Advancing Accurate and Objective Cybercrime Metrics

Stephen Cobb*

Introduction

The goal of this paper is to advance efforts to improve cybercrime metrics, measures of the scale and impact of cybercrime that are widely considered to be an essential part of any comprehensive enforcement strategy against cybercriminals. Enforcing laws to protect citizens and their property against harms caused by criminal behavior is a basic function of modern society. Measuring the scale and impact of criminal activity has long been an essential part of that function. "[A]ccurate and valid data and research information on both crime and victimization are critical for an understanding of crime. . . and for any assessment of the quality of the activities and programs of the criminal justice system."[1]

When it comes to tackling criminal activity involving or targeting computers, the importance of metrics to crime deterrence are critical and obvious. As reflected in this observation from 15 years ago: "[u]ntil there are accepted measures and benchmarks for the incidence and damage caused by computer-related crime, it will remain a guess whether we are spending enough resources to investigate or protect against such crimes. . . In short, metrics matter."[2]

Given that many countries have well-established procedures for producing official government reports on the incidence of traditional or *meatspace* crime;[3] there would appear to be a "cybercrime metrics gap," a global shortage of official data on crimes committed in cyberspace. However, this apparent "cybercrime metrics gap" is an illusion. Even the most affluent of nations have not yet managed to consistently generate acceptable statistics about any crimes, cyber or non-cyber, where acceptable means the level of accuracy, detail, completeness, and timeliness required to satisfy the needs of those who shape, make, and enforce the law.[4] While a deficiency in crime metrics clearly hampers enforcement efforts

* Stephen Cobb, CISSP, is an independent researcher and public-interest technologist with more than 30 years' experience in the information system security industry.

[1] *See* John V. Pepper & Carol V. Petrie, *Overview*, *in* MEASUREMENT PROBLEMS IN CRIMINAL JUSTICE RESEARCH: WORKSHOP SUMMARY 1, 1 (Alfred Blumstein ed., 2003).

[2] *See* Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, 9 VA. J.L. & TECH. 1, 1 (2004).

[3] The term *meatspace* appears to originate in Gibson's 1984 novel *Neuromancer*, entering the Oxford English Dictionary in 2001 and giving rise to *meatcrime* or *meatspace crime* as a useful shorthand for crime occurring in the physical world, sometimes referred to as traditional crime or non-cyber crime. *See* David Wall, *Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime*, 11 INFO., COMMC'N & SOC'Y 861, 863-864 (2008).

[4] *See, e.g.*, Pepper & Petrie, *supra* note 1 (stating "there are significant and substantive measurement problems with the existing surveys"); K. J. Strom & E. L. Smith, *The Future of Crime Data: The Case for the National Incident-Based Reporting System (NIBRS) as a Primary Data Source for Policy*

for all forms of crime, it would seem to be particularly damaging to nascent efforts to deter and defeat cybercrime.

Currently, there is broad consensus – among academics, policymakers, security practitioners and solution providers – that cybercrime has increased dramatically in this century. By 2019 it was possible for an academic study to conclude that cybercrime accounts for "half of all property crime, by volume and value."[5] There is no shortage of data pointing to a dire state of affairs in cyberspace, published under headlines like "Global Breach Costs Set to Top $5 Trillion By 2024,"[6] and "Mobile Cyberattacks on the rise."[7] The manner in which such numbers and claims are quoted – and requoted – may lead the casual observer to believe they are based on official cybercrime metrics, yet few if any of these reports are the product of a comprehensive effort to consistently and objectively catalogue cybercriminal activity over time.[8] One body of research that has applied scientific standards to measuring the cost of cybercrime is an academic project that has only issued – albeit heroically – two reports, the one from 2019 referenced earlier in this paragraph, and another published in 2012.[9]

In the seven sections that follow, this paper addresses the challenge of producing accurate and objective cybercrime metrics. Section I outlines the cybercrime measurement problem, explaining the need for crime metrics and describing some of the more useful ways in which cybercrime has been defined and categorized. Section II discusses the standard methodologies of crime measurement and their shortcomings as currently implemented, drawing on two reports produced by the "Modernizing Crime Statistics" project of the National Academies of Sciences, Engineering, and Medicine (NMCS).[10] The NMCS project was the work of a panel of experts convened by the Bureau of Justice Statistics (BJS) and

Evaluation and Crime Analysis, 16 CRIMINOLOGY & PUB. POL'Y 1027, 1028 (2017) (stating "the stark reality is that at a national level, and within many states, those detailed data do not exist").

[5] Ross Anderson et al., *Measuring the Changing Cost of Cybercrime*, *in* WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (2019) [hereinafter Anderson, *Measuring the Cost 2019*], https://perma.cc/6RM3-48U2.

[6] Phil Muncaster, *Global Breach Costs Set to Top $5 Trillion By 2024*, INFOSECURITY MAG. (Aug. 29, 2019), https://perma.cc/A8DK-J85L.

[7] *See, e.g.*, Eileen M. Decker, *Full Count?: Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score*, 10 J. NAT'L SECURITY L. & POL'Y 583 (2020).

[8] *See generally* Stephen Cobb, *Sizing Cybercrime: Incidents and Accidents, Hints and Allegations*, VIRUS BULL. (Sept. 30, 2016) [hereinafter Cobb, *Sizing Cybercrime*], https://perma.cc/4N33-ERMB; *see also* Julie J.C.H Ryan & Theresa I. Jefferson, *The Use, Misuse and Abuse of Statistics in Information Security Research* (Am. Soc'y for Eng'g Mgmt., Working Paper, 2003) at 6 ("In most of the surveys [analyzed herein], many respondents from the same organization were chosen as part of the targeted population. What might have been a single virus incident, therefore, might have been reported many times, inflating the true incident rate of the problem."); Ross Anderson et al., *Measuring the Cost of Cybercrime*, *in* WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY 1, 2 (2012) [hereinafter Anderson, *Measuring the Cost 2012*], https://perma.cc/X6MB-H3YA.

[9] Anderson, *Measuring the Cost 2012*, *supra* note 8.

[10] NAT'L ACAD. OF SCI., ENG'G, & MED., MODERNIZING CRIME STATISTICS: REPORT 1: DEFINING AND CLASSIFYING CRIME (2016) [hereinafter NMCS R1], https://perma.cc/J7NM-HGUJ; NAT'L ACAD. OF SCI., ENG'G, & MED., MODERNIZING CRIME STATISTICS: REPORT 2: NEW SYSTEMS FOR MEASURING CRIME (2018) [hereinafter NMCS R2], https://perma.cc/97C8-MF96.

the Federal Bureau of Investigation (FBI), at the suggestion of the US Office of Management and Budget. The panel was charged with making "recommendations for the development of a modern set of crime measures in the United States and the best means for obtaining them."[11] Section II also illustrates the implications of the status quo for cybercrime metrics with a brief case study of one particular crime – identity theft.

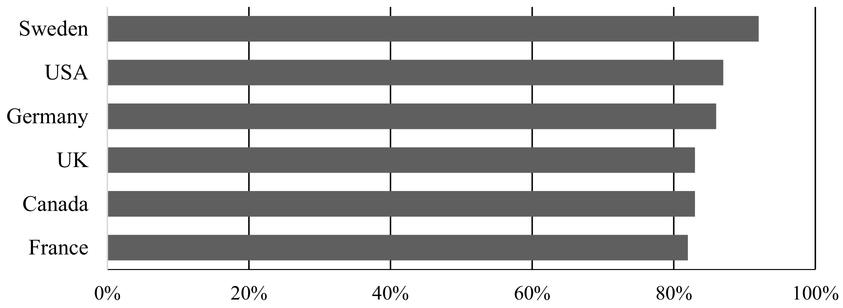
Section III discusses issues in adapting existing crime measurement tools to fully capture the scale and impact of cybercrime together with the importance of measuring all of the harms inflicted by cybercrime. Section IV reviews the current state of cybercrime metrics and presents a promising path toward more complete, accurate, and reliable cybercrime metrics. Section V notes obstacles to moving forward and suggests strategies for overcoming them. And section VI notes the paper's limitations and omissions. The final section summarizes the prospects for achieving the kind of improvements to cybercrime metrics that could empower efforts to develop and implement a comprehensive and much needed enforcement strategy against global cybercrime.

I. Defining the Cybercrime Metrics Problem

Cybercrime is a global problem that negatively impacts everyone – from commercial enterprises to government agencies, non-governmental organizations, and the public – in every nation and territory.[12] Multiple surveys in countries with high levels of Internet adoption suggest a high degree of concern that the risk of becoming a victim of cybercrime is increasing (see Figure 1).[13]

Figure 1: Risk of cybercrime increasing

Percentage of respondents who "believe the risk of becoming a victim of cybercrime is increasing" (totally agree + tend to agree)



[11] NMCS R1, *supra* note 10, at 1.

[12] It is not unusual for security product vendors to support licensed users of their software in "200 countries and territories." *See, e.g.*, Enjoy Safer Tech., https://perma.cc/K376-QW6W (last visited Dec. 29, 2019).

[13] Stephen Cobb, *ESET Cybersecurity Barometer USA* 2018, We Live Security (Jan. 24, 2019, 5:57 PM) [hereinafter Cobb, *Barometer USA*], https://perma.cc/2YZ9-Q8QB; European Comm'n, Special Eurobarometer 480 Report on Europeans' attitudes towards Internet security 69 (2019).

Despite these high levels of concern, none of these countries – or any others – can claim to be producing trusted metrics that comprehensively quantify the scale and impact of cybercrime over time and in a timely manner. Even as public opinion strongly suggests that current efforts to prevent crimes in cyberspace are falling short,[14] governments are still struggling to obtain reliable data with which to determine whether this is true, and if so, to what extent.[15] This parlous situation is – in the author's opinion – the result of a longstanding neglect of crime measurement responsibilities at the national and international level, neglect that has undermined our ability to develop information-based policies for tackling crimes of all kinds, not just those committed in cyberspace.[16]

A. *Why Measure Crime?*

Awareness of the benefits of quantifying criminal activity has existed since at least the eighteenth century.[17] In the following century the benefits of crime data analysis were clearly illustrated,[18] long before the bootstrapping of the first computing devices.[19] Today, the most frequently cited reasons for measuring crime of all kinds can be stated as the need to answer the six questions listed in Table 1:[20]

[14] *See* Stephen Cobb, *Towards an International "Who-cares-ometer" for Cybercrime*, VIRUS BULL. (Oct. 4, 2018) [hereinafter Cobb, *"Who-cares-ometer"*], https://perma.cc/5UC7-GGBX (noting that less than half of North American respondents agreed that law enforcement is doing enough to fight cybercrime).

[15] *See generally* Directorate Gen. for Internal Policies, *The Economic, Financial & Social Impacts Of Organised Crime In The European Union*, PE 493.018 (2013) ("So is cybercrime a threat, and to whom? It is a threat to all of us. The question is how much of a threat.").

[16] James Comey, Director, Fed. Bureau of Investigation, Remarks at the 2015 International Association of Chiefs of Police Conference (Oct. 26, 2015), https://perma.cc/Q2Q8-RYUH (noting "We can't tell you on a national level how many shootings there were in any particular city last weekend, when parts of private industry can tell you how many people saw the movie "The Martian" last weekend. How can we address a rise in violent crime without good information? And without information every single conversation in this country about policing and reform and justice is uninformed and that is a very bad place to be.").

[17] In the eighteenth-century, Bentham "saw the need to collect and maintain statistical data regarding crime, primarily because this would provide information that legislators needed to fulfill their responsibilities." ENCYCLOPEDIA OF CRIMINOLOGICAL THEORY 92 (Francis T. Cullen et al. eds., 2010).

[18] *See*, *e.g*., Andre-Michel Guerry et al., A TRANSLATION OF ANDRE-MICHEL GUERRY'S ESSAY ON THE MORAL STATISTICS OF FRANCE (1883): A SOCIOLOGICAL REPORT TO THE FRENCH ACADEMY OF SCIENCE (2002).

[19] It should be noted that analysis of crime data has been a serious motivator of computational technology, dating back to Guerry's invention of the Ordonnateur Statistique. *See generally* Michael Friendly & Nicolas de Sainte Agathe, *André-Michel Guerry's "Ordonnateur Statistique*: *The First Statistical Calculator?*, 66 AM. STATISTICIAN, 195, 195-200 (2012).

[20] *See* SHARON L. LOHR, MEASURING CRIME: BEHIND THE STATISTICS 13 (2019).

Table 1: Reasons to measure crime

1	How much crime has occurred?
2	What types of crime are increasing or decreasing
3	Who are the victims and offenders?
4	What are the costs of crime to victims and to society?
5	What crime-prevention and crime-reduction strategies are effective?
6	Where should law enforcement resources be allocated?

These are the questions that the process of collecting and analyzing crime metrics attempts to answer. Ideally, for the purposes of information-based criminal policy, they should be asked in a consistent manner, on a recurring basis, by a trusted entity.

B. What is Cybercrime?

Before the questions in Table 1 can be answered with respect to cybercrime,[21] the term needs to be defined. In general and for the purposes of this paper, cybercrime means: "crimes in which computer networks are the target or a substantial tool."[22] Examples of cybercrime range from physical theft of computer equipment and the cloning of data for illegal resale – popular in the 1980s – to unauthorized access to systems and data for use in criminal enterprises, enabled by the rapid growth of networking in the 1990s.

This century has seen extensive criminal diversification into many different forms of computer-enabled or digitally enhanced malfeasance including numerous varieties of identity theft, fraud, and extortion. These crimes, made possible by almost universal electronic connectivity between people, companies, governments, and institutions of all kinds, can be committed at scale across national boundaries. Recent cybercrime trends include the abuse of encryption technology to enable ransom demands, unauthorized access to information systems for the purposes of mining cryptocurrency, and the manipulation of electronic messaging and Voice over Internet Protocol (VoIP) telephony to perpetrate scams like advance fee fraud and business email compromise.[23]

[21] While "cyberspace crime" is arguably a more accurate way to describe this category of crime than cybercrime, the latter "prevails as the accepted term." Wall, *supra* note 3, at 863. Similarly, although some information security professionals still balk at the use of "cybersecurity" to describe the activity of protecting networked computer systems and the data they process, store, and communicate, cybersecurity has prevailed as the term of choice. *Id.*

[22] Bert-Jaap Koops, *The Internet and its Opportunities for Cybercrime*, *in* TRANSNATIONAL CRIMINOLOGY MANUAL 735 (M. Herzog-Evans ed., 2010).

[23] In 2018, the IC3 received 20,373 BEC/E-mail Account Compromise (EAC) complaints with adjusted losses of over $1.2 billion. FED. BUREAU OF INVESTIGATION, 2018 INTERNET CRIME (2019), https://perma.cc/893B-PGBY.

The preceding trends are just a few of the many activities in this category of crime. The scale and complexity of these activities greatly complicate efforts to measure cybercrime as well as efforts to defend against it. These defensive efforts can be collectively described as cybersecurity. Indeed, in addition to the "problem of measuring cybercrime" we also have a "measuring cybersecurity problem."[24] Efforts to improve the availability of better cybercrime metrics will not only support cyber-enforcers in a wide range of agencies, but also assist cyber-defenders throughout society, from commercial companies to government bodies, NGOs, and the citizenry at large.

Debates about the ontology of computer-related crimes began toward the end of the last century and involved multiple parties with differing interests and agendas, including academics, lawyers, security industry professionals, internet service providers, security solution vendors, and corporate risk managers.[25] Over time it became clear that some computer crimes are unique to computers while others are traditionally prohibited forms of human misbehavior enhanced by technology. This distinction was embodied in the 2001 Council of Europe Convention on Cybercrime under the four titles shown in Table 2:[26]

Table 2: Council of Europe Convention on Cybercrime Titles

Title 1	Offences against the confidentiality, integrity and availability of computer data and systems
Title 2	Computer-related offences
Title 3	Content-related offences
Title 4	Offences related to infringements of copyright and related rights

Grabosky suggested three forms of cybercrime based on whether the computer was the instrument of crime, the target of the crime, or incidental to the crime.[27] In one of the most substantive works on measuring the cost of cybercrime,[28] a similar threefold definition is adopted from the European Commission's 2007

[24] *See generally* Karl Frederick Rauscher, *Measuring the Cybersecurity Problem*, EASTWEST INSTITUTE (Oct. 21, 2013), https://perma.cc/K226-YQT2 ("We do not have even an order-of-magnitude estimate of some of the most basic aspects of the cybersecurity problem that can be validated.").

[25] *See generally* Donn Parker, *The dark side of computing: SRI International and the study of computer crime*, 29 IEEE ANNALS OF THE HISTORY OF COMPUTING 3 (2007); Marc Goodman, *Why the police don't care about computer crime*, 10 HARV. J.L. & TECH. 465 (1996), https://perma.cc/4UXD-U4RB ("There is disagreement nationally and globally as to what exactly constitutes a computer crime. The term 'computer crime' covers such a wide range of offenses that unanimity has been an elusive goal.").

[26] Convention on Cybercrime, *opened for signature* Nov. 23, 2001, E.T.S. 185, https://perma.cc/47Q3-SAQW. Similar distinctions were embedded in the US Computer Fraud and Abuse Act of 1986 and the United States Senate ratified the convention in 2006, see *Reservations and Declarations for Treaty No.185 - Convention on Cybercrime*, COUNCIL OF EUROPE, https://perma.cc/FLV6-Z4SM.

[27] *See* Rick Sarre, Laurie Yiu-Chung Lau & Lennon Y.C. Chang, *Responding to cybercrime: current trends*, 19 POLICE PRACTICE & RESEARCH 515 (2018), https://perma.cc/4ZRG-YNJ9 (quoting PETER GRABOSKY, ELECTRONIC CRIME (2008)).

[28] *See generally* Anderson, *Measuring the Cost 2012*, *supra* note 8, at 3.

Communication “Towards a general policy on the fight against cyber crime.”[29]

1. Traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems;
2. The publication of illegal content over electronic media (e.g., child sexual abuse material or incitement to racial hatred);
3. Crimes unique to electronic networks, e.g., attacks against information systems, denial of service and hacking.[30]

Entities that have attempted to measure public attitudes to cybercrime and cybersecurity have tended to use more specific lists of crimes. One example, shown in Table 3, is the list of “situations” used in the Eurobarometer-style surveys of public attitudes towards cybersecurity and related issues. The numbers in the second column of Table 3 indicate the percentage of North American respondents in a 2018 study who said that they had experienced those situations “often” or “occasionally.”[31] The third column shows the equivalent response from the most recent Eurobarometer survey on internet security.[32]

Table 3: EU Barometer cybersecurity situations with NA prevalence data

How often have you experienced or been a victim of:	NA	EU
Receiving fraudulent emails or phone calls asking for your personal details	71%	34%
Discovering malicious software (viruses, etc.) on your device	58%	33%
Being a victim of bank card or online banking fraud	34%	11%
Your social network account or email being hacked	31%	12%
Online fraud where goods purchased are not delivered, counterfeit, as advertised	29%	15%
Identity theft (somebody stealing your personal data and impersonating you)	27%	7%
Being asked for a payment in return for getting back control of your device	24%	9%
Not being able to access online services like banking or public services because of cyber-attacks	23%	11%

[29] EUR. PARL. DOC. (COM 267) (2007), https://perma.cc/48DB-87RX.

[30] It is worth noting that the term *hacking* has multiple meanings, some of which are positive. Many security professionals now avoid using *hacking* as shorthand for *illegal computer intrusion* or implying that *hacker* means *criminal*; the terms *criminal hacking* and *criminal hacker* are preferable.

[31] Cobb, *“Who-cares-ometer”*, *supra* note 14.

[32] EUROPEAN COMM’N, *supra* note 13.

A number of important ways in which computer crime differs from traditional crime were enumerated by Brenner's landmark 2004 law journal article on cybercrime metrics. She suggested that cybercrime may be categorically different from traditional crime, in terms of scale, action at a distance, and evidentiary challenges.[33] However, she concluded that "cybercrime is, after all, simply crime."[34]

It should be noted that several very detailed and complex cybercrime taxonomies have been proposed;[35] however, while undoubtedly of great value for in-depth research into cybersecurity, they may have limited utility in cybercrime metrics at the collection and reporting phase, where resources can be scarce in terms of time, knowledge, and skillsets. The more pressing need is for terminology that describes cybercriminal activity accurately but in plain language, amenable to reporting and surveying, and with sufficient granularity to permit useful insights when analyzed.

II. CRIME DATA: SOURCES AND CHALLENGES

Unfortunately, even with consensus on the ontology of cybercrime, we would still be a long way from providing a clear picture of its scale and impact to those who shape, make, and enforce the law. This is not because the problems inherent in measuring cybercrime are impossible to solve – this paper argues that they are not – but because there is a bigger problem: the governments of the world have not yet achieved statistical mastery of crime in general, whether it occurs in cyberspace or meatspace.

This problem is well-illustrated by recent reassessments of the apparent decline in traditional crime rates in the US and UK between 1990 to 2010. This trend, widely referred to in the literature as 'the crime drop,' might not have been as significant as once thought according to recent research into the underlying metrics.[36] The implications for crime policy and policing are serious, especially if the crime drop turns out to be an example of *crime displacement*.[37]

Some criminologists are now hypothesizing that traditional criminal activity began to move online at the start of this century rather than simply ceasing.[38] If

[33] Brenner, *supra* note 2, at 9.

[34] *Id.* at 52.

[35] *See, e.g.*, Ravinder Barn & Balbir Barn, *An Ontological Representation of a Taxonomy for Cybercrime*, TWENTY-FOURTH EUROPEAN CONF. ON INFO. SYS., Paper No. 45 (2016).

[36] *See* Maria Tcherni et al., *The Dark Figure of Online property Crime: is Cyberspace Hiding a Crime Wave?*, 33 JUST. Q. 890 (2016); Mike Maguire & Sue McVie, *Crime Data and Criminal Statistics: A Critical Reflection*, THE OXFORD HANDBOOK OF CRIMINOLOGY 163, 180 (2017).

[37] *See* David Weisburd et al., *Does Crime Just Move Around the Corner? A Controlled Study of Spatial Displacement and Diffusion of Crime Control Benefits*, 44 CRIMINOLOGY 549, 549-591 (2006).

[38] *See, e.g.*, Matt Hopkins, *The Crime Drop and the Changing Face of Commercial Victimization: Reflections on the 'Commercial Crime Drop' in the UK and the Implications for Future Research*, 16 CRIMINOLOGY & CRIM. J. 410 (2016), https://perma.cc/2AYH-TGHM; Stefano Caneppele & Marcelo F Aebi, *Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes*, 13 POLICING 66 (2019); Anderson, *Measuring the Cost 2012*, *supra* note 8, at 6 ("If this interpretation is correct, then cybercrime is now the typical volume property crime in the UK, and the case for more vigorous policing is stronger than ever.").

better crime metrics had been available, governments might have alerted to this possibility sooner, enabling policies to be developed and resources allocated to stem the growth of cybercrime before it became an established alternative form of criminality.

However, while it is disappointing to discover that cybercrime is not the only area of crime measurement that needs serious attention, the need for wholesale improvements in all forms of crime metrics may mean that there is an opportunity to bundle the creation of solid cybercrime metrics into a broader project to improve the measurement of crime in general. There will be more on this possibility in section IV.

A. Reporting and Surveying Crime

Historically, there have been two main approaches to measuring the magnitude, nature, and impact of crime.[39] You can collect data about crimes when they are reported to the authorities or you can ask members of the public if they know of any crimes that have been committed. These two approaches are broadly referred to as reporting and surveying.

In many countries, the aggregation and publication of data on crimes reported to the police has been a routine function of central government for decades. The US government's main effort in this regard has been the Universal Crime Reporting (UCR) Program. Under this program, administered by the US Department of Justice (DOJ), the FBI coordinates reports from some 18,000 local law enforcement agencies.[40] The UCR Program consists of the Summary Reporting System (SRS), which dates back to 1930, and the more recently developed National Incident-Based Reporting System (NIBRS) to which SRS is scheduled to be fully converted by 2021 (referred to jointly as SRS/NIBRS for current purposes).[41]

The crime measurement efforts under SRS/NIBRS suffer from a deficiency common to all crime reporting systems – not all crime is reported to the appropriate authorities. There are many reasons for this, including low expectations of police response, fear of retaliation, and concerns about self-incrimination with respect to illegal substances or immigration status. The complex nature of offender-victim relationships may also lead to crimes going unreported.[42] Even with drastic improvements in policing it is likely that there will always be a number of crimes that are not reported.

Fortunately, it is possible to learn a lot about the level of criminal activity in society by asking people if they have been the victim of such activity. This can be done at scale through surveys, using well-tested techniques to question a

[39] *See* Fed. Bureau of Investigation, *The Nation's Two Crime Measures*, UNIF. CRIME REPORTING, https://perma.cc/8LJB-ZDZE (last visited Dec. 25, 2019).

[40] *See* NMCS R1, *supra* note 10, at 3

[41] *Id.* at 23.

[42] *See* Josephine Wolff, *How Unreliable Data Leads to the Undercounting of Cybercrime*, PAC. STANDARD (Feb. 20, 2018), https://perma.cc/Q5R5-X2EZ.

representative sample of survey subjects. While the use of what are typically referred to as "victimization surveys" cannot eliminate the so-called dark figure of crime – the amount of crime that remains unknown – it is clear that surveys have the potential to reduce that figure.[43]

Properly administered, surveys provide a less intimidating avenue of communication, one that is anonymous and quite different from interacting with law enforcement. Well-designed surveys can help us learn a lot about the criminal activity that people have experienced. Furthermore, when formulated appropriately, surveys can help us better understand what activities people consider to be criminal, and how people perceive law enforcement's response to such experiences. According to the late Finnish criminologist, Kauko Aromaa, at least 18 criminal policy objectives can be met or supported by victimization surveys, far more than can be listed here.[44] Notable among these are the potential to produce a much more accurate picture of the amount of crime, the context in which it occurs, the harm it causes, and how victims respond to it.[45]

In the US, the National Crime Victimization Survey (NCVS), first fielded in full in 1973, uses direct interviews with a carefully chosen sample of people and households to document their experiences with crime victimization.[46] Administered by BJS, the NCVS has been repeatedly improved over time, notably by the adoption of a modular approach to address new and emerging crimes – like identity theft – using supplemental surveys in addition to the main survey.[47]

Naturally, there is a cost associated with the use of surveys to measure crime. While the preparation of crime reports by law enforcement agencies is not free, it is reasonable to fund that activity from policing budgets. But surveys require a dedicated agency, staffed with professional statisticians. Sample sizes for surveys may need to be quite large if the rate at which a particular crime occurs is low. Historically, the funds required to maintain the NCVS have suffered from budgetary pressures, possibly because some lawmakers are not sufficiently aware of the benefits that these surveys provide.[48]

B. Challenges in Crime Reporting and Surveying

Fortunately, the challenges of crime reporting and surveying in the US have been comprehensively documented by the NMCS. Furthermore, this work was performed in the context of efforts to bring crime measurement up to the

[43] *See* Albert D Biderman & Albert J. Reiss Jr., *On exploring the" dark figure" of crime*, 374 ANNALS AM. ACAD. POL. & SOC. SCI. 1, 1-15 (1967), https://perma.cc/V8HP-CF67; Kauko Aromaa, *Victimisation Surveys–What Are They Good For?*, 15 TEMIDA 85, 88-90 (2012), https://perma.cc/J2QL-YBB3.

[44] Aromaa, *supra* note 43.

[45] *See id.*

[46] Fed. Bureau of Investigation, *supra* note 39.

[47] *See* Lynn Langton, Michael Planty & James P. Lynch, *The Second Major Redesign of the National Crime Victimization Survey (NCVS)*, 16 CRIMINOLOGY & PUB. POL'Y 1049, 1054 (2017).

[48] Pepper & Petrie, *supra* note 1 ("the problems may be growing worse because of eroding federal investment in data systems and social science research on crime and victimization.").

standards required to develop and administer effective information-based crime policy.[49] The two NMCS reports provide comprehensive analysis of the future of both SRS/NIBRS and NCVS. Specific issues with SRS/NIBRS are low levels of reporting,[50] delays in reporting,[51] lack of detail about the crimes reported,[52] and the limited number of crime types included.

The last of these limitations – the fact current reports are focused on traditional crimes like homicides, burglaries, motor vehicle thefts[53] – may seem the most salient to a discussion of cybercrime metrics, but an equally serious limitation is that they exclude some important categories of traditional crime. For example, there is a serious lack of data in either SRS/NIBRS or NCVS pertaining to either fraud or commercial victimization.[54] These two topics will be addressed after a quick look at the state of play in cybercrime metrics.

C. A Case Study in Cybercrime Metrics: Identity Theft

A cursory glance at the volume of internet search results for cybercrime metrics and related topics might suggest that there is no need to invest any more money in efforts to measure the scale and impact of cybercrime. For example, when people go looking for information about identity theft, they will find plenty of search results touting impressive numbers like: "in 2016 an estimated 26 million persons, or about 10% of all U.S. residents age 16 or older, reported that they had been victims of identity theft during the prior 12 months."[55] That statistic comes from an NCVS supplementary report, and that report does provide a large collection of solid survey-based metrics relating to identity theft, enabling a detailed view of the problem.

However, while the report is headline worthy – revealing that identity theft cost Americans $17 billion in 2016, possibly more than losses due to household burglary, motor vehicle theft, and property theft combined – it also highlights some potential limitations of victim surveys as a source of crime metrics. For a start, that report was not published until January of 2019, even though everyone knows that one of the most notable characteristics of cybercrime is the speed at

[49] *See* NMCS R2, *supra* note 10.

[50] In 2017 only 7,073 (42%) of the 18,855 U.S. law enforcement agencies submitted NIBRS-style data. *See* Gary Warner, *FBI's Crime Data Explorer: What the Numbers Say about Cybercrime*, SECURITY BOULEVARD (Sept. 30, 2018), https://perma.cc/GBF3-P3GF.

[51] The FBI reports the numbers to the public, principally in the annual Crime in the United States publication. This document typically appears about 10 months after the end of the calendar year, see NMCS R2 *supra* note 10, at 34. This means that the latest annual report available as of June, 2019 is *Crime in the United States, 2017*, FED. BUREAU OF INVESTIGATION (Sept. 24, 2018), https://perma.cc/5HKG-4T5C. Although semiannual updates are issued, see *Preliminary Semiannual Crime Statistics for 2018 Released*, FED. BUREAU OF INVESTIGATION (Feb. 25, 2019), https://perma.cc/HFJ6-7RMA.

[52] *See* Strom & Smith, *supra* note 4.

[53] *See* NMCS R1, *supra* note 10, at 37 box 2.1.

[54] *See* Langton, *supra* note 47, at 1053.

[55] ERIKA HARRELL, U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS, VICTIMS OF IDENTITY THEFT, 2016 (2019), https://perma.cc/Z34D-QN8M.

which it evolves.[56] So the practical value of knowing the state of identity theft in 2016, even in great detail, is open to question if that knowledge is not available for action and analysis until 2019. More questions are raised when you realize that the Google search, which found the 26 million number, also found this headline: "Identity Fraud Hit 15.4 Million US Victims in 2016."[57] Not only is this a much lower victim count for 2016, it is based on a report for 2016 published two years before the one from BJS.

Furthermore, the private sector entity that conducted the research behind the 15.4 million number for 2016 – Javelin Strategy & Research – has since conducted two more surveys, indicating that the victim count rose to 16.7 million in 2017, then fell to 14.4 million in 2018.[58] (These surveys are funded by a variety of commercial sponsors, and access to the data, which is tightly controlled, typically costs thousands of dollars.)

The apparent discrepancy between the two 2016 surveys, one from government and the other from the private sector, cannot be resolved by simply averaging them and assuming there were 20.7 million victims – statisticians would cringe at the idea. Further complicating the task of assessing the current scale of identity theft are other findings that point to even higher numbers. An independent 2018 survey of 2,500 internet-using adults in the US found that the percentage of respondents who had "experienced or been a victim of identity theft" was 31%.[59] That suggests far more Americans may be dealing with identity theft than either the BJS or Javelin surveys are identifying, but a lack of consistent survey language makes it hard to be sure.[60]

To be clear, this situation, of which similar examples can be found across the last three decades of cybercrime measurement, has serious implications for both public policy and commercial interests, not to mention the members of society who are seeking some relief from what is currently perceived as the most concerning of cybercrimes (47.5% of American adults responding to a 2018 survey said they were very concerned about experiencing or being a victim of identity theft, and only 13% were not concerned).[61]

III. AREAS OF CONCERN

If, as this paper argues, the way forward for cybercrime metrics is integration into established crime reporting and surveying mechanisms together with some additional specialized measurement infrastructure, then several areas of concern need to

[56] *See, e.g.*, John Leyden, *Ransomware Is So 2017, It's All Cryptomining Now Among The Script Kiddies*, REG. (July 12, 2018, 2:26 PM), https://perma.cc/DWR5-H4HQ.

[57] Ionut Arghire, *Identity Fraud Hit 15.4 Million US Victims in 2016: Report*, SECURITY WEEK (Feb. 2, 2017), https://perma.cc/8N4X-52C4.

[58] *See Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, https://perma.cc/UD2H-XU4M.

[59] Cobb, *Barometer USA*, *supra* note 13, at 7.

[60] *Id.* ("When they were asked 'how often have you experienced or been a victim of. . .identity theft (somebody stealing your personal data and impersonating you)?' less than two thirds replied 'never.'").

[61] *Id.*

be addressed, notably (A) the perception of computer crime as fraud and abuse, (B) the victimization of organizations, and (C) the accounting of harms caused by cybercrime.

A. Computer Crime as Fraud and Abuse

One of the reasons why our efforts to measure the extent to which the evolution of digital technology has enabled criminal activity have not fared well is the early adoption of the term "computer fraud and abuse." This phrase occupies a contentious place in the history of malfeasance associated with computers.[62] Memorialized by US lawmakers in the 1984 legislation known as the Computer Fraud and Abuse Act(CFAA) – a law that has arguably been enforced unevenly, and at times controversially[63] – computer fraud and abuse is a holdover from the infancy of computer crime terminology, a time when criminal law was still catching up to criminal reality.[64]

Unfortunately for those who took seriously the risk of criminals turning their attention to computers, "abuse" smacks of mischief rather than crime, and fraud is a category of crime that has not been taken seriously enough according to some criminologists. Levi and Burrows put it like this in a 2008 article on measuring the impact of fraud in the UK:

> It is by no means certain that governments, whether in Britain or elsewhere, really do want to devote resources to fraud, given that policing agencies are already 'full' with other politically prioritized tasks.[65]

The authors assert that this lack of government concern can result in *responsibilization* of the private sector to do its own policing, like the efforts that banks and payment card issuers make to not only reduce fraud but also to identify serious offenders and bring cases against them.[66] We have certainly seen commercial organizations operate as though defending against crime in cyberspace is their responsibility, initiating investigations of cybercriminals and working closely with law enforcement to take down purveyors and enablers of cybercrime, from bullet proof hosts to malware authors,[67] botnet operators,[68] and perpetrators of click fraud.

[62] *See, e.g*, John K. Taber, *A survey of computer crime studies*, 2 COMPUTER L.J. 275, 289 (1980).

[63] *See* Melissa Anne Springer, *Social Media and Federal Prosecution: A Circuit Split on Cybercrime and the Interpretation of the Computer Fraud and Abuse Act*, 86 U. CIN. L. REV. 315, 315-335 (2018).

[64] One of the first professional researchers of computer crime was Don Parker, but because his employer at the time would not let him use that term, he settled on computer abuse. Thus began the tendency to align computer crime with the "soft crime" of abuse. *See* DON B. PARKER, CRIME BY COMPUTER 298 (1976).

[65] *See* Michael Levi & John Burrows, *Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey*, 48 BRIT. J. CRIMINOLOGY 293 (2008).

[66] *Id.* at 298.

[67] Marc-Etienne M.Léveillé, *ESET Research Team Assists FBI in Windigo Case – Russian Citizen Sentenced to 46 Months*, WE LIVE SECURITY (OCT. 30, 2017, 11:59 AM), https://perma.cc/MD3K-BX47.

[68] Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J. L. & TECH. 237, 246 (2014).

The fact that some fraud schemes – in both meatspace and cyberspace – can be so complex that expert knowledge is required to investigate them is another potential barrier to law enforcement engagement. Producing useful metrics on such crimes requires considerable commitment and enthusiasm from those who set policy and priorities, possibly more than crime measurement programs currently enjoy.

B. The Victimization of Organizations

One common characteristic of SRS/NIBRS and NCVS is that they are focused on crimes against people, not crimes against commercial organizations. Yet these organizations are owned and staffed by people (and those people have a direct interest in the security of the organization). This reflects a longstanding bias among criminologists, and efforts to redress this bias are a relatively recent development in criminological research.[69]

The attention paid to commercial victims was initially focused on the retail sector where a certain amount of theft of goods – either by customers or employees – has long been factored into the cost of doing business as "shrinkage."[70] This is another example of responsibilization, an industry taking upon itself many aspects of law enforcement, including gathering crime metrics.[71] While the retail industry in the US has made considerable progress in refining those metrics in recent years,[72] the fact remains that shrinkage includes criminality, the scale and impact of which is largely unknown to the public, its societal impact arguably under-estimated by policymakers.

The reporting of organizational victimization is further complicated by sensitivity to reputational damage. This can occur if the public thinks the organization could or should have done a better job of protecting its interests and those of its customers, employees, or investors. Fear of reputational damage is particularly problematic in the case of data breaches, denial of service attacks, and ransomware incidents. These events may not come to light unless there are regulatory reporting requirements in place, or a third party is impacted (for example a customer or supplier).

Despite these challenges, it is feasible to survey organizations to gather metrics on their experience of cybercriminal activity. In 2005, BJS conducted a survey of 7,818 businesses called the Cybercrime Against Businesses.[73] Sadly, the funds to repeat this study were not forthcoming, leaving BJS in the embarrassing position of referring requests for business cybercrime metrics to commercial reports.[74]

[69] Hopkins, s*upra* note 38, at 413.

[70] ADRIAN BECK, NEW LOSS PREVENTION: REDEFINING SHRINKAGE MANAGEMENT 27 (2009).

[71] NMCS R2, *supra* note 10, at 199.

[72] *See* ADRIAN BECK, RETAIL INDUS. LEADERS ASS'N, BEYOND SHRINKAGE: INTRODUCING TOTAL RETAIL LOSS (2016).

[73] RAMONA RANTALA, BUREAU OF JUSTICE STATISTICS, CYBERIME AGAINST BUSINESSES, 2005 (2008), https://perma.cc/PT83-5NPE.

[74] Stephen Cobb, *Sizing Cybercrime*, *supra* note 8.

However, other countries offer hope that governments may yet be persuaded to step up to the challenge of measuring cybercrime's impact on companies. The UK produced studies in 2017 and 2019, enabling measurement of changes over time.[75] Canada has done similar work.[76] In 2018, Belgian authorities produced a highly detailed study of harms caused by cybercrime.[77]

C. Accounting for Cybercrime Harms

One of the clearest statements of why cybercrime needs to be "mapped and measured" emerged from a forum of experts convened at the Oxford Internet Institute (OII) in 2010. They produced the following list of reasons: inform crime reduction initiatives; enhance local and national responses; identify gaps in response; provide intelligence and risk assessment; identify preventative measures; facilitate reporting; educate and inform the public; and identify areas for further research.[78]

To that list should be added "measuring the harm caused by cybercrime." In fairness to the OII forum it did address harm reduction, arguably a higher goal than crime reduction (a priority reflected in law enforcement policy in several countries).[79] When it comes to cybercrime, assessing the harm it causes is particularly important because the mechanisms by which that harm is inflicted are so very different from those of pre-computer crimes like robbery, burglary, assault, and so on. Cybercrime typically involves no physical interaction between perpetrator and victim[80] and no risk of physical harm to any of the parties involved. Nevertheless, cybercrimes can inflict emotional pain as well as financial loss, on multiple parties, at scale.[81]

Of course, crime rates, such as the number of times online banking credentials are compromised by criminals, are very important. Quickly identifying and reporting changes in patterns of the cybercriminal activity enables institutions and individuals to be more effective defenders of their digital domains. However, a country that cannot document the amount of pain endured by victims who, for example, lost their cherished family photographs to malware or their lifesavings

[75] REBECCA KHLAR ET AL., UK DEP'T FOR CULTURE, MEDIA & SPORT, CYBER SECURITY BREACHES SURVEY, 2017: MAIN REPORT (2017), https://perma.cc/3N39-FLCU; *see also* RISHI VALDYA, UK DEP'T FOR CULTURE, MEDIA & SPORT, CYBER SECURITY BREACHES SURVEY, 2019: MAIN REPORT (2019), https://perma.cc/CMX5-DJ6J.

[76] *See, e.g.*, *Impact of Cybercrime on Canadian businesses, 2017*, STAT. CANADA (Oct. 15, 2018, 8:30 AM), https://perma.cc/5QZJ-DS5S.

[77] LETIZIA PAOLI ET AL., BELGIAN SCIENCE POLICY OFFICE, BELGIAN COST OF CYBERCRIME: MEASURING COST AND IMPACT OF CYBERCRIME IN BELGIUM 18 (2018) [hereinafter BELGIAN COST OF CYBERCRIME], https://perma.cc/W37V-LWRZ.

[78] STEFAN FAFINSKI ET AL., OXFORD INTERNET INSTITUTE, MAPPING AND MEASURING CYBERCRIME 4 (2010), https://perma.cc/8GQQ-2WGQ.

[79] *See, e.g.*, Memorandum submitted by the UK Serious Organised Crime Agency (Mar. 3, 2010), https://perma.cc/3EGT-SRYJ ("The overarching aim of the [Organised Crime] Control Strategy is to achieve a tangible and lasting reduction in the harm caused to the UK by organised crime.").

[80] *See* Brenner, *supra* note 2, at 6.

[81] David Modic & Ross Anderson, *It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud*, 13 IEEE SECURITY & PRIVACY 99, 99-103 (2015).

to an online scam, may have a hard time providing its citizens with appropriate levels of cybercrime prevention, deterrence, response, and recovery.

Sociologists like Modic have made a strong case that individuals victimized by cybercrime experience emotional harms.[82] Solove and Citron have articulated a sound theory of data breach harm.[83] There are also solid grounds for thinking that cybercrime can cause systemic harm, [84] with unrestrained cybercrime posing a serious threat to modern economies. Consider the economic impact if rising fears of cybercrime caused a 20% drop in consumer use of digital devices for commercial purposes (online banking, bill payment, shopping, travel booking, ride sharing, advertising, and so on). Research suggests this scenario is not far-fetched. Several surveys indicated that as many of 20% of Americans cut back their online activity in response to the Snowden revelations about secret digital surveillance.[85] Reduced online activity in response to cybercrime has been detected by surveys in the US,[86] Canada,[87] Belgium[88], and across the EU.[89]

IV. MOVING FORWARD

The challenge facing those who believe that better cybercrime metrics are essential to the cyber enforcement effort is not simply the need to add new categories of data reporting and surveying to current crime measurement tools. Those tools are already in need of an overhaul. As the NMCS study proclaimed:

> Improvement in the nation's crime statistics will require enhancements to and expansions of the current data collections, as well as new data collection systems for the historically neglected crime types highlighted by the proposed crime classification.[90]

Fraud in its many forms is one of those neglected types, as are crimes against companies, and cybercrimes of all kinds. The good news here is that the push for cybercrime metrics may be able to leverage proposals for a broader overhaul of crime measurement capabilities. This possibility will be examined in more detail after a brief discussion of current sources of cybercrime metrics.

[82] *Id.*

[83] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 747-73 (2018).

[84] *See* Brenner, *supra* note 2, at 24.

[85] Stephen Cobb, *Privacy and Security Post-Snowden: Pew Research Parallels ESET Findings*, WE LIVE SECURITY (Nov. 17, 2014), https://perma.cc/2FWL-9LFG.

[86] Cobb, *Barometer USA*, *supra* note 13.

[87] Stephen Cobb, *ESET Cybersecurity Barometer Canada* 2018, WE LIVE SECURITY (2018), https://perma.cc/H5BY-CXMT.

[88] *See, e.g.*, BELGIAN COST OF CYBERCRIME, *supra* note 77.

[89] EUROPEAN COMM'N, *supra* note 13, at 480.

[90] NMCS R2, *supra* note 10, at 27.

A. *Where are Cybercrime Metrics Today?*

The sources and methods of current cybercrime metrics are diagrammed in Table 4. There are two main methodologies: crimes reported to a designated entity (Reported) and crimes discovered by surveying victims (Surveyed). The sources of crime metrics can be grouped into five categories: Law Enforcement, Government, Private Sector, NGO, and Academia. For each method-source pair there are two victim types: consumer (C) and business (B).

Table 4: Crime metrics sources, methods, victim types

	Reported		**Surveyed**	
Law enforcement	C	B	C	B
Government agencies	C	B	C	B
Private sector	C	B	C	B
NGOs	C	B	C	B
Academia	C	B	C	B

An example of research that references multiple cybercrime metrics is the previously cited series of two articles by Anderson et al. presented at WEIS, the Workshop on the Economics of Information Security. The first appeared in 2012 and broke new ground as an attempt to answer the question of how you measure the cost of cybercrime cost in an academically rigorous manner.[91] Part of the motivation for this significant undertaking was the shortcomings of previous attempts to answer that question,[92] particularly those made by commercial entities such as the purveyors of cybersecurity products and services.[93]

In 2019, Anderson et al. provided a significant update in their study, "Measuring the Changing Cost of Cybercrime."[94] This included a critique of new sources such as the US NCVS identity theft supplement and the UK Office for National Statistics report on crime in England and Wales that has been expanded to include some cybercrimes. While the authors welcomed the increase in cybercrime victimization studies between 2012 and 2019 – including those from Australia,[95] Belgium,[96] France, and the EU[97] – the continuing lack of consistent

[91] Anderson, *Measuring the Cost 2012*, *supra* note 8.

[92] *See* Cobb, *Sizing Cybercrime*, *supra* note 8.

[93] *See, e.g.*, D. FLORÊNCIO & C. HERLEY, *Sex, lies and cyber-crime surveys*, *in* ECONOMICS OF INFORMATION SECURITY AND PRIVACY III (Springer ed., 2013).

[94] Anderson, *Measuring the Cost 2019*, *supra* note 5.

[95] Susan Goldsmid et al., *Identity Crime and Misuse in Australia: Results of the 2017 Online Survey*, AUSTRALIAN INST. CRIMINOLOGY STAT. REPORT 11. (Dec. 30, 2018), https://perma.cc/8XP4-6Z47.

[96] BELGIAN COST OF CYBERCRIME, *supra* note 77.

terminology and methodology makes aggregation and analysis of such studies challenging at best.

While most of the cited sources were government funded, the authors referenced several commercial sources as well. However, they eschewed the Verizon Data Breach Investigations Report and numerous studies from the Ponemon Institute, two sources that have frequently addressed the scale and cost of cybercrime's impact on organizations, as have PwC and other large vendors of IT security services, and security product vendors such as Cisco, Fireye, ESET, and McAfee. This reflects an unfortunate disconnect between academia and those who are actively engaged in defending information systems against criminal actors. This is partly due to theoretical doubts about the economic value of security products,[98] but also an historical skepticism toward crime statistics published by purveyors of such products.[99]

Some private sector studies of data breaches and other assaults on the security of information systems at the organizational level have, in recent years, improved in terms of statistical rigor and more prominent caveats regarding the interpretation and use of their findings. However, some industry statistics are still undermined by non-standard terminology, small sample sizes, and the perception – often accurate – that their primary raison d'etre is something other than supporting law enforcement efforts. That said, cybersecurity firms have the potential to be a great source of cybercrime metrics, as discussed in section IV(B).

B. A Promising Path Forward

Whether seeking to measure the scale of cybercrime or its impact on victims – individually or at large – the most expeditious path to better cybercrime metrics could well be adaptation of the existing machinery of crime measurement, namely the reporting and surveying programs used by many governments. However, to track the full range of criminal activity, cyber and non-cyber, more is needed, namely a comprehensive overhaul of how governments perform crime measurement, starting with a uniform approach to crime classification. This would enable differential analysis of crime trends at the regional, national, and international levels. To this end, NMCS has advocated basing a revised US classification system on the International Classification of Crime for Statistical Purposes (ICCS), a framework developed and maintained by the United Nations Office on Drugs and Crime (UNODC).[100] The NMCS panel of experts concluded

[97] Markus Riek et al., *Estimating the Costs of Consumer-Facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries*, *in* WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (2016), https://perma.cc/FD5S-ZNNA.

[98] William Jackson, *Study: Spend Less on Antivirus, More on Catching Cyber Crooks*, GCN (June 18, 2012), https://perma.cc/FF5G-5QAN. When it comes to preventing cybercrime, the medicine might be worse than the diseases, according to a new study led by Cambridge University. *Id.*

[99] *See* Julie J.C.H Ryan & Theresa I. Jefferson, *The Use, Misuse and Abuse of Statistics in Information Security Research* (Am. Soc'y for Engineering Mgmt., Working Paper, 2003).

[100] *See generally* UNITED NATIONS OFFICE ON DRUGS AND CRIMES, INTERNATIONAL CLASSIFICATION OF CRIME FOR STATISTICAL PURPOSES (2015), https://perma.cc/28P5-48H2.

that this framework, "meets the desired criteria for a modern crime classification," and that "the use of shared, international frameworks enables studies of transjurisdictional and locationless crime."[101]

In addition to improved crime classification, the US also needs, according to the second NMCS report, "enhancements to and expansions of the current data collections, as well as new data collection systems for the historically neglected crime types highlighted by the proposed crime classification."[102] The report envisions "a new crime data infrastructure" consisting of three main components: incident-based reporting; a survey data component; and "crime measurement clearinghouse function," used to address "new crime types that are outside the scope of either police-report or household survey methods."[103] These three components – and a possible fourth element – will now be discussed.

1. Incident-based Reporting

The NMCS reports see great value in an improved incident-based recording system that covers offenses known to law enforcement agencies. Central to the proposed improvement, which would leverage the exiting SRS/NIBRS infrastructure, is a revised classification of crime for statistical purposes. This classification was solidified by the first NMCS report and is based on criminal actions rather than the means by which they are committed.[104] This means that where cybercrimes are included – and happily many are – they are not a first-level category. For example, identity theft appears in Category 7 under the title *Acts involving fraud*.[105] The expectation is that data about criminal acts counted in this category will include details of how the crime was carried out.

However, acts against computer systems do get a second level entry in Category 5, *Acts against property only*. There we find section 5.3 *Acts against computer systems*. This section is divided into four sub-sections, as shown in Table 5.

Table 5: NMCS's proposed "Acts against computer systems"

5.3.1	Unlawful access to a computer system
5.3.2	Unlawful interference with a computer system or computer data
5.3.2.1	Unlawful interference with a computer system
5.3.2.2	Unlawful interference with computer data
5.3.3	Unlawful interception or access of computer data

[101] NMCS R2, *supra* note 10, at 124.

[102] *Id*. at 39.

[103] *Id*.

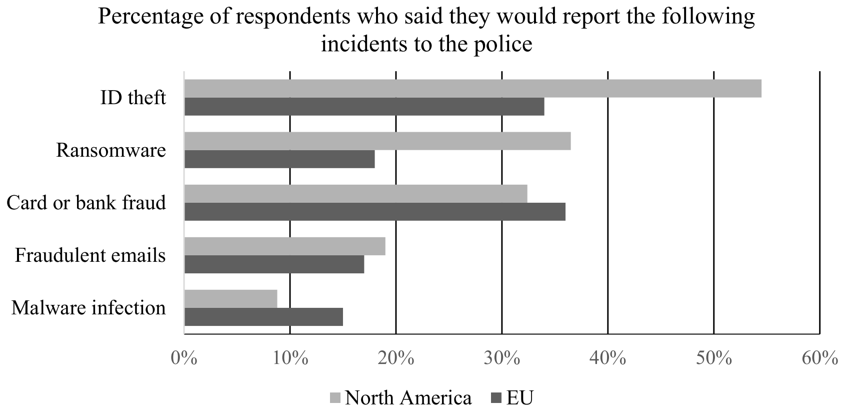
[104] *Id*. at 117.

[105] *Id*. at 126.

The NMCS approach to crime reporting, if fully implemented, has much to recommend it and would greatly improve America's ability to measure the scale of cybercriminal activity impacting Americans. Unfortunately, as past efforts to improve SRS/NIBRS have shown, full implementation of crime reporting requires an appropriate allocation of resources. Conversely, lack of funding contributes to a lack of participation, as evidenced in an article describing 2017 information about SRS/NIBRS, released in 2018, which asserts that "of the 18,855 law enforcement agencies in the United States, 16,207 of them submitted SRS "old-style" UCR data. Only 7,073 (42%) submitted NIBRS-style data."[106]

The article also notes that SRS/NIBRS reports have yet to include many cybercrime numbers. This may be due to resource constraints or lack of police engagement with cybercrime – as the research charted in Figure 2 suggests, with the exception of identity theft, most do not see the police as a source of help when they encounter cybercrime. While anecdotal evidence suggests that some law enforcement agencies are working to improve the level of cybercrime reporting by the public,[107] a more concerted effort is clearly needed. There is also room for innovation in this regard, as shown by the emerging use in the US of the 211 phone number as a cybercrime victim support line, as described in section IV(C).

Figure 2: Cybercrime reporting levels



2. Expanded Surveying

The second component of the three-pronged overhaul of crime measurement proposed by NMCS is the use of surveys, principally the National Crime Victimization Survey (NCVS) and its topic-specific supplements. As noted in section II(A), this "supplemental" approach has already produced useful

[106] Warner, *supra* note 50.

[107] The U.S. Secret Service encouraged businesses to report cybercrimes during several events in 2019 attended by the author as a member of the Southern California Electronic Crimes Task Force.

"official" metrics on identity theft. NCVS surveys addressing cybercrimes would deliver substantial benefits in policymaking because they cannot be dismissed or undercut with claims of commercial bias and are freely available to academic researchers and members of the public. However, the number of surveys, the breadth of their sampling, and the timeliness of their results, are all dependent upon BJS' funding, which would have to be increased substantially from current levels.

3. Crime Measurement Clearinghouse Function

The third part of the NMCS strategy goes beyond enhancing and evolving traditional reporting and surveying of crime to propose a crime measurement clearinghouse function. The goal is to aggregate a variety of "primarily administrative-record-type data sources."[108] You need look no further than the review of current cybercrime metrics in section IV(A) to see that there are numerous sources which match that description, and so it is heartening that NMCS acknowledged that "there are many crime offense types for which neither police-report data nor survey data are apt or workable as a source of offense counts and characteristics."[109]

A primary goal of the proposed clearinghouse is to measure new crime types that are outside the scope of either police reports or household crime surveys, for example "crimes against governments and businesses that are not specifically spatial in a way that is linked to a local police jurisdiction."[110] Clearly that includes crimes committed in cyberspace and useful sources of government data at the federal level include the Securities and Exchange Commission, the Federal Trade Commission, Health and Human Services, the Internet Crime Complaint Center (IC3), and the Federal Communications Commission. State level data might include data breach notifications. According to NMCS, the intent is "not simply to link or refer to external data but to actively assimilate them within national crime statistics".[111]

If successfully executed, the clearinghouse, and the reports that it would be able to publish, could prove very helpful to domestic policymakers, especially those who prefer to make decisions based on a centralized, trusted source of reviewed and verified data. Scholars, consumers, and private companies, would also benefit, as would other countries of the world, if the U.S. government adopts the internationally recognized framework of crime classification recommended by NCMS. Of course, this will all take time and resources, as NCMS openly acknowledges: "overcoming the procedural/implementation difficulties will require great effort."[112]

[108] NMCS R2, *supra* note 10, at 8.

[109] *Id.*

[110] *Id.*

[111] *Id.* at 45.

[112] *Id.* at 46.

4. The Fourth Element

Unfortunately, the proposed crime data clearinghouse that forms the third prong of the NCMS recommendations does not adequately address one source of highly useful cybercrime data: the cybersecurity industry. However, the potential for specific industries to bolster crime metrics does receive some attention in Appendix D of the second NMCS report which notes, "it is likely that a fourth option involving the cultivation of 'safe havens' for information sharing between organizations may need to be developed."[113] This realization came from the project's exploration of shrinkage, which observed that, "collecting data on crimes affecting businesses largely amounts to trying to achieve information sharing in a culture where information sharing is anathema."[114]

Ironically, the report goes on to suggest that, "one possible model here is the National Cyber-Forensics and Training Alliance (NCFTA),"[115] the irony being that the cybersecurity industry as a whole differs from most others in that it already shares vast amounts of information (for example: malware samples, known bad websites, phishing emails, indicators of compromise, and domain name algorithms). This information sharing makes possible the near-real-time updating of our digital devices to prevent us clicking on a malicious link in an email or visiting a booby-trapped website, regardless of who made the device, or email app, or browser. Companies that offer "endpoint protection" products constantly receive data about potentially criminal activity from millions of endpoints around the world. Furthermore, they receive thousands of calls a day from customers who are experiencing cybercrime.

If properly managed, the NMCS suggestion of an independent "safe haven" for such data, from which cybercrime metrics could be derived, has the potential to significantly increase the grasp that policy makers have on the scale and complexity of cybercriminal activity. For example, they may better understand how even the largest purveyors of technology, companies like Google and Microsoft, can be repeatedly wrong-footed by the speed and technical skill with which vulnerabilities in their products and services are exploited by cybercriminals.

C. Victim Assistance as Data Source

When members of the public are victimized by cybercriminals, they often feel there is nowhere to turn for help. A new NGO-driven program being rolled out in the US aims to change that while also addressing the underreporting of cybercrime to the police. In 2018, a non-profit organization called Cybercrime Support Network (CSN) began working to offer cybercrime victims an alternative to 911, the emergency response phone number. Many people are reluctant to call 911 when they experience a crime that does

[113] *Id.* at 181.
[114] *Id.* at 180.
[115] *Id.* at 181.

not involve physical danger to themselves or others (or about which they think the police will do very little).[116]

CSN is a public-private collaboration created "to meet the challenges facing millions of individuals and businesses affected each and every day by cybercrime." The organization is enabling 211 to operate as a source of assistance to cybercrime victims (most 211 centers in the US are locally operated or funded by United Ways).[117] This extension of the 211 service will not only help people deal with cybercrime incidents, it will provide a fresh source of cybercrime metrics as well as funnel cases to law enforcement as appropriate. Right now, 211 is taking calls from cybercrime victims in several states and plans to be nationwide as soon as funding permits. A website called FraudSupport.org will supplement the support for cybercrime victims offered via 211 and "lead cybercrime victims through the Report, Recover and Reinforce process after an incident occurs."

V. Discussion: Promise, Problems, and Affordability

The parlous state of cybercrime metrics is a serious hindrance to developing a meaningful enforcement strategy against cybercriminals. While the US government has, in recent years, taken some substantial steps toward securing better crime metrics in general and has begun to report some meaningful cybercrime metrics (such as the NCVS identity theft surveys), much more needs to be done – and at much greater speed than we have seen so far – if the seemingly relentless progression of cybercrime is to be stalled, let alone reversed.

A. The Promise of NMCS

The NMCS project to determine the best path towards better measurement of crime was commissioned by BJS and FBI at a time when the shortcomings of cybercrime metrics were already being documented, as were the deficiencies of SRS/NIBRS and NCVS. In other words, the problems were recognized and the need for significant improvements across all crime metrics was widely accepted when the US government prompted the NMCS reports. Those reports offer a thoroughly researched vehicle which, with appropriate input, could deliver much better cybercrime metrics than we have today.

Leveraging the NMCS recommendations may be the best way for advocates of improved cybercrime metrics to gain traction. Given the flexibility of the three-plus-one approach proposed by NMCS, it should, if put into practice, provide comprehensive and "official" data on all the major forms of cybercriminal activity.

[116] *See, e.g.*, Taryn Porter, *CybercrimeStories – Giving Victims a Voice*, CYBERCRIME SUPPORT NETWORK (Nov. 5, 2019), https://perma.cc/96WV-VMAC.

[117] In 2000, the United Way organization and other non-profits running local helplines persuaded the FCC to make 211 a dedicated number for people "in need of local information and resources." *See Dial 211 for Essential Community Services*, FED. COMMC'NS COMM'N (Oct. 20, 2017), (last visited on Dec. 27, 2019), https://perma.cc/7YKJ-9DNG.

B. What is Missing?

Currently lacking is any certainty that NCMS recommendations will be fully endorsed or funded by the current administration. According to Janet Lauritsen, a leading NCMS contributor, the first NMCS report, delivered in 2016, was well received. However, the second report, delivered in 2018, was not – in her opinion – met with equal enthusiasm.[118] She cites staff reductions at BJS as an indicator that crime metrics are not an administration priority.

Unless and until government makes crime metrics a priority, the quest for more accurate and objective cybercrime metrics faces an even tougher challenge than sorting out the logistics of obtaining and analyzing cybercrime data. From both operational and professional perspectives, the NMCS proposals offer the US a clear path forward, so at this point in time the quest for trusted and timely cybercrime metrics faces good news and bad. The good news is that such metrics are attainable if enough of the right questions are asked of a sufficient number of people and the answers are processed in a short enough period of time. The bad news is that many politicians will consider the cost of that undertaking to be too high. Fortunately, it is possible that those politicians could be persuaded to see things differently by the people who believe that trusted and timely cybercrime metrics are a vital part of the cybercrime reduction effort.

C. Affordability

The question of "affordability" of improved cybercrime metrics can be met head on by arguing that (a) significant and documented reduction in cybercrime is impossible without better metrics, (b) the benefits of reducing cybercrime are demonstrably large, (c) the opportunity costs of not reducing cybercrime are potentially huge, and (d) some of the options for funding the necessary improvements to cybercrime metrics could be relatively painless.

Solid research exists to back all four parts of this argument, starting with the 800 pages of the combined NMCS reports. The benefits of a permanent global reduction in the levels of criminal activity in cyberspace would seem to be obvious but they can be spelled out. Realistic aggregated opportunity costs can be calculated from available data. While a detailed consideration of funding options for a worldwide program to improve cybercrime metrics is beyond the scope of this paper, several come to mind.

1. Taxing Domain Names

A global effort to improve cybercrime metrics could be funded to the tune of well over $300 million if a $1 fee was levied once per registered domain name. An annual revenue stream of equal amount could be created by making that $1 an annual tax. To put this in perspective, the author estimates that the annual spend

[118] Author's personal communications with Lauritsen, May 21, 2019.

on gathering and reporting crime statistics by the US government has never topped $80 million even at the height of support from the Obama administration.

2. Tax Breaks for Corporate Support

The erosion of trust in digital technology puts at risk the welfare of many corporations, not just the obvious ones like Google, Facebook, Apple, and Amazon. Technology companies would benefit greatly if they funded a trusted source of cybercrime metrics. Tax breaks for such funding would seem to be an appropriate mechanism, provided donors agreed to keep their distance from decisions about how the funds are used.

3. Tax Breaks for Data Donations

The "safe haven" concept of sharing cybercrime-related information outlined in section IV(B)(4) could be bootstrapped through tax breaks for commercial entities that contribute data. As noted earlier, information-sharing is not new to cybersecurity companies, and the technical challenges that a safe haven would face are not insurmountable.

VI. Limitations and Omissions

Measuring cybercrime is a large and sprawling topic. For practical reasons this paper has focused on a portion of the problem: the need to measure property and financial crimes committed in cyberspace and/or by means of computer networks. In doing so, the paper has neglected discussion of several important criminal abuses of information and communication technologies (ICTs), such as to bully and harass at risk persons, generate and purvey child pornography, conduct disinformation campaigns, and carry out nation state espionage. These are serious problems for our society today and they do need to be measured and deterred.

The paper is also US-centric but has benefited greatly from non-US sources. Furthermore, the importance of international cooperation on cybercrime metrics was frequently noted, as was the international alignment on crime classification proposed by NMCS. As the original developer of much of the technology that is currently abused by cybercriminals, the US has a responsibility to provide leadership in cybercrime measurement as well as deterrence. And US politicians would do well to bear in mind that not all cybercrime comes from other countries. Plenty of digital malfeasance targeting Americans is home grown and in dire need of serious deterrence.

Conclusion

Meaningful action on crime measurement in general, and cybercrime metrics in particular, will require the generation – through public pressure and the democratic process – of a considerable amount of political will. If this will can be generated, then there is room for optimism to accompany the solid body of research that already exists to guide the way forward.

Surveys show that most internet-using American adults think that cybercrime is bad for the country, its economy, and themselves. A sizeable majority believes that the risk of becoming a victim of cybercrime is increasing and less than half think that the police and other law enforcement authorities are doing enough to fight cybercrime. There appears to be broad consensus – among consumers and across companies, governments, NGOs, and the academies – that serious improvements in cyber enforcement are needed. The view of many technologists, economists, and experts in criminal justice and law enforcement is that accurate and objective cybercrime metrics have a vital role to play in justifying and documenting the making of those improvements.

In 2013, Ross Anderson, lead author of the WEIS studies on measuring the cost of cybercrime, remarked, "Stop wasting money on measuring cybercrime. . . spend it on the police instead."[119] Hopefully, this paper has made a strong case for saying that money spent on measuring cybercrime is not wasted. Further, it is hoped that the research presented here will bolster efforts to generate the political resolve necessary to adequately fund both the policing of cyberspace and the improvements in cybercrime measurement that are needed to guide and manage the essential work of cybercrime deterrence. Fortunately, the data we already have is enough to know that if this work is not done, the cost to society could be far more than any money saved by not doing it.

[119] Paul Hyman, *Cybercrime: It's Serious, but Exactly How Serious?*, 56 COMMC'NS OF THE ACM 18, 18–20 (2013), https://perma.cc/6MTP-AW89.