) integration and widening of the data base for the development of an universal criminology.

But the prevalence estimates between countries are incomparable due to, most of all, question wording. That is why we propose that institutes standardise the questionnaires on cybercrime prevalence as much as possible. We have some recommendations that refer to question wording. Firstly, of course, question wording has to be very precise and avoid incorrect interpretations. Special attention has to be given to the correct dating of the offences. In many questionnaires dating is done by starting with a screening question that investigates if the respondent has been a victim in the preceding 5 years and followed by a more precise question about the incidence in the last 12 months. Support for the importance of screening questions has been provided by recent research (Reep 2014, 2017). In this research self-reported offences from the victim survey have been compared with the police records by means of reverse record checks. For online shopping fraud, 40% of the self-reported offences that could be traced in the police records happened before the selected time frame. As the telescoping rate was not this high for the other types of offences that did include a screening question, most of the telescoping will be caused by the lack of the screening question. Secondly it is advisable to include questions which provide more detail on what actually happened, and on the emotional or financial harm or time loss for the victim. We think this is very important to gain insight in the character of the offences and on the actual burden of cybercrime. This information can also help in deciding which offences to include and which not. Thirdly, many surveys on crime keep the wording constant over succeeding years in order to be able to measure trends. This is useful when the nature of the crime does not change, for example for bicycle theft, or robbery. But for cybercrime this is different. The appearance and modus operandi of the offences have been changing continuously, especially for crimes where the computer is the target and the category that includes all 'other frauds'. It is advisable to develop some fairly abstract main categories that are valid over a long timescale. The illustrations, often included in the survey questions, should thus be modernised whenever criminals have found new ways to attack.

All in all, our review shows that the cybercrime surveys in Europe give us an indication of the level to which individuals are victims of cybercrime. For comparative purposes, however, the surveys should be aligned with regard to the overall methodology and research design.

Additional files

Additional file 1: Appendix S1. Wording core question(s) on which the cybercrime prevalence is based.

Additional file 2: Appendix S2. Cybercrime: self reported crime prevalence per year.

Additional file 3: Appendix S3. Cybercrime: self reported crime prevalence per year, after adjustment to allow comparison between the surveys discussed in this article.

Authors' contributions
Study conception and design: MJ, CMMR. Acquisition of data: CMMR. Analysis and interpretation of data: CMMR. Drafting of manuscript: MJ, CMMR. Critical revision: MJ, CMMR. Both authors read and approved the final manuscript.

Author details
[1] Statistics Netherlands, Heerlen, Netherlands. [2] University of Twente, Enschede, The Netherlands.

Acknowledgements
We want to thank the following colleagues who provided extra data or information for this review: Emelie Hambrook, Anna Frenzel, Sara Westerberg and Johanna Skinnari (Brå), Johannes Rieckmann (WISIND project), Nathalie Leitgöb-Guzy and Christoph Birkel (Bundeskriminalamt), Guillaume OSIER (STATEC), Cyril Rizk (INSEE), and Michael Samson, Betaalvereniging Nederland (Dutch Payments Association).

Competing interests
The authors declare that they have no competing interests.

Availability of data and materials
Not applicable, analyses have been performed on existing data.

Consent for publication
Not applicable, analysis on existing data.

Ethics approval and consent to participate
We added the sentence 'Given that this study is based solely on secondary data, we did not need the approval of an ethical committee.'

Funding
No funding.

Publisher's Note

Received: 27 September 2017 Accepted: 7 March 2018
Published online: 04 April 2018

References

Addington, L. A. (2008). *Current issues in victimization research and the NCVS's ability to study them*. Paper presented at the prepared for presentation at the Bureau of Justice Statistics Data User's Workshop. Washington, DC.

ADISP. (2015). *Cadre de Vie et Sécurité—2015 (Living conditions and Safety—2015)*. Paris: Archives de Données Issues de la Statistique Publique. https://www.cmh.ens.fr/greco/enquetes/XML/lil.php?lil=lil-1003.

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.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265–300). Berlin: Springer.

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015). *2020 Cybercrime economic costs: No measure no solution*. In Paper presented at the availability, reliability and security (ares), 2015 10th international conference on.

Armin, J., Thompson, B., & Kijewski, P. (2016). Cybercrime economic costs: No measure no solution. In *Combatting cybercrime and cyberterrorism* (pp. 135–155). Berlin: Springer.

Aycock, J. (2006). Computer viruses and malware. In *Advances in information security* (Vol. 22).

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *The International Journal of Cyber Criminology, 4,* 643–656.

Birkel, C., Guzy, N., Hummelsheim, D., Oberwittler, D., & Pritsch, J. (2014). *Der Deutsche Viktimisierungssurvey 2012. Erste Ergebnisse zu Opfererfahrungen, Einstellungen gegenüber der Polizei und Kriminalitätsfurcht*. Wiesbaden, Germany: Bundeskriminalamt. https://www.bka.de/DE/UnsereAufgaben/Forschung/Dunkelfeldforschung/dunkelfeldforschung.html.

Brå. (2016). *The Swedish crime survey*. Stockholm http://bra.se/bra/bra-in-english/home/crime-and-statistics/swedish-crime-survey.html. Retrieved from http://bra.se/bra/bra-in-english/home/crime-and-statistics/swedish-crime-survey.html.

Bregant, J., & Bregant, R. (2014). Cybercrime and computer crime. In *The encyclopedia of criminology and criminal justice*. Hoboken: Blackwell Publishing Ltd.

Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting and Financial Studies Journal, 11*(3), 43–56.

Cantor, D., & Lynch, J. P. (2000). *Self-report surveys as measures of crime and criminal victimization*.

CBS. (2017). *Veiligheidsmonitor 2016*. Retrieved from Voorburg/Heerlen: https://www.cbs.nl/nl-nl/publicatie/2017/09/veiligheidsmonitor-2016.

Choi, K.-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308–333.

Cliff, G., & Desilets, C. (2014). White collar crime: What it is and where it's going. *Notre Dame Journal of Law, Ethics & Public Policy, 28*(2), 481–523.

Cohen, L. E., & Felson, M. (1979). Social-change and crime rate trends—routine activity approach. *American Sociological Review, 44,* 588–608.

Conteh, N. Y., & Royer, M. D. (2016). The rise in cybercrime and the dynamics of exploiting the human vulnerability factor. *International Journal of Computer (IJC), 20*(1), 1–12.

Dijk, J. V. (2007). The international crime victims survey and complementary measures of corruption and organized crime. In M. Hough & M. Maxfield (Eds.), *Surveying crime in the 21st century: Commemorating the 25th anniversary of the British crime survey* (Vol. 22, pp. 125–144). Monsey, NY: Criminal Justice Press.

Dutch Banking Association (Producer). (2017). Fact Sheet Security and Fraud.

Eckberg, D. (2015). Trends in conflict: Uniform crime reports, the national crime victimization surveys, and the lethality of violent crime. *Homicide Studies, 19*(1), 58–87.

Enisa. (2010). *How to shop safely online*. Heraklion: ENISA—European Union Agency for Network and Information Security.

Eurostat. (2016). *Community survey on ICT usage in households and by individuals 2016 quality report*. https://www.cbs.nl/-/media/_pdf/2017/03/ict-hh2016quality%20report%20final%20version%20netherlands.pdf. Luxembourg: European Commission.

FFA. (2016). *Fraud, the facts 2016. The definitive overview of payment industry fraud*. London: Financial Fraud Action UK. Retrieved from https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/Fraud-the-Facts-A5-final.pdf.

Gartner, R. (1993). Methodological issues in cross-cultural large-survey research on violence. *Violence and Victims, 8*(3), 199.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*(1), 13–20.

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, IL: The University of Chicago Press.

Harrell, E., & Langton, L. (2013). *Victims of identity theft, 2012*. Retrieved from Washington DC.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1–25.

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice, 29*(4), 420–436.

Hough, M., & Maxfield, M. (2007). *Surveying crime in the 21st century: Commemorating the 25th anniversary of the British crime survey*. Monsey, NY: Criminal Justice Press.

Hough, M., Maxfield, M., Morris, B., & Simmons, J. (2007). British crime survey after 25 years. In J. Hough & M. Maxfield (Eds.), *Surveying crime in the 21st century: Commemorating the 25th anniversary of the British crime survey* (Vol. 22, pp. 7–32). Monsey, NY: Criminal Justice Press.

Internet World Stats. (2017). Internet World Stats. Retrieved from http://www.internetworldstats.com/.

ITRC. (2014). *Identity theft: The aftermath 2013*.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993.
Jewkes, Y., & Yar, M. (Eds.). (2010). *Handbook of internet crime*. Cullompton, UK: Willan Publishing.
Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2013). Online harassment in context: Trends from three Youth Internet Safety Surveys (2000, 2005, 2010). *Psychology of Violence, 3*(1), 53.
Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017, June 19–20, 2017). *Towards the normalization of crime victimization. A routine activities analysis of cybercrime in Europe.* In Paper presented at the international conference on cyber situational awareness, data analytics and assessment (CyberSA 2017), London, UK.
Kanich, C., Chachra, N., McCoy, D., Grier, C., Wang, D., Motoyama, M., Levchenko, K., Savage, S., & Voelker, G. M. (2011). No plan survives contact: Experience with cybercrime measurement. In Proc. of 4th USENIX CSET.
Karstedt, S. (2001). Comparing cultures, comparing crime: Challenges, prospects and problems for a global criminology. *Crime, Law and Social Change, 36*(3), 285–308.
Kerstens, J., & Veenstra, S. (2015). Cyber bullying in the Netherlands: A criminological perspective. *International Journal of Cyber Criminology, 9*(2), 144.
Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. American Psychological Association.
Leukfeldt, R. (Ed.). (2017). *Research agenda the human factor in cybercrime and cybersecurity*. The Hague: Eleven International Publishing.
Lynch, J. P. (2006). Problems and promise of victimization surveys for cross-national research. *Crime and Justice, 34*(1), 229–287.
Lynch, J. P. (2014). The evolving role of self-report surveys of criminal victimization in a system of statistics on crime and the administration of justice. *Statistical Journal of the IAOS, 30*(3), 165–169.
Maxfield, M., Hough, M., & Mayhew, P. (2007). Surveying crime in the 21st century: Summary and recommendations. In J. Hough & M. Maxfield (Eds.), *Surveying crime in the 21st century: Commemorating the 25th anniversary of the British crime survey* (Vol. 22, pp. 303–316). Monsey, NY: Criminal Justice Press.
Messner, S. F., & Zimmerman, G. M. (2014). Understanding cross-national variation. In *Encyclopedia of criminology and criminal justice* (pp. 5345–55). Berlin: Springer.
Milletary, J., & Center, C. C. (2005). Technical trends in phishing attacks. Retrieved December 1, 2007, 3.3.
Moons, E. (2013). Three percent of online buyers and sellers victims of fraud. *Web magazine*. Retrieved from http://www.cbs.nl/en-GB/menu/themas/veiligheid-recht/publicaties/artikelen/archief/2013/2013-3921-wm.htm.
Nansel, T. R., Overpeck, M. D., Haynie, D. L., Ruan, W. J., & Scheidt, P. C. (2003). Relationships between bullying and violence among US youth. *Archives of Pediatrics and Adolescent Medicine, 157*(4), 348–353.
Näsi, M., Aaltonen, M., & Kivivuori, J. (2016). Youth hate crime offending: the role of strain, social control and self-control theories. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 17*(2), 177–184.
National Fraud & Cyber Reporting Centre. (2016). Types of fraud. Retrieved from http://www.actionfraud.police.uk/fraud-az-online-fraud.
Newman, G. R. (2009). Cybercrime. Handbook on crime and deviance. In M. D. Krohn, A. J. Lizotte, & G. P. Hall (Eds.) (pp. 551–584). New York: Springer.
Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*. Retrieved from http://www.cybercrimejournal.com/ngo2011ijcc.pdf.
Office for National Statistics (ONS). (2015). *CSEW Fraud and cyber-crime development: Field trial*. London. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/methodologies/crimeandjusticemethodology#methodological-notes.
Office for National Statistics (ONS). (2017). *Crime in England and Wales, year ending September 2016*. London: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016. Retrieved from http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/period-ending-march-2013/stb-crime–period-ending-march-2013.html.
Powers, R. A. (2015). National crime victimization survey. In *The encyclopedia of crime and punishment*. New York: Wiley.
Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267–296. https://doi.org/10.1177/0022427810365903.
Rand, M. R. (2007). The national crime victimization survey at 34: looking back and looking ahead. In J. Hough & M. Maxfield (Eds.), *Surveying crime in the 21st century: Commemorating the 25th anniversary of the British crime survey* (Vol. 22, pp. 125–144). Monsey, NY: Criminal Justice Press.
Reep, C. (2013a). *Responsgedrag bij de Veiligheidsmonitor 2012. Onderzoek naar responsgedrag en selectiviteit bij inzet van internet en papier (Only available in Dutch)*. Retrieved from Heerlen, Nl: https://www.cbs.nl/-/media/_pdf/2016/46/slachtoffer-geweest.pdf.
Reep, C. (2013b). *Responsgedrag bij de Veiligheidsmonitor (in Dutch) (Response Behavior in the Safety Monitor)*. Retrieved from Heerlen, Nl: https://www.cbs.nl/nl-nl/achtergrond/2017/15/responsgedrag-bij-de-veiligheidsmonitor.
Reep, C. (2014). *Slachtoffer geweest? Antwoorden uit de Veiligheidsmonitor vergeleken met politieregister (only available in Dutch)*. Retrieved from Heerlen, Nl: https://www.cbs.nl/-/media/_pdf/2016/46/slachtoffer-geweest.pdf.
Reep, C. (2017). *Fraude met online handel. Antwoorden uit de Veiligheidsmonitor vergeleken met het politieregister (Online trading fraud. Information from the Security Monitor compared with the Police Register)*. Retrieved from Den Haag, Nl.
Reyns, B. W., & Henson, B. (2015). The thief with a thousand faces and the victim with none identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, 0306624X15572861.
Reyns, B. W., Henson, B., & Fisher, B. S. (2014). Cybercrime. In *The encyclopedia of theoretical criminology*. New York: Wiley.
Rieckmann, J., & Kraus, M. (2015). Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe. *DIW-Wochenbericht, 82*(12), 295–301.
Schneider, A. L. (1981). Methodological problems in victim surveys and their implications for research in victimology. *The Journal of Criminal Law and Criminology, 72*(2), 818–838.
Schouten, B., van den Brakel, J., Buelens, B., van der Laan, J., & Klausch, T. (2013). Disentangling mode-specific selection and measurement bias in social surveys. *Social Science Research, 42*(6), 1555–1570.
Skogan, W. G. (1986). Methodological issues in the study of victimization. In *From crime policy to victim policy* (pp. 80–116). Berlin: Springer.
Smith, A. (2006). *Crime statistics: An independent review (carried out for the Secretary of State for the Home Department)*. London, UK. Retrieved from http://webarchive.nationalarchives.gov.uk/20110218135832/http:/rds.homeoffice.gov.uk/rds/pdfs06/crime-statistics-independent-review-06.pdf.
STATEC. (2015). *Victimization and Safety in Luxembourg – Findings of the "Enquête sur la sécurité 2013".* Data were enriched with extra information provided by STATEC. Grand Duchy of Luxembourg: National Institute for statistics and economic studies. http://www.statistiques.public.lu/catalogue-publications/economie-statistiques/2015/85-2015.pdf.
Statistics Netherlands. (2013). *Veiligheidsmonitor 2012*. Voorburg, Nl.: Centraal Bureau voor de Statistiek. http://www.cbs.nl/NR/rdonlyres/F27A063A-EBF9-4A08-A8D7-12BC79DB7B47/0/2013Veiligheidsmonitor2012pub.pdf.
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.
Stol, W. (2012). Cyberspace and safety. In R. Leukfeldt & W. Stol (Eds.), *Cyber safety: An introduction* (pp. 19–30). The Hague: Eleven.
Stopbullying.gov. (2017). What is Cyberbullying. Retrieved from https://www.stopbullying.gov/cyberbullying/what-is-it/index.html.
Tourangeau, R., & McNeeley, M. E. (2003). *Measuring crime and crime victimization: Methodological issues.* In Paper presented at the measurement problems in criminal research: Workshop summary, Washington, DC.
Tuli, K., & Juneja, N. (2015). Evolution of identity thefts and online frauds on internet. *International Journal of Advanced Research in Engineering and Applied Sciences*.
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.
van Wilsem, J. (2013a). 'Bought it, but never got it'. Assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168–178.
van Wilsem, J. (2013b). Hacking and harassment—do they have something in common? Comparing risk factors for online

victimization. *Journal of Contemporary Criminal Justice*. https://doi.org/10.1177/1043986213507402.
Wachs, S., Whittle, H., Hamilton-Giachritsis, C., Wolf, K., Vazsonyi, A., & Junger, M. (2017). Correlates of mono-and dual-victims of cybergrooming and cyberbullying: evidence from four countries. *CyberPsychology, Behavior, and Social Networking*.
Wall, D. S. (2005). The Internet as a Conduit for Criminal Activity. In A. Pattavina (Ed.), *Information technology and the criminal justice system* (pp. 77–98). Thousand Oaks, CA: Sage.
Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge, UK: Polity Press.
Westerberg, S. (2017). [Online banking fraud and its prevention (personal communication)].
Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking, 15*(3), 181–183.
Wittebrood, K., & Junger, M. (2002). Trends in violent crime: a comparison between police statistics and victimization surveys. *Social Indicators Research, 59*(2), 153–173.
Wortley, R., & Mazerolle, L. (Eds.). (2008). *Environmental criminology and crime analysis*. London: Willan.