THE ROUTLEDGE INTERNATIONAL HANDBOOK OF ONLINE DEVIANCE

Edited by
Roderick S. Graham
Stephan G. Humer
Claire Seungeun Lee
Veronika Nagy

First published 2025

ISBN: 978-1-032-23447-2 (hbk)
ISBN: 978-1-032-23455-7 (pbk)
ISBN: 978-1-003-27767-5 (ebk)

2

MEASURING CYBERCRIME AND CYBERDEVIANCE IN SURVEYS

David Buil-Gil, Nicolas Trajtenberg and Marcelo F. Aebi

DOI: 10.4324/9781003277675-4

The funder of the Open Access version of this chapter is University of Lausanne.

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

2

MEASURING CYBERCRIME AND CYBERDEVIANCE IN SURVEYS

David Buil-Gil, Nicolas Trajtenberg and Marcelo F. Aebi

Introduction

Crime researchers have been preoccupied with the accuracy of crime measures at least since the early 19th century. As soon as the first national court statistics were published in France, Alphonse de Candolle (1830 [1987], 1832 [1987]) pointed out that they were likely affected by a variety of factors external to crime events, including whether incidents are identified by someone, if the person responsible is identified and if the court has enough evidence to convict the offender. Since then, many have studied the extent to which crime estimates recorded from different data sources accurately reflect the volume and nature of crime in society (Biderman & Reiss, 1967; Coleman & Moynihan, 1996; Skogan, 1977). Currently, the development of digital technologies is leading researchers and practitioners worldwide to recognize that measuring cybercrime and cyberdeviance is even more challenging than measuring more traditional forms of criminal and deviant behavior (Aebi et al., 2022; Caneppele & Aebi, 2019; Decker, 2020; Furnell et al., 2015). For instance, using data from the Crime Survey for England and Wales 2019–2020, the UK Office for National Statistics (2021) estimated that while 49% of violence, 45% of robbery, 37% of theft and 33% of damage incidents are reported to the police, public authorities are only informed of 13% of cyber-enabled frauds and 4% of computer misuse incidents (including computer viruses and unauthorized access to personal information). This chapter addresses the measurement of cybercrime with a focus on estimates obtained from surveys. It describes, categorizes and compares the measures of cybercrime and cyberdeviance included in the main national crime surveys, and discusses the opportunities and limitations of these measures to generate accurate estimates to study the prevalence, incidence, distribution and nature of cybercriminal and cyberdeviant behavior.

The chapter builds upon the comprehensive conceptualization of cybercrime presented by McGuire and Dowling (2013), which is used as a primary criterion for cybercrime counting in the UK and other countries. According to them, cybercrime can be defined as a set of offences that are dependent on or enabled by computers, computer networks or other forms of information and communication technologies. Policy documents distinguish cyber-dependent crimes (i.e., offenses that can only be committed through digital systems,

DOI: 10.4324/9781003277675-4

which mainly include malware, hacking and denial of service attacks) from cyber-enabled crimes (i.e., traditional crimes which have increased in scale or reach due to the use of digital technologies, including cyber-enabled fraud as well as other cyber-enabled predatory offences and crimes against individuals). This definition is nonetheless restricted to those behaviors categorized as 'criminal' by the criminal law, thus excluding other forms of online deviant behavior with harmful consequences (Graham & Smith, 2020). Although the distinction between 'cybercrime' and 'cyberdeviance' is not always clear-cut (Cioban et al., 2021), most national surveys have tended to focus on criminal behaviors. Less attention has been given to cyberdeviant behavior such as cyber-enabled bullying, online harassment, online hate speech or online gambling (Castaño-Pulgarín et al., 2021; Chun et al., 2020; Lee, 2018). In addition, researchers are warning about the challenges posed by hybrid crimes, which are crimes that take place both online and offline; for example, when an adolescent is bullied at school and on social media (Aebi, 2022).

Both cyber-enabled and cyber-dependent crime figures have seen rapid increases at least since the early 2000s (EUROPOL, 2021) and spiked in the aftermath of the COVID-19 pandemic (Buil-Gil et al., 2021a). Estimates from the International Telecommunication Union (2021), the United Nations' specialized agency for information and communication technologies, show that 4.9 billion people (63% of the world's population) had access to the internet in 2021, compared to 1 billion in 2005. This increase seems mainly related to the exponential growth of smartphones, which multiplied the number of potential offenders and victims of cybercrime. With the increase in cybercrime and cyberdeviance, it becomes urgent to adequately understand its volume, characteristics and distribution to study its causes and consequences, and in turn design and evaluate prevention strategies. There is a growing need for reliable data on cybercrime offending and victimization. While police-recorded cybercrime data is regularly criticized for failing to capture the vast majority of cybercrime incidents (Caneppele & Aebi, 2019; Correia, 2022; Decker, 2020), crime surveys probe representative population samples about their experiences with crime and deviance and are often used to obtain estimates of cybercrime prevalence and incidence (Furnell et al., 2015; Reep-van der Bergh & Junger, 2018) and to study the precursors of victimization (Holt & Bossler, 2008; Leukfeldt & Yar, 2016) and offending (McGuire & Dowling, 2013; Weulen Kranenbarg, 2022). Survey data offer apparent advantages over more traditional sources of cybercrime and cyberdeviance data, but surveys are not free from limitations, and temporal and cross-national comparisons are not always possible.

Data sources to measure cybercrime and cyberdeviance

A variety of data sources have traditionally been used to measure crime. Crime researchers, police forces and policy makers use data recorded from criminal justice statistics, calls for police services, ambulance dispatches and victimization and self-report surveys to study the nature and volume of crime (Aebi et al., 2002; Bottoms et al., 1987; Huey & Buil-Gil, 2024). While all these data sources offer important information about crime, none of them allow for error-free crime measurements. Different data sources are affected by different kinds of measurement error and fail to capture many crimes that happen in society. To mention some examples, police records do not document incidents that are not reported to the police or those that the police deem not serious enough; health emergency services' statistics only measure incidents that result in physical injuries; victim surveys fail to capture so-called 'victimless' crimes (e.g., drug offenses, tax fraud) and vital offenses; and

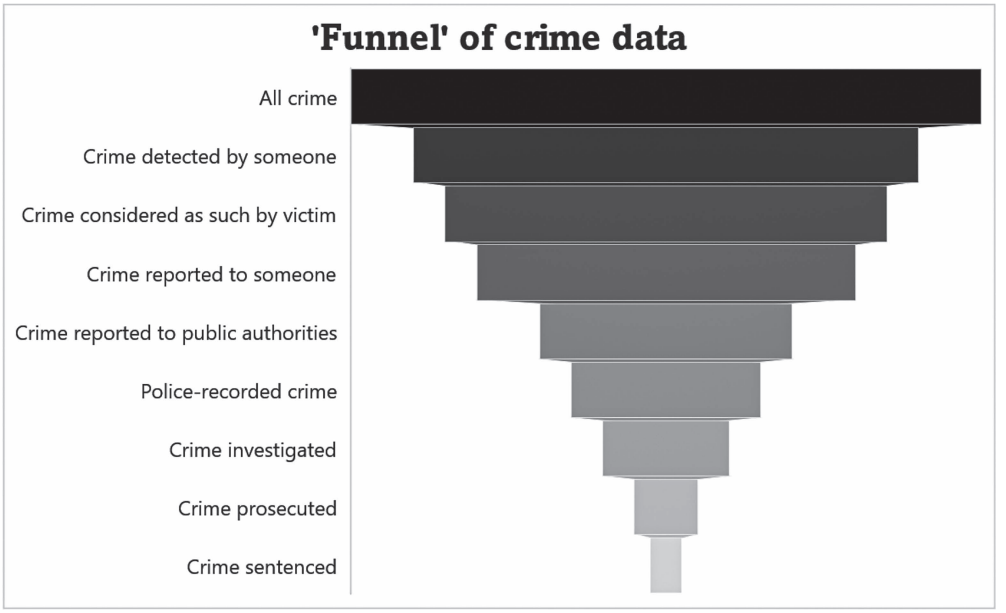

Figure 2.1 'Funnel' of crime data

self-report studies are often limited to delinquent and deviant behavior in adolescents. As a consequence, estimates of crime obtained from different sources often show remarkably different trends (Lynch & Addington, 2006) and spatial distributions (Buil-Gil et al., 2022).

Crime data users often prioritize data sources that are closer to the crime event in terms of legal procedure, as crime records shrink through the stages of the criminal justice system process. This is often referred to as the 'Sellin's dictum'—"the value of a crime rate for index purposes decreases as the distance from the crime itself in terms of procedure increases" (Sellin, 1931, p. 346). The dwindling of crime records through the legal procedure stages is commonly visualized as the 'funnel' (Figure 2.1) or the 'sieve' of crime statistics (Chopin & Aebi, 2020). In this regard, crime surveys, which probe representative population samples about their direct experiences with crime, are typically assumed to allow for more valid estimates of 'all crime' than official sources of crime data.

Similarly, a variety of sources of data have been used in research and practice to measure and study cybercrime. Public administrations increasingly publish aggregated statistics of known online crimes. Some of the most widely known examples of open-access cybercrime data repositories and reports are the annual report of the FBI's Internet Crime Complaint Center IC3 in the US,[1] the interactive data dashboard of Action Fraud in the UK,[2] the annual Internet Organized Crime Threat Assessment of EUROPOL's European Cybercrime Centre EC3[3] and the Australian Cyber Security Centre Annual Cyber Threat Report.[4] The European Sourcebook of Crime and Criminal Justice Statistics publishes cross-national records of cyber-enabled fraud, and for some countries cyber-dependent crime, recorded each year in official statistics and national surveys in European countries (Aebi et al., 2021). The non-governmental organization Private Rights Clearinghouse provides detailed descriptions of data breaches sentenced in US courts.[5]

Alongside official cybercrime records, private organizations, mainly technology and cybersecurity software companies, are increasingly developing their own estimates of cybercrime based on data sources often unavailable to public administrations (Furnell et al., 2015). McAfee, one of the largest security software companies, publishes data aggregates about ongoing and emerging ransomware threats identified by the company in an interactive data dashboard called MVISION Insights.[6] F-Secure, a cybersecurity company with headquarters in Finland, set up a network of honeypots to identify malware trends and publishes aggregated data in its annual Attack Landscape report.[7] F-Secure also publishes data recorded from surveys with IT decision makers in the private sector. A network of honeypots is also used by Broadcom, an American software company, to record data and publish descriptive statistics about cyber-dependent threats.[8] Broadcom also utilizes email processing technology to identify and share data about spam, phishing and email malware trends. All these sources of data published by private initiatives provide highly important information about ongoing and emerging cyber-dependent and in some cases cyber-enabled crimes, and can serve to identify changes in trends. Nonetheless, private organizations seldomly publish microdata about specific incidents, and there is often a lack of transparency about methodologies used to estimate and forecast crime threats, which makes this data of very limited use for the more advanced statistical techniques needed to understand the nature of cybercrime. This opacity regarding data sharing practices in the private sector is most probably due to the interest of businesses in protecting highly competitive market shares against organizational competitors, and perhaps due to data privacy implications (Young et al., 2019). Academic organizations are also developing similar initiatives and sharing the data through user agreements and online requests. As an example, the Cambridge Cybercrime Centre records data about underground and extremist online forums, defaced websites, investment scams, denial of service attacks, phishing, spam and malware.[9] The Korea University's Hacking and Countermeasure Research Lab records data about malware, hacking and attacks against Internet of Things devices.[10]

There is also a growth of digital platforms that record crowdsourced data about cybercrime and cyberdeviance. A variety of platforms exist that allow individuals to report details of individual incidents, thus allowing others to protect themselves against similar threats. 'Ransomwhere' is an open code website that allows victims of ransomware to share details about the incident, including free text descriptions of each crime and the Bitcoin address where the ransom was requested or paid.[11] Bitcoin Abuse offers similar functionalities.[12] These data sources are open-source, easily accessible and sometimes record information over long periods of time (Gundur et al., 2021). The main issue with crowdsourced datasets of incidents is that these are recorded from non-probability samples, and the mode of production of these data may contribute to severe self-selection biases and overrepresentation of so-called 'super-contributors' (Solymosi & Bowers, 2018). Unsolicited online data recorded from encrypted 'darknets' is also used to analyze drug markets (Enghoff & Aldridge, 2019; Paquet-Clouston et al., 2018), and social media data to analyze cyber-enabled hate crime (Burnap & Williams, 2016), but may be of limited use to analyze most other types of cybercrime.

While many different sources of cybercrime data are becoming available and used in research and practice to understand online crime and deviance, many argue that surveys are today the most fit-for-purpose tool to study the volume, distribution and characteristics of cybercrime and cyberdeviance.

Crime surveys

Since the 1930s, social surveys have been used to measure a variety of aspects of people's social and political lives, including voting intentions, opinion polls, market preferences, trust in government agencies and social attitudes. A door-to-door inquiry about burglaries conducted in Aarhus, Denmark, in 1730, is often considered a predecessor of contemporary victimization surveys (Wolf & Hauge, 1975; cited in Sparks, 1981). In 1945, the Gallup Poll included measures of personal crime victimization in the last 12 months, including theft, burglary, robbery, assault, trespassing and fraud, in a social survey conducted in Finland (Aebi & Linde, 2014). Nonetheless, the first survey specifically designed to measure crime and victimization was sponsored by the US President's Commission on Law Enforcement and Administration of Justice in 1965 (Ennis, 1967). The 'Attitudes and Experience Questionnaire: Victimization Study' asked a sample of US respondents about their experiences with crime, namely with burglary, car theft, robbery, larceny, malicious mischief or arson, counterfeiting, rape, other sex crimes, assault, threat, auto offenses, intrafamilial violence, consumer fraud, building violations, bribing, homicide and kidnapping. It also included follow-up measures about details of the victims and offender, crime reporting to the police, consequences of crime and perceptions about the police.

Since then, victimization surveys have become a common instrument at the national (Aebi & Linde, 2014), local (Maguire, 1997) and international levels (van Dijk et al., 2007). Some of the main national victimization surveys are the US National Crime Victimization Survey (NCVS), the Crime Survey for England and Wales (CSEW; formerly known as British Crime Survey), the Mexico National Survey on Victimization and Perception of Public Safety (ENVIPE), the Netherlands Safety Monitor and the Chilean National Urban Survey on Citizen Security (ENUSC). The International Crime Victims Survey (ICVS) recorded data across many countries worldwide in 1989, 1992, 1996, 2000 and 2004/2005.[13] Victimization surveys have been key for the advancement of explanations of victimization (Hindelang et al., 1978; Pratt et al., 2010; Tilley & Tseloni, 2016) and revictimization risk (Farrell & Pease, 1993; Osborn & Tseloni, 1998), fear of crime (Brunton-Smith & Sturgis, 2011), crime reporting (Kemp et al., 2023; Tarling & Morris, 2010) and the geographic distribution of crime in communities (Cernat et al., 2022; Osborn et al., 1992; Sampson & Groves, 1989). Most victimization surveys only began including measures of cybercrime in the late 2010s (Reep-van der Bergh & Junger, 2018).

Aside from victimization surveys, self-reported delinquency studies have also been instrumental for the study of crime and deviance. These are surveys in which respondents are asked about instances in which they have been actively involved in crime or deviant behavior (Hindelang et al., 1981; Junger-Tas & Marshall, 1999). Self-report offending studies have been key for measuring juvenile delinquency and developing and testing some of the main theories of criminal and deviant behavior. Wallerstein and Wyle (1947) surveyed nearly 1,700 adults in New York and found that most respondents had committed at least one offense in the last year, but these were mostly trivial incidents. Short and Nye (1958) found little relationship between socio-economic status and self-reported delinquency. Gold (1970) found that most self-reported youth delinquent behavior was committed with other peers. Hirschi (1969) used cross-sectional self-report offending surveys to study the link between juvenile crime and social control. Longitudinal self-report surveys have also gained traction in criminological research. A key example is the US National Youth Survey, which started in 1976 following 1,725 adolescents aged 11 to 17 and became the National

Youth Survey Family Study in 2000 (Elliott et al., 1985). Lauritsen (1993) analyzed this survey and found that juvenile delinquency is strongly concentrated in a very small proportion of the households sampled. Another noteworthy example of cross-national self-report delinquency survey is the International Self-Report Delinquency Study, which has been conducted four times since the beginning of the 1990s (Junger-Tas, 2010). Self-report offending surveys have also been utilized to study active involvement in cybercrime (e.g., Allen et al., 2005; Weulen Kranenbarg et al., 2019), as will be described in more detail. On the contrary, research has shown that their main limitation is that their validity is doubtful with adult populations unless they are somehow "captive", as is the case with inmates or drug addicts enrolled in heroin prescription programs (Aebi, 2006).

The next two sections describe, categorize and compare the measures of cybercrime and cyberdeviance included in some of the main national victimization and self-report offending surveys, and discuss the opportunities and limitations of these measures to generate accurate estimates to study the nature of cybercrime and cyberdeviance.

Measuring cybercrime victimization using surveys

Individual and household crime surveys

To better understand the measurement of cybercrime in victimization surveys, we have selected a sample of population surveys and extracted information from them using a standardized form. More specifically, after consulting with colleagues and experts in victimization survey data, we have selected a set of surveys that meet the following criteria:

(a) national victimization surveys, thus excluding surveys with a local and regional focus and general social surveys;
(b) surveys that record random samples representative of the national population, thus excluding non-probability samples;
(c) surveys that recorded data annually or biannually, thus excluding surveys undertaken only at one point in time;
(d) surveys that provide meta-data and questionnaire documentation in either English, Spanish, Dutch or French (languages spoken by authors or collaborators); and
(e) where possible, at least one national crime survey on each continent.

The sample, presented in Table 2.1, does not seek to be exhaustive nor representative of national victimization surveys worldwide. It includes the NCVS and the CSEW, which are by far the most quoted surveys in the scientific literature, as well as the national crime surveys in the Netherlands, Mexico, Chile, South Africa and New Zealand. Our review does not include the Korean Crime Victims Survey—the only Asian survey that meets the criteria presented earlier[14]—because we did not obtain access to its methodological documentation in English, Spanish, Dutch or French. We also note that some of the countries included in our sample undertake other surveys that may include indicators of cybercrime and cyberdeviance (e.g., CSEW questionnaire for persons aged under 16, the Chilean Survey of Local Authorities, New Zealand Crime and Safety Survey), but the focus of our analysis is the main crime survey in each country.

For each survey, we record information about whether and how they record information about victimization related to different types of cybercrime. We summarize this information in Table 2.2. All surveys measure both the prevalence and incidence of

Table 2.1 National crime surveys of individuals or households included in analysis

Name	*Name in original language*	*Acronym*	*Country*	*Frequency*	*Round analyzed*	*Sample*
Crime Survey for England and Wales		CSEW	England and Wales	Annual	2019–20	33,734 households (aged 16 or more)
Safety Monitor	'Veiligheidsmonitor'	VM	Netherlands	Every 2 years	2019	135,000 adults (aged 15 or more)
National Crime Victimization Survey (Identity Theft Supplement)		NCVS-ITS	USA	Every 2 years	2018	102,400 respondents (aged 16 or more)
National Survey of Victimization and Perception of Public Safety	'Encuesta Nacional de Victimización y Percepción de Seguridad Pública'	ENVIPE	Mexico	Annual	2021	102,297 households (aged 18 or more)
National Urban Survey on Citizen Security	'Encuesta Nacional Urbana de Seguridad Ciudadana'	ENUSC	Chile	Annual	2021	22,180 households (aged 15 or more)
Victims of Crime Survey		VOCS	South Africa	Annual	2017	33,000 households (aged 16 or more)
New Zealand Crime and Victims Survey		NZCVS	New Zealand	Annual	2021	6,244 residents (aged 15 or more)

Table 2.2 Measures of cybercrime victimization included in sampled national crime surveys of individuals or households*

	Cyber-dependent crime			*Cyber-enabled financial crime*				*Cyber-enabled personal crime/ deviance*	
	Malware	*Hacking*	*Spam/phishing*	*Online shopping fraud*	*Online banking fraud*	*ID fraud*	*Advance fee fraud*	*Hate crime*	*Online harassment*
CSEW	"computer or other internet-enabled device been infected or interfered with, for example by a virus"	"stolen personal information or details held on computer or in online accounts (e.g. email, social media)"		"anyone tricked or deceived you out of money or goods, in person, by telephone or on-line"	"personal information or account details used to obtain money, or buy goods or services without your permission or knowledge"	As a result of crime . . . "personal information or details accessed or used without permission"	Was crime related to . . . "chance to make investment with guaranteed high return"	For crimes registered . . . "incident motivated by offender's attitude towards . . . (race, religion, sex, disability, etc.)"	"anyone put personal, obscene or threatening information about you on internet on more than one occasion and which caused you fear, alarm or distress"

(*Continued*)

Table 2.2 (Continued)

	Cyber-dependent crime			*Cyber-enabled financial crime*				*Cyber-enabled personal crime/ deviance*	
	Malware	*Hacking*	*Spam/phishing*	*Online shopping fraud*	*Online banking fraud*	*ID fraud*	*Advance fee fraud*	*Hate crime*	*Online harassment*
VM		"hacked into or logged into computer, email account, website, or profile site (e.g., Facebook, Twitter)"		"been cheated when buying or selling goods or services, e.g., purchased goods were not delivered"	"identity fraud. This involves using someone's personal data for financial gain without permission (e.g., withdrawing money, taking loans)"				"bullying, stalking, blackmail or threats" If yes, was it: "embarrassing or hurtful website or profile about you", "messages under your name on Internet forum or social media", "extorted, blackmailed"
NCVS-ITS		If personal information misused by	If personal information misused by		"someone, without your permission,	"misuse of account such as telephone, cable, gas			

(*Continued*)

Table 2.2 (Continued)

Cyber-dependent crime			*Cyber-enabled financial crime*				*Cyber-enabled personal crime/ deviance*	
Malware	*Hacking*	*Spam/phishing*	*Online shopping fraud*	*Online banking fraud*	*ID fraud*	*Advance fee fraud*	*Hate crime*	*Online harassment*
	someone else . . . was it accessed "Someone hacked into my computer"	someone . . . "I responded to scam email/phone call"		used or attempted to use your existing checking or savings account, including any debit or ATM cards"	or electric accounts, online payment account, insurance, entertainment account"; "other fraudulent purpose, such as filing fraudulent tax return, getting medical care, applying for a job or benefits"			

(*Continued*)

Table 2.2 (Continued)

	Cyber-dependent crime			*Cyber-enabled financial crime*				*Cyber-enabled personal crime/ deviance*	
	Malware	*Hacking*	*Spam/phishing*	*Online shopping fraud*	*Online banking fraud*	*ID fraud*	*Advance fee fraud*	*Hate crime*	*Online harassment*
ENVIPE				"paid money for product or service that you never received (consumer fraud)"	"someone used your checkbook, credit card or bank account without your consent to make payments or obtain money from account (bank fraud) or gave you counterfeit cash"				
ENUSC	"remotely destroying your hard drive or content in computer"			"fraud while buying online"	"forged your identify to access your bank account or credit card"	"forged your identity in email accounts or social media"		For crimes registered . . . "believe it was motivated by your personal character-istics or believes? Nationality, sex . . ."	"threats through internet or email"; "harassment trough inappropriate or obscene messages, communications, unrequested images, or sexual requests"
VOCS				"Consumer fraud" within last 5 years and last 12 months					

(*Continued*)

Table 2.2 (Continued)

	Cyber-dependent crime			*Cyber-enabled financial crime*				*Cyber-enabled personal crime/ deviance*	
	Malware	*Hacking*	*Spam/phishing*	*Online shopping fraud*	*Online banking fraud*	*ID fraud*	*Advance fee fraud*	*Hate crime*	*Online harassment*
NZCVS	"computer or Internet-enabled device been infected or interfered with, for example by a virus or someone accessing without permissions"			"tricked or deceived you, in order to obtain money, goods or a service"	"used or attempted to use bank card, credit card, cheque or other document without your permission, to obtain money, or buy goods or services"				

*The wording of some questions has been shortened

victimization and include survey weights to allow estimates of crime for the target population. All these surveys also included measures of crime reporting, hence enabling analyzing the proportion of incidents that are known to public authorities each year (van de Weijer et al., 2019).

As can be seen in Table 2.2, the way in which cybercrime is measured varies extensively from survey to survey. With regard to cyber-dependent crime, while three surveys included measures that may in some cases refer to malware victimization, the CSEW is the only to include a question specifically designed to measure this type of crime. The NZCVS, for example, probes respondents about instances where computer devices are infected or interfered with by a virus or someone else, hence referring to either cases of malware or hacking. Similarly, the ENUSC probes about the remote destruction of hard drive or content in computer, which may also refer to both malware and hacking victimization. With the exception of ENVIPE and VOCS, all other surveys include indicators that can be used to measure at least one type of cyber-dependent crime. The only survey to include an indicator of phishing victimization is the NCVS-ITS. Yet this question is only asked to those who had previously answered that their information had been misused by someone else. Some surveys also include follow-up questions for each crime reported, such as the methods used by offenders to access the data, devices affected and changes in behavior and prevention measures taken after the incident, in the CSEW.

The measurement of cyber-enabled crime also varies across crime surveys. We recorded measures of cyber-enabled financial crime (i.e., those that target a financial gain) and cyber-enabled personal crime (i.e., those that seek to harm someone). With the exception of the NCVS-ITS, all other surveys included at least one measure that may in some cases refer to online shopping fraud. However, the only survey that measures specifically *online* shopping fraud is the ENUSC. The CSEW question, for example, includes both incidents committed via telephone and online. The VM, ENVIPE and NZCVS include all forms of shopping fraud in the same question, and the VOCS measure refers to all kinds of consumer fraud, which may also refer to online banking fraud and ID fraud. It is true, however, that most of these questionnaires include follow-up measures for each crime reported, which allows distinguishing cyber-enabled frauds from those committed offline and via telephone. The VOCS, for instance, asks respondents if the consumer fraud refers to "banking fraud (e.g., internet)", "identity fraud", "illegal duplication of bankcard/ATM fraud", amongst other options. Likewise, the ENVIPE asks whether frauds took place online.

All surveys include at least one measure of either online banking fraud or ID fraud, but item wording varies extensively across surveys, and in some cases, it is not clear if the measure refers to the illegal access and use of personal information to access finances through online banking (i.e., online banking fraud) or for other purposes. The VM, for example, probes about the use of personal data for financial gain, "withdrawing money, taking loans, etc.", and the ENVIPE asks about the use of data to "make payments or obtain money from your account (bank fraud) or gave you counterfeit cash". Even though some government agencies such as the UK Action Fraud recommend these to be treated as separate crime types, this distinction is not clearly defined in any of the surveys explored. The CSEW is the only survey to include a measure of advance fee fraud, which can be cyber-enabled in some cases, but this measure is included as a follow-up question for victims only.

With regard to cyber-enabled personal crime, only two surveys, the CSEW and the ENUSC, included a follow-up question to victims of crime to disentangle whether each crime was motivated by racial, religious, gender or other types of hatred. This measure is also included in the main questionnaire of the NCVS, but not in the Identity Theft Supplement. However, these indicators do not allow distinguishing cyber-enabled hate crime from traditional forms of hate crime. Analysts would need to first subset those crimes that took place on the internet, and then explore how many of those were motivated by hate towards certain population groups. The CSEW, VM and ENUSC also included measures of cyber-enabled harassment, though as can be seen in Table 2.2 the design and wording of these questions is remarkably different, hence making cross-national comparisons difficult. In Mexico, each year the National Survey on the Availability and Use of Information Technologies at Home (MOCIBA) also includes measures of cyber-harassment,[15] but these are not included in the ENVIPE. The ENVIPE includes measures of threats and extortion in general terms.

Most of these surveys also include a number of other key indicators. The VM measures how information was intercepted in the first place (e.g., email, internet, ATM), and the CSEW includes items to capture satisfaction with the police response. Questions about the harms of each crime are included in most surveys. The CSEW and ENUSC also include measures of perceptions about cybercrime trends and worry about cybercrime. The VOCS includes a set of questions about concerns about hate crime, fraud and identity document theft.

Business crime surveys

A first *International Commercial Crime Survey* was conducted in eight European countries in 1994 using a standardized questionnaire pilot-tested in four other countries, used later in several others and then adapted to focus on corruption, fraud and extortion before being used for a second wave of the survey—renamed the *International Crime Business Survey*—in nine Central-East European cities in 2000 (Alvazzi del Frate, 2004). This international effort was discontinued, but its results, combined with those obtained in countries that conduct national crime business surveys, highlight the need for such studies, which must be conducted using questionnaires that include cybercrimes at a time when a substantial part of economic transactions take place online (Dupont, 2019; Junger et al., 2020). Some estimate that the financial losses suffered by businesses due to cybercrime may greatly exceed that suffered by individuals. For instance, in 2017, the UK Annual Fraud Indicator estimated that frauds were responsible for £140 billion losses for the private sector, £40 billion losses for the public sector and £6.8 billion losses for individuals (Crowe, 2017). Taking into account the magnitude of these losses and knowing the limitations of official crime statistics (Kemp et al., 2023), several national governments have launched recurring business cybercrime surveys. In this chapter, we analyze three that have been conducted at least two times and have been used in research and policy making (Buil-Gil et al., 2021b; Rantala, 2008): the UK Cybersecurity Breaches Survey, the US National Computer Security Survey and the Canadian Survey of Cyber Security and Cybercrime. We exclude surveys undertaken by cybersecurity businesses and consultancy companies and surveys undertaken only at one point in time (e.g., in 2021, a Eurobarometer included measures of corporate cybercrime victimization across 27 European Union countries[16]). Details about the three surveys included for analysis are presented in Table 2.3.

Table 2.3 National crime surveys of businesses included in analysis

Name	*Acronym*	*Country*	*Frequency*	*Round analyzed*	*Sample*
Cyber Security Breaches Survey	CSBS	UK	Annual	2021	1,419 businesses, 487 charities and 378 education institutions
National Computer Security Survey	NCSS	USA	2001 and 2005	2005	7,818 businesses
Canadian Survey of Cyber Security and Cybercrime	CSCSC	Canada	Every 2 years	2021	12,158 businesses

While these three surveys are not representative of how business cybercrime victimization is measured elsewhere, a comparison of their questionnaires may reveal inconsistencies in the way business cybercrime victimization is measured in these three countries, and potentially also elsewhere. Australia, for example, includes measures of business cybercrime victimization in its Small Business Survey, and in Mexico the National Survey of Victimization of Businesses (ENVE) also asks victimized companies whether each incident took place offline or online (e.g., in the case of fraud and extortion). In order to keep our search manageable, we did not include in our analysis other business victimization surveys in UK, USA and Canada that may also include measures of cybercrime, such as the UK Cyber Security Longitudinal Survey.[17]

Table 2.4 presents the item wording used in these three surveys to measure five types of cyber-dependent crime (i.e., malware, hacking, Denial of Service (DoS), website defacement and spam/phishing), two types of cyber-enabled crime (i.e., fraud and identity theft) as well as unauthorized access to data by someone inside or outside the organization. The crime types included in business surveys are quite different from those included in household surveys, mirroring the variations and nuances in the types of crimes suffered by organizations and individuals. For instance, questions about website defacements and unauthorized access to data are not included in household surveys, and those on fraud are more generic in business surveys than in household surveys.

In terms of the design of these surveys, while the CSBS and NCSS directly pose a question for each type of crime, the CSCSC has a generic filter question about whether the company suffered any kind of cybercrime attack that had an impact on the business and, if that is the case, it poses follow-up questions for each type of cybercrime. Specifically, the CSCSC asks all businesses in the sample whether they suffered concrete cybersecurity incidents that aimed to disrupt the business or web presence, steal personal information, steal money or demand a ransom, steal or manipulate intellectual property, access unauthorized areas, monitor business activity or any other motive. Only those businesses that answer affirmatively are then asked about the "method" to execute the attack—which more closely matches the crime definitions of the CSBS and NCSS. Thus, while the CSBS and NCSS ask about crime types, the CSCSC asks first about the motive of the incident and then about the

Table 2.4 Measures of cybercrime victimization included in national crime surveys of organizations*

	Cyber-dependent crime					*Cyber-enabled financial crime*		*Other*	
	Malware	*Hacking*	*DoS*	*Website defacement*	*Spam/ phishing*	*Fraud*	*Identity theft*	*Unauthorized access (internal)*	*Unauthorized access (external)*
CSBS	"Computers becoming infected with ransomware"; "with other malware (e.g viruses or spyware)"	"Hacking or attempted hacking of online bank accounts"	"Denial of service attacks, i.e. attacks that try to slow or take down website, applications or services"	"Takeovers or attempts to take over website, social media accounts or email accounts"	"Phishing attacks, i.e. staff receiving fraudulent emails or arriving at fraudulent websites"		"People impersonating organisation in emails or online"	"Unauthorised accessing of files or networks by staff, even if accidental"	"Unauthorised accessing of files or networks by people outside organisation"
NCSS	"intercept computer viruses before they could infect computer systems"; "detect viruses which infected computer systems"	"company detect any other computer security Incidents" If yes . . . "hacking"	"detect any incidents of denial of service (noticeable interruption of Internet connection or e-mail service)"		"company detect any other computer security Incidents" If yes . . . "phishing"	"someone inside or outside this company used a computer to commit fraud against this company"		"someone inside or outside company used a computer to obtain intellectual property from this company"; "someone inside or outside company used a computer to obtain personal or financial information from this company"	

(*Continued*)

Table 2.4 (Continued)

	Cyber-dependent crime					*Cyber-enabled financial crime*		*Other*	
	Malware	*Hacking*	*DoS*	*Website defacement*	*Spam/ phishing*	*Fraud*	*Identity theft*	*Unauthorized access (internal)*	*Unauthorized access (external)*
CSCSC	For crimes registered . . . "what the method . . .": "ransom-ware"; "other malicious software"	For crimes registered . . . "what the method . . .": "exploiting software, hardware or network vulner-abilities"; "hacking or password cracking"	For crimes registered . . . "what the method . . .": Denial of service or Distributed denial of service"	For crimes registered . . . "what the method . . .": "disruption or defacing of web presence"		For crimes registered . . . "what the method . . .": "scams or fraud"	For crimes registered . . . "what the method . . .": "identify theft"	For crimes registered . . . "what the method . . .": "abuse of access privileges by a current or former internal party"	

*The wording of some questions has been shortened

method. The combination of these two measures can then be used to estimate crime prevalence (Bilodeau et al., 2019). Looking more closely at the item wording, we also observe that while the CSCSC measures incidents that did have an impact on the business, the CSBS and NCSS also consider attempted attacks that were detected but did not have significant impacts.

In practice, there are relevant differences in the types of crimes included in the surveys as well as in most of their definitions. Regarding malware, the CSBS and CSCSC differentiate ransomware from other types of malware whilst the NCSS refers to computer viruses. The NCSS asks about hacking in general, the CSBS about hacking of bank accounts, and the CSBS about the exploitation of computer or network vulnerabilities and "hacking or password cracking". Measures of DoS exist in the three surveys, but the definitions provided in the CSBS and NCSS vary as the former describes attacks on websites, applications or services, while the latter refers to attacks targeting internet connection or e-mail services. The CSBS and the CSCSC measure website defacement, which is excluded from the NCSS, while the latter and the CSBS include phishing, which is excluded from the CSCSC. Identity theft is included as such in the CSCSC, whilst the CSBS refers to someone impersonating the organization online, and the NCSS excludes that cyber-offense. Another key difference between the household and business surveys studied here is that the former differentiate between different types of fraud, but the NCSS and the CSCSC refer to fraud in general terms.

Finally, all three surveys include measures of unauthorized access to files and data, but there are two important differences in the way it is measured. First, regarding the target of the intrusion, the CSBS refers to files or networks, the NCSS to either intellectual property or personal or financial information and the CSCSC to abuse of access privileges more generally. Second, regarding the person responsible for the unauthorized access, the CSBS differentiates internal from external threats (Williams et al., 2019), the NCSS includes both types of actors in the same question, and the CSCSC only refers to insiders. Both the NCSS and the CSCSC also include a follow-up question about whether the suspect is an insider or outsider.

Aside from the offenses included in Table 2.4, the CSBS also measures unauthorized listening of videos or messages, and the NCSS measures electronic vandalization or sabotage of computer systems as well as the use of the latter to commit embezzlement. All three surveys also include questions about the cybersecurity measures applied by the organization, cybersecurity priorities, investment in cybersecurity, online presence, crime reporting and consequences of each incident.

Measuring cybercrime offending and deviance through self-report delinquency studies

Self-report delinquency studies are the main alternative to measure the frequency, distribution and nature of cybercrime (e.g., Allen et al., 2005; Weulen Kranenbarg et al., 2019). As explained in the Introduction, research on the validity of self-reported delinquency studies has shown that they are mainly valid with adolescents. Here we include information about how some of the main extant self-report crime surveys measure cybercrime offending and deviance. We have purposively selected three of the main self-report crime surveys that are openly available, have been conducted at least twice and include clear questionnaire

Table 2.5 Self-report offending surveys included in analysis

Name	*Acronym*	*Country*	*Frequency*	*Round analyzed*	*Sample*
Offending, Crime and Justice Survey	OCJS	UK	Annual, 2003 to 2006	2006	5,354 respondents aged 10 to 29
Youth Delinquency Survey	YDS	Netherlands	Quinquennial	2015	1,471 respondents aged 12 to 23
International Self-Report Delinquency Study	ISRD4	Cross-national	1991/91, 2006/08, 2012/19, 2021/22	2021/22	Varies by country (respondents aged 13 to 17)

documentation. As in the previous sections, Table 2.5 summarizes the main characteristics of the surveys, while Table 2.6 presents the measures of cybercrime and cyberdeviance included in them.

Again, while these three surveys are not representative of how self-reported cybercrime offending is measured elsewhere, a comparison of their questionnaires discloses inconsistencies in the way active involvement in juvenile cybercrime and cyberdeviance is measured in three of the main self-report studies. Beyond these three surveys, the measurement of cybercrime offending is scarce and mostly confined to small and non-representative samples or case studies. There are, however, emerging initiatives to record data on self-reported cybercrime offending, such as Virginia Tech's Longitudinal Survey of Cybercriminology (Dearden & Parti, 2021).

One of the first nationally representative surveys to include measures of cybercrime offending and deviance was the OCJS, which was conducted between 2003 and 2006 in the UK (Allen et al., 2005). The survey included measures of cyber-dependent crimes such as malware, hacking and digital piracy, as well as cyber-enabled behaviors such as online harassment and online credit card fraud. This survey also asked respondents whether they had accessed deviant forums or websites (i.e., "visited a website that showed you how to commit a crime, or might have helped you commit a crime" and "visited a website that might be thought of as racist, either because you supported their views or because you were thinking of becoming a member") and whether they had bought stolen goods on the internet.

The YDS also includes measures of cybercrime offending (van der Laan et al., 2021). Its first two waves focused on a more limited set of online crime items such as digital piracy (i.e., downloading online material illegally), online threats/harassment and sending computer viruses; but the third wave extended the range of cyber-enabled offenses to hacking, DoS and online shopping fraud (Rokven et al., 2018). The YDS is also the only survey to include measures of identity theft ("impersonated somebody else on the internet") and distribution of online child sexual exploitation material ("distributed sexual material of minors through your smartphone or over the internet"), which has not been included in Table 2.6 due to space restrictions.

Table 2.6 Measures of cybercrime offending included in self-report crime surveys*

	Cyber-dependent crime				*Cyber-enabled financial crime*		*Cyber-enabled personal crime/ deviance*	
	Malware	*Hacking*	*DoS*	*Digital piracy*	*Online banking fraud*	*Online shopping fraud*	*Hate speech*	*Online harassment*
OCJS	"used internet to send viruses on purpose to other computers"	"used internet to hack intro other computers? by hacking we mean using a computer to illegally get access to another computer's files"		"used internet to download software, music or films that you knew to be pirated or unauthorized"	"bought anything over the internet using payment card or card details that did not belong to you, without the card owner's permission"			"sent email message to someone in order to harass, scare or threaten them"; "sent voice or text message on your phone . . ."
YDS	"intentionally sent out viruses through e-mail or over the internet"	"logged on to somebody else's computer, email or social media account without informed consent"; "changed someone's account password (computer or social media) to prohibit them from accessing"; "logged on onto somebody else's computer, email or social media account without informed consent, and manipulated or deleted information"	"tried to disrupt a website or email account by sending out large amounts of data"			"sold something through internet, but not sending out goods after receiving payment"; "bought something through internet, but not paying for goods after receiving items"		"threatened someone through text messages, e-mails or in chat boxes"; "threatened someone through social media, such as WhatsApp, Facebook, Twitter, etc."

(*Continued*)

Table 2.6 (Continued)

	Cyber-dependent crime				*Cyber-enabled financial crime*		*Cyber-enabled personal crime/ deviance*	
	Malware	*Hacking*	*DoS*	*Digital piracy*	*Online banking fraud*	*Online shopping fraud*	*Hate speech*	*Online harassment*
ISRD4		"hacked or broken into a private account or computer to acquire data, get control of an account, or destroy data"				"used internet, e-mail or social media to dupe or deceive others (like phishing, selling worthless or illegal things, etc.) to make money"	"sent hurtful messages or comments on social media about someone's race, ethnicity or nationality, religion, gender identity, etc."	

*The wording of some questions has been shortened

Finally, the ISRD is probably the only *cross-national* self-report offending survey to include measures of online offending, which were introduced in its third wave (Haen-Marshall et al., 2022). Table 2.6 presents the main cybercriminal and cyberdeviant behaviors measured in its fourth wave, which included a larger variety of cybercrime types as well as improved wording for the offenses previously included. These include hacking and cyber-enabled behaviors such as online hate speech, online shopping fraud and sharing intimate images of others online (the latter not included in the table).

Table 2.6 shows that measurement varies extensively across surveys. Although all of them include measures of both cyber-enabled and cyber-dependent crime and deviance, the specific types of behaviors vary significantly. For example, when it comes to cyber-enabled crime and deviance, online hate speech and intimate posting are only measured in the ISRD. Distribution of child pornography and identity theft were only measured in the YDS. In addition, digital piracy and access to deviant websites were only included in the OCJS, while online harassment is only absent in the ISRD. Other cyber-enabled offenses like online shopping fraud are included in at least two of the surveys, but not only is there variation in how the items are formulated but also in the number of questions included (e.g., while the YDS probes about committing online shopping fraud both as seller and buyer, the ISRD includes a general question about deceiving others for money). With regard to cyber-dependent offenses, hacking is measured in all the surveys. However, while the OCJS and ISRD use more general questions about hacking into others' devices without their consent, the YDS provides a more exhaustive measurement of this behavior. Concretely, it includes multiple items that interrogate not only about illegally accessing email accounts or websites but also distinguishing between logging into computers to block access and to manipulate or destroy information.

The three surveys measure the prevalence of cybercriminal and cyberdeviant behavior (i.e., percentage of respondents involved in each type of behavior) but differ in the type of period prevalence measured. The YDS refers to lifetime prevalence (crime and deviant behaviors committed at any point in time) and the OCJS measures the last 12 months' prevalence, while the ISRD-4 measures both. In addition, the ISRD-4 also measures the incidence or frequency of offending (i.e., the number of times the offence was committed by the respondent). Furthermore, in the case of hacking, the ISRD-4 also includes additional follow-up questions about the motivation, *modus operandi*, detection by authorities or victim and rate of success (Haen-Marshall et al., 2022). All these measures can be particularly useful for the development of typologies of cyber offenders (Weulen Kranenbarg, 2022).

Ways forward and conclusions

Cybercrime has been on the rise since the 1990s (Caneppele & Aebi, 2019), and so is the need for researchers and public administrations to better estimate its prevalence, incidence, distribution and nature. The limitations of police statistics as measures of crime are widely known and seem even more severe—in terms of the volume of unrecorded offenses—in the case of cybercrimes (Decker, 2020; van de Weijer et al., 2019). The problem of under-recording may be even more acute for crimes suffered by organizations (Kemp et al., 2023). From that perspective, victimization surveys with national representative samples are seen as the main alternative to obtain more valid and reliable estimates of cybercrime

and cyberdeviance (Aebi et al., 2022; Reep-van der Bergh & Junger, 2018). Self-reported delinquency studies can provide information on juvenile cybercrime and cyberdeviance from the point of view of the offenders and, if accompanied by a victimization module, on the incidents suffered by the younger generations. Surveys also provide information on many other variables that are absent from police or court recorded crimes, related to the personal characteristics of individuals, their everyday activities, cybersecurity practices and so on, which allow identifying key risk factors and testing different theories of online crime and deviance (Holt & Bossler, 2008; Leukfeldt & Yar, 2016). In addition, surveys conducted regularly can also be key to assessing temporal changes in overall criminal behavior (Caneppele & Aebi, 2019).

While we have seen a rapid increase in the number of crime surveys that include measures of cybercrime since the early 2010s, our scoping review has identified a series of practices that could be refined to better measure online victimization and offending, and to enable cross-national and temporal comparisons. Overall, it seems reasonable to state that cybercrime and cyberdeviance is measured less adequately than more traditional crime types. This might be in part due to the ever-changing nature of cyberspace. For instance, music downloading seemed a major threat to intellectual property rights in the 1990s and early 2000s, until streaming services radically changed the way we interact with music. Similarly, online social media platforms follow each other constantly, in such a way that once survey items have been tested and seem valid for one of them, there is a new social media platform that dominates the market, hence making the previous questions irrelevant. Consequently, survey administrators must be constantly on guard to capture the set of crimes that probably represent the major criminal and deviant behaviors taking place in hybrid societies (Aebi, 2022). Our review of victimization surveys and self-reported delinquency studies is based on a purposively selected sample and therefore is not representative of how cybercrime and cyberdeviance is measured across the world, but it allows us to identify a series of inconsistencies across and within surveys that are likely to apply to other surveys at the national and local levels.[18]

One of the main implications of this review is that cross-national comparisons of cybercrime victimization are nowadays extremely challenging, if not impossible. Different surveys have different designs, consider different cybercrime types and conceptualize and operationalize cybercrime and cyberdeviance in different ways. Cross-national comparisons of online offending and deviance, at least of hacking, distribution of intimate images of others, online shopping fraud and hate speech committed by persons aged 13 to 17, are enabled by the ISRD (Haen-Marshall et al., 2022; Junger-Tas, 2010). In many cases, measures of cybercrime do not allow temporal comparisons, because these have only been included recently or have been changed in recent years. The fear of changing questions and thus losing historical series is one of the main reasons why some ongoing victimization surveys still do not include questions on cybercrime, often combined with the fear of increasing respondent fatigue and ultimately non-response or attrition bias (Guzy & Leitgöb, 2015; Hart et al., 2005). While we understand these concerns, cybercrime is undoubtedly an issue important enough both in terms of its prevalence and incidence, as well as because of its harms (Agrafiotis et al., 2018), to warrant its own measurement in crime surveys.

Our review suggests that the different sets of cybercrimes included in various surveys are not necessarily related to the main cybersecurity issues faced in each country. At best,

these could be explained by policy priorities which are not described in the documentation of surveys. The review also allows us to suggest that household victimization surveys should, at the very least, include direct measures of malware, hacking, spam/phishing, online shopping fraud, online banking fraud (if possible, distinguishing between online banking and credit card fraud), ID fraud, advance fee fraud, online hate crime and online harassment. Business surveys should also include measures of DoS, website defacements and internal threats, while self-reported delinquency studies should not forget digital piracy. Importantly, where possible these measures should be designed to match official definitions of crime, to enable estimates of the 'dark figure of crime', but always considering that their main role is probably to allow for cross-national and temporal comparisons. Additionally, surveys should include items to measure other forms of online deviant behaviors that are not necessarily categorized as 'criminal' (e.g., hate speech, harassment, bullying, etc.), which are already considered in a few of the sampled studies. Considerations such as whether questions refer to completed or attempted incidents, whether they refer to "at any point in time" or the last 12 months, whether they measure prevalence or incidence, and the wording of items more generally, should where possible also consider the measurement of cybercriminal and cyberdeviant behavior in other countries. In this regard, the creation of international networks of researchers and survey administrators may be essential in the future (e.g., Aebi et al., 2022). Finally, measures of cybercrime and cyberdeviance could be further refined by applying more sophisticated item validation measures and considering measurement invariance and item response theory (Murray et al., 2021; Osgood et al., 2002).

All things considered, both in terms of research and policy and practice, it is essential for national governments to come together and launch a new ICVS with a set of measures of cyber-dependent and cyber-enabled crime. The design of the ICVS with indicators of cybercrime and cyberdeviance would be key for a more accurate assessment of the extent and nature of cybercrime at a global scale, as well as potentially unearthing important cross-national patterns in victimization, and serve as a unique opportunity to capture these key measures in countries without instituted national crime surveys, especially in the Global South. While crime surveys are not free from limitations and are known to be affected by issues such as memory failures, social-desirability bias, underestimation or exaggeration of situations, telescoping and measurement non-invariance (Schneider, 1981; Skogan, 1975), they are still the best data source available to complement official statistics and better understand cybercrime and cyberdeviance. Ideally, future research should not only focus on describing differences in item wording and survey design across surveys, but also apply advanced psychometric assessment of cybercrime measures to ensure they enable reliable and valid estimates of cybercrime and cyberdeviance, both for national and international studies.

Notes

1 Annual reports of the Internet Crime Complaint Center IC3. www.ic3.gov/Home/AnnualReports
2 Interactive data dashboard of Action Fraud. www.actionfraud.police.uk/data
3 Internet Organized Crime Threat Assessment of EUROPOL. www.europol.europa.eu/publications-events/main-reports/iocta-report
4 Australian Cyber Security Centre Annual Cyber Threat Report. www.cyber.gov.au/acsc/view-all-content/reports-and-statistics

5 Private Rights Clearinghouse's data breaches dataset. https://privacyrights.org/data-breaches
6 McAfee's MVISION Insights dashboard. www.mcafee.com/enterprise/en-us/lp/insights-preview.html
7 Reports published by F-Secure. www.f-secure.com/en/press/media-library/reports
8 Reports published by Broadcom. www.broadcom.com/support/security-center/publications/archive
9 Access to data recorded by the Cambridge Cybercrime Centre can be requested through. www.cambridgecybercrime.uk/
10 Access to data recorded by the Korea University's Hacking and Countermeasure Research Lab can be requested through. https://ocslab.hksecurity.net/Datasets
11 Ransomwhere data. https://ransomwhe.re/
12 Bitcoin Abuse database. www.bitcoinabuse.com/api-docs
13 International Crime Victims Survey. https://wp.unil.ch/icvs/
14 To our knowledge, the Korean Crime Survey is the only recurring victimization survey in Asia, while non-recurring national crime surveys were undertaken in Thailand between 2006 and 2012, in Philippines in 2012 and in Kazakhstan in 2018.
15 Mexico's National Survey on the Availability and Use of Information Technologies at Home. www.inegi.org.mx/programas/mociba/2020/
16 2021 Eurobarometer on cybervictimization of organisations. https://eucrim.eu/news/survey-on-the-experience-of-smes-with-cybercrime/
17 Cyber Security Longitudinal Survey. www.gov.uk/government/publications/cyber-security-longitudinal-survey
18 The Islington Crime Survey, in the UK, and the Barcelona Victimization Survey, in Spain, are two examples of local crime surveys that also include measures of cybercrime.

References

Aebi M. F. (2006). *Comment Mesurer la Délinquance?* Armand Colin.

Aebi, M. F. (2022). Lessons learned from a council of Europe's conference on measuring cybercrime. In M. F. Aebi, S. Caneppele, & L. Molnar (Eds.), *Measuring cybercrime in Europe: The role of crime statistics and victimisation surveys* (pp. 7–18). Eleven.

Aebi, M. F., Caneppele, S., Harrendorf, S., Hashimoto, Y. Z., Jehle, J., Khan, T. S., Kühn, O., Lewis, O., Molnar, L., Smit, P., Þórisdóttir, R., & National Correspondents. (2021). European sourcebook of crime and criminal justice statistics 2021 (6th ed.). *Series UNILCRIM*, 1. UNILCRIM.

Aebi, M. F., Caneppele, S., & Molnar, L. (Eds.). (2022). *Measuring cybercrime in Europe: The role of crime statistics and victimisation surveys*. Eleven.

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.

Aebi, M. F., and Linde, A. (2014). National victimization surveys. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. 3228–3242). Springer.

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006.

Allen, J., Forrest, S., Levi, M., Roy, H., & Sutton, M. (2005). *Fraud and technology crimes: Findings from the 2002/3 British crime survey and 2003 offending, crime and justice survey* [Online Report 34/05]. Home Office.

Alvazzi del Frate, A. (2004). The international crime business survey: Findings from nine central—Eastern European Cities. *European Journal on Criminal Policy and Research*, *10*(2), 137–161.

Biderman, A. D., & Reiss, A. J. (1967). On exploring the "dark figure" of crime. *The ANNALS of the American Academy of Political and Social Science*, *374*(1), 1–15.

Bilodeau, H., Lari, M., & Uhrbach, M. (2019). *Cyber security and cybercrime challenges of Canadian businesses, 2017* [Report 85–002-X]. Statistics Canada.

Bottoms, A. E., Mawby, R. I., & Walker, M. A. (1987). A localised crime survey in contrasting areas of a city. *The British Journal of Criminology*, *27*(2), 125–154.

Brunton-Smith, I., & Sturgis, P. (2011). Do neighborhoods generate fear of crime? An empirical test using the British crime survey. *Criminology*, *49*(2), 331–369.

Buil-Gil, D., Brunton-Smith, I., Pina-Sánchez, J., & Cernat, A. (2022). Comparing measurements of violent crime in local communities: A case study in Islington, London. *Police Practice and Research*, *23*(4), 489–506.

Buil-Gil, D., Lord, N., & Barrett, E. (2021b). The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention. *Victims & Offenders*, *16*(3), 286–315.

Buil-Gil, D., Zeng, Y., & Kemp, S. (2021a). Offline crime bounces back to Pre-COVID levels, cyber stays high: Interrupted time-series analysis in Northern Ireland. *Crime Science*, *10*(26).

Burnap, P., & Williams, M. L. (2016). Us and them: Identifying cyber hate on twitter across multiple protected characteristics. *EPJ Data Science*, *5*(11).

Candolle, A. de (1830/1987). Considérations sur la statistique des délits. *Déviance et Société*, *11*(4), 352–355.

Candolle, A. de (1832/1987). De la statistique criminelle. *Déviance et Société*, *11*(4), 356–363.

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.

Castaño-Pulgarín, S. A., Suárez-Betancur, N., Vega, L. M. T., & López, H. M. H. (2021). Internet, social media and online hate speech. systematic review. *Aggression and Violent Behavior*, *58*, 101608.

Cernat, A., Buil-Gil, D., Brunton-Smith, I., Pina-Sánchez, J., & Murrià-Sangenís, M. (2022). Estimating crime in place: Moving beyond residence location. *Crime & Delinquency*, *68*(11), 2061–2091.

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

Chun, J., Lee, J., Kim, J., & Lee, S. (2020). An international systematic review of cyberbullying measurements. *Computers in Human Behavior*, *113*, 106485.

Cioban, S., Lazăr, A. R., Bacter, C., & Hatos, A. (2021). Adolescent deviance and cyber-deviance. A systematic literature review. *Frontiers in Psychology*, *12*, 748006.

Coleman, C., & Moynihan, J. (1996). *Understanding crime data: Haunted by the dark figure*. Open University Press.

Correia, S. G. (2022). Making the most of cybercrime and fraud crime report data: A case study of UK action Fraud. *International Journal of Population Data Science*, *7*(1), 09.

Crowe. (2017). *Annual frau indicator 2017. Identifying the cost of fraud to the UK economy*. Crowe UK.

Dearden, T. E., & Parti, K. (2021). Cybercrime, differential association, and self-control: Knowledge transmission through online social learning. *American Journal of Criminal Justice*, *46*, 935–955.

Decker, E. (2020). Full count?: Crime rate swings, cybercrime misses and why we don't really know the score. *Journal of National Security Law and Policy*, *10*, 583–604.

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, *5*(1).

Elliott, D. S., Huizinga, D., & Ageton, S. S. (1985). *Explaining delinquency and drug use*. SAGE.

Enghoff, O., & Aldridge, J. (2019). The value of unsolicited online data in drug policy research. *International Journal of Drug Policy*, *73*, 210–218.

Ennis, P. H. (1967). *Criminal victimization in the United States. A report of a national survey*. US Government Printing Office.

EUROPOL. (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Publications Office of the European Union.

Farrell, G., & Pease, K. (1993). *Once bitten, twice bitten: Repeat victimisation and its implications for crime prevention* [Crime Prevention Unit Series Paper No. 46]. Home Office Police Department.

Furnell, S., Emm, D., & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. *Computer Fraud & Security*, *10*, 5–12.

Gold, M. (1970). *Delinquent behavior in an American city*. Brooks.

Graham, R. S., & Smith, S. K. (2020). *Cybercrime and digital deviance*. Routledge.

Gundur, R. V., Berry, M., & Taodang, D. (2021). Using digital open source and crowdsourced data in studies of deviance and crime. In A. Lavorgna & T. J. Holt (Eds.), *Researching cybercrimes* (pp. 145–167). Palgrave Macmillan.

Guzy, N., & Leitgöb, H. (2015). Assessing mode effects in online and telephone victimization surveys. *International Review of Victimology*, *21*(1), 101–131.

Haen-Marshall, I., Birkbeck, C. H., Enzmann, D., Kivivouri, J., Markina, A., & Steketee, M. (2022). *International Self-Report Delinquency (ISRD4) study protocol: Background, Methodology, And Mandatory Items For the 2021/2022 survey* [ISRD Technical Report 4]. Northeastern University.

Hart, T. C., Rennison, C. M., & Gibson, C. (2005). Revisiting respondent "fatigue bias" in the national crime victimization survey. *Journal of Quantitative Criminology*, *21*(3), 345–363.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Ballinger Publishing.

Hindelang, M. J., Hirschi, T., & Weis, J. G. (1981). *Measuring delinquency*. SAGE.

Hirschi, T. (1969). *Causes of delinquency*. University of California Press.

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

Huey, L., & Buil-Gil, D. (Eds.). (2024). *The crime data handbook*. Bristol University Press.

International Telecommunication Union. (2021). *Measuring digital development: Facts and figures 2021*. ITU Publications.

Junger, M., Wang, V., & Schlömer, M. (2020). Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime Science*, *9*(13).

Junger-Tas, J. (2010). The significance of the International Self-report Delinquency Study (ISRD). *European Journal on Criminal Policy and Research*, *16*, 71–87.

Junger-Tas, J., & Marshall, I. H. (1999). The self-report methodology in crime research. *Crime and Justice*, *25*, 291–367.

Kemp, S., Buil-Gil, D., Miró-Llinares, F., & Lord, N. (2023). When do businesses report cybercrime? Findings from a UK study. *Criminology & Criminal Justice*, *23*(3), 468–489.

Lauritsen, J. L. (1993). Sibling resemblance in juvenile delinquency: Findings from the national youth survey. *Criminology*, *31*(3), 387–409.

Lee, B. H. (2018). Explaining cyber deviance among school-aged youth. *Child Indicators Research*, *11*(2), 563–584.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280.

Lynch, J. P., & Addington, L. A. (Eds.). (2006). *Understanding crime statistics: Revisiting the divergence of the NCVS and UCR*. Cambridge University Press.

Maguire, M. (1997). Crime statistics, patterns, and trends: Changing perceptions and their implications. In M. Maguire, R. Morgan, & R. Reiner (Eds.), *The Oxford handbook of criminology* (2nd ed., pp. 135–188). Oxford University Press.

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence* [Research Report 75]. Home Office.

Murray, A. L., Eisner, M., Ribeaud, D., Kaiser, D., McKenzie, K., & Murray, G. (2021). Validation of a brief self-report measure of adolescent bullying perpetration and victimization. *Assessment*, *28*(1), 128–140.

Office for National Statistics. (2021). *Table D10: Percentage of CSEW incidents reported to the police or action fraud, year ending December 1981 to year ending March 2020 CSEW*. Retrieved from www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesannualtrendanddemographictables/current (Last accessed 02 April 2022).

Osborn, D. R., Trickett, A., & Elder, R. (1992). Area characteristics and regional variates as determinants of area property crime levels. *Journal of Quantitative Criminology*, *8*, 265–285.

Osborn, D. R., & Tseloni, A. (1998). The distribution of household property crimes. *Journal of Quantitative Criminology*, *14*, 307–330.

Osgood, D. W., McMorris, B. J., & Potenza, M. T. (2002). Analyzing multiple-item measures of crime and deviance I: Item response theory scaling. *Journal of Quantitative Criminology*, *18*, 267–296.

Paquet-Clouston, M., Décary-Hétu, D., & Morselli, C. (2018). Assessing market competition and vendors' size and scope on AlphaBay. *International Journal of Drug Policy*, *54*, 87–98.

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.

Rantala, R. (2008). *Cybercrime against businesses, 2005. Special report, bureau of justice statistic*s. US Department of Justice.

Reep-van der Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, *7*, 5.

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.

Sampson, R. J., & Groves, B. W. (1989). Community structure and crime: Testing social disorganization theory. *American Journal of Sociology*, *94*(4), 774–802.

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.

Sellin, T. (1931). The basis of a crime index. *Journal of Criminal Law and Criminology*, *22*(3), 335–356.

Short, J. F., & Nye, F. I. (1958). Extent of unrecorded juvenile delinquency: Tentative conclusions. *The Journal of Criminal Law, Criminology, and Police Science*, *49*(4), 296–302.

Skogan W. G. (1975). Measurement problems in official and survey crime rates. *Journal of Criminal Justice*, *3*(1), 17–31.

Skogan, W. G. (1977). Dimensions of the dark figure of unreported crime. *Crime & Delinquency*, *23*(1), 41–50.

Solymosi, R., & Bowers, K. (2018). The role of innovative data collection methods in advancing criminological understanding. In G. J. N. Bruinsma & S. D. Johnson (Eds.), *The Oxford handbook of environmental criminology* (pp. 210–237). Oxford University Press.

Sparks, R. F. (1981). Surveys of victimization-an optimistic assessment. *Crime and Justice*, *3*, 1–66.

Tarling, R., & Morris, K. (2010). Reporting crime to the police. *The British Journal of Criminology*, *50*(3), 474–490.

Tilley, N., & Tseloni, A. (2016). Choosing and using statistical sources in criminology: What can the crime survey for England and Wales tell us? *Legal Information Management*, *16*(2), 78–90.

van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, *16*(4), 486–508.

van der Laan, A. M., Rokven, J., Weijters, G., & Beerthuizen, M. (2021). The drop in juvenile delinquency in the Netherlands: Changes in exposure to risk and protection. *Justice Quarterly*, *38*(3), 433–453.

van Dijk, J. J. M., van Kesteren, J., & Smit, P. (2007). *Criminal victimisation in international perspective. key findings from the 2004–2005 ICVS and EU ICS*. WODC.

Wallerstein, J. S., & Wyle, C. J. (1947). Our law-abiding law-breakers. *Probation*, *25*, 107–112.

Weulen Kranenbarg, M. (2022). When do they offend together? Comparing co-offending between different types of cyber-offenses and traditional offenses. *Computers in Human Behavior*, *130*, 107186.

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, *40*(1), 40–55.

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior*, *40*(9), 1119–1131.

Young, M., Rodriguez, L., Keller, E., Sun, F., Sa, B., Whittington, J., & Howe, B. (2019). Beyond open vs. Closed: Balancing individual privacy and public accountability in data sharing. In *Proceedings of the conference on fairness, accountability, and transparency* (pp. 191–200). Association for Computing Machinery.