This report was prepared by RTI International using federal funding provided by the Bureau of Justice Statistics.

Document Title:	An Environmental Scan of Cybercrime Measurement: Recommendations for the National Crime Victimization Survey
Authors:	Julia Brinton, RTI International Lynn Langton, PhD, RTI International Christopher Krebs, PhD, RTI International Michelle Casper, RTI International
BJS Project Manager:	Heather Brotsos, Chief of Victimization Statistics
Document No.:	NCJ 306766
Publication Date:	August 2023
Award No.:	This project was supported by award number 2017-MU-MU-K048.

Abstract:

This report is an environmental scan of information on the types, definitions, and measurement of cybercrime and provides recommendations for potential revisions to the National Crime Victimization Survey (NCVS) that would broaden the NCVS's ability to capture cybercrime victimization. The report presents research, evidence, and recommendations regarding (1) existing cybercrime classifications/taxonomies, definitions, and measures (including state and federal laws and classifications from the International Classification of Crime for Statistical Purposes and the National Academies of Sciences, Engineering, and Medicine); (2) the existing measurement of cybercrime in the NCVS and a detailed comparison to the comprehensive cybercrime classification system by K. Phillips and colleagues (2022); and (3) recommendations for revision to the measurement of cybercrime in the NCVS.

This page intentionally left blank.

National Victimization Statistical Support Program (NVSSP)
Cooperative Agreement (COA) 2017-MU-MU-K048
RTI Project Number: 0217713

An Environmental Scan of Cybercrime Measurement: Recommendations for the National Crime Victimization Survey

August 2023

Prepared for
Bureau of Justice Statistics
810 Seventh Street, NW
Washington, DC 20001

Prepared by
Julia Brinton
Lynn Langton, PhD
Christopher Krebs, PhD
Michelle Casper

RTI International
3040 E. Cornwallis Road
Post Office Box 12194
Research Triangle Park, NC 27709-2194

Contents

Figures

Number **Page**

This page intentionally left blank.

Executive Summary

The Better Cybercrime Metrics Act directs the Bureau of Justice Statistics (BJS), in coordination with the Bureau of the Census, to include questions relating to cybercrime victimization on the National Crime Victimization Survey (NCVS). This report, developed through a cooperative agreement between the Bureau of Justice Statistics (BJS) and RTI International, provides an environmental scan of existing definitions and measures, federal and state laws, and the extant literature on the topic of cybercrime and cyber-enabled crimes in an effort to determine if and how the NCVS could expand and improve measurement of cybercrime; the additional questions or crime types that would need to be added to the core survey or supplements to generate national estimates; and how BJS should proceed with testing and adding additional measures.

Although cybercrime has existed and been studied for decades, there is no currently agreed-upon definition or taxonomy of cybercrime in the empirical literature, in the educational and governmental classifications systems, or even in legislation (no jurisdiction has a single agreed-upon definition of cybercrime). Classification systems approach cybercrime based on the method that was used to commit the crime, while federal and state laws approach cybercrime based on the level of harassment to the victim. The seemingly conflicting approaches regarding how to define and classify cybercrime are reflected in the massive amount of theoretical and empirical research on cybercrime against persons and/or institutions. Researchers have attempted to mitigate this issue by suggesting various taxonomies for organizing and classifying cybercrime. However, the speed at which cybercrime is evolving, coupled with the variability in terminology and inconsistencies across legislation, has made this difficult and resulted in multiple organizing frameworks. In recent years, researchers have begun exploring a taxonomical approach to classifying cybercrime. This approach allows for the categorization of various types of cybercrime without getting hindered by terminologies.

A comprehensive meta-analysis revealed a complete and thorough taxonomy by Phillips and colleagues (2022). Phillips and colleagues' (2022) taxonomy incorporates previous classification and taxonomy approaches while also incorporating the Council of Europe's Convention of Cybercrime definition, widely recognized as "the only globally recognized agreement around cybercrime." The authors of this report used Phillips and colleagues' taxonomy as a basis for comparison to the existing NCVS.

Although the NCVS covers a broad range of crime victimization types, it does not systematically assess victimization experiences committed via cyber-enabled means compared to victimization experiences committed in person or measure crimes that can only be committed via cyber means. This report describes cybercrime types from the taxonomy and identifies whether they are already being measured through the NCVS either partially or fully. For those covered only partially, this report discusses how they are currently being measured and any recommended revisions for expanding the scope of those measures. Relevant state or federal laws relating to the crime type are also referenced. The report also details crimes from the taxonomy that are not currently assessed in the NCVS, but that should be considered for inclusion in future iterations. The report details crimes from the taxonomy not currently assessed in the NCVS and not recommended for inclusion in future iterations because they are out of scope for the NCVS.

In addition to examining cybercrime types collected through the NCVS, this report presents recommendations on whether estimates should be presented individually by cybercrime type or aggregately as a composite measure that reflects total cybercrime victimization.

A measure could be created through (1) the development of a single survey question, or a short series of questions, used to generate a single estimate of cybercrime, or (2) by aggregating across multiple cyber-related measures as is done to create composite measures for violent and property crime. However, there are several challenges with this approach. These include, but are not limited to, the following:

- The range of victimization experiences included under the heading of cybercrime is diverse enough that it might be difficult to effectively define the various crime types in the context of one question or a few questions.
- The ages of focus for the cybercrime types vary (i.e., cyberbullying is currently measured for persons 12-18; identity theft is only asked of people 16 or older).
- Some cybercrime types overlap or could occur in the context of the same incident (cyber fraud and forgery; stalking and nonconsensual porn), but there would not be a way to parse this out to the same extent the NCVS does this currently.
- The NCVS supplements, some of which cover certain cybercrime types, have different reference periods than the core NCVS, focus on producing prevalence rates rather than incident rates, do not have a bounding adjustment, have different rules related to proxy respondents, and have different weights.
- Finally, defining and measuring incidents will be especially challenging because it is hard to determine the start/stop of cybercrime victimization types. For that reason, it is recommended that BJS focus on measuring prevalence only.

These differences make combining estimates from the supplements and core somewhat problematic. We recommend that BJS focus on measuring individual types of cybercrime, rather than an aggregate or composite approach.

An Environmental Scan of Cybercrime Measurement

1 Introduction

On May 5, 2022, President Biden signed S. 2629, the Better Cybercrime Metrics Act[1], which directs the Bureau of Justice Statistics (BJS), in coordination with the Bureau of the Census, to include questions relating to cybercrime victimization in the National Crime Victimization Survey (NCVS). In response, RTI International, in collaboration with BJS, has undertaken an environmental scan of existing measures, federal and state laws, and the extant literature on the topic of cybercrime and cyber-enabled crimes in an effort to determine if and how the NCVS could expand and improve how it goes about measuring cybercrime, the additional questions or crime types that would need to be added to the core survey or supplements to generate national estimates, and how BJS should proceed with testing and adding additional measures. This report provides (1) an overview of existing cybercrime taxonomies, definitions, and measures (including state and federal laws and classifications from the International Classification of Crime for Statistical Purposes and the National Academies of Sciences, Engineering, and Medicine), (2) an overview of the comprehensive cybercrime classification system by Phillips and colleagues (2022), describes the existing measurement of cybercrime in the NCVS as it relates to Phillips and colleagues' (2022) taxonomy, and (3) recommendations for revisions to the measurement of cybercrime in the NCVS.

2 Cybercrime Classification Systems

Although cybercrime has existed and been studied for decades, there is currently no agreed-upon definition or taxonomy of cybercrime in the empirical literature, in the educational and governmental classifications systems, or even in legislation (no jurisdiction in the world has a single agreed-upon definition of cybercrime)[2,3,4,5,6,7]. Reports from national organizations, such as the National Academy of Sciences, Engineering, and Medicine (NAS),[8] confirmed a lack of consensus on a cybercrime definition or taxonomy. NAS *Modernizing Crime Statistics* Report 1 notes that "cybercrime is much like fraud or intentional homicide—a sufficiently broad and diverse concept that it could warrant a fully realized three- or four-level hierarchical classification on its own."[9] NAS *Modernizing Crime Statistics* Report 2 goes further to recommend considering the space in which cybercrime takes place; "is 'cyberspace' a location outside of conventional geographic space or is it truly 'location-less'?"[10] The nearly-constant changing nature of the mode of cybercrime—social media alone is continually developing new platforms for consumers—makes creating a definitionally-based taxonomy difficult.

A review of the International Classification of Crime for Statistical Purposes – ICCS (developed by the UNECE-UNODC Joint Task Force on Crime Classification and endorsed by the Conference of European Statisticians to finalize an international classification of crime for statistical purposes) suggests defining cybercrime as a "fraud offence perpetrated through the use of a computer" and to classify it as a fraud with a "cybercrime-related tag." Additionally, the ICCS recommends that the following minimum set of disaggregating variables should be applied to criminal offenses where relevant:

- event descriptions (e.g., degree of completion, type of weapon used, situational context, geographical location, date and time, type of location, motive)
- victim descriptions (e.g., sex, age, citizenship, legal status, intoxication status)
- perpetrator descriptions (e.g., sex, age, victim-perpetrator relationship, citizenship, legal status, intoxication status, repeat offender).[11]

Yet even this terminology differs from the extant literature. The empirical literature does not utilize the "cyber-related" terminology and instead defines cybercrime as mostly cyber-enabled or cyber-dependent. Cyber-enabled crimes are crimes that could occur without the involvement of a computer, though a computer plays a role in the crime (e.g., cyberbullying). In contrast, cyber-dependent crimes occur when the computer itself is a target, or when the crime cannot be committed without a computer (Paoli et. al., 2018, Sarre et. al., 2018, McGuire et al 2013, and Brenner 2007).[12,13,14,15]

To combat the language issue, NAS suggests not focusing too intently on cybercrime terminology and instead suggests researchers retain ICCS's per-offense attribute of cybercrime involvement—a binary yes/no flag based on whether computer systems or data were integral to the modus operandi of the offense.

> "Our classification system relies heavily on the cybercrime-involved flag included in the attributes section to indicate offenses where computers or networks are critical to the modus operandi of the criminal offense. It is in this way that we avoid carving out categories for specific cybercrime offenses for which keeping up with terminology could be a losing battle. To this end, we rely on the cybercrime flag to facilitate construction of derived categories of interest, such as ransomware (in terms of behavior, the combination of extortion and cybercrime-involvement) or cyberbullying (harassment in combination with cybercrime)."[10]

With the NAS approach, any given measure of crime could potentially be converted to cybercrime; harassment can be modified and reanalyzed to detect cyber harassment or cyberbullying, as can cyber-enabled stalking, identity theft (using computer means), and others. The FBI's National Incident-Based Reporting System (NIBRS) takes a similar approach to coding cybercrime, which the FBI then uses to define and collect crime incidents. NIBRS added cybercrime in 2015 as an incident category, specifically two additional fraud offenses (Identity Theft and Hacking/Computer Invasion) were added. However, NIBRS later clarified *Cyberspace* as a "location code." For example, identity theft could happen as a "location code" in person with someone stealing your license or identity theft could happen as a "location code" for cyberspace where it occurred online/using a computer.[16] Although these classification systems chose to approach cybercrime using "location codes" and binary yes/no internet-based flags, empirical researchers as well as state and federal laws on cybercrime have taken different approaches.

2.1 State and Federal Cybercrime Laws

Regarding cybercrimes and cyber-enabled crimes, states vary widely in terms of their statutes. All 50 U.S. states have a law prosecuting those who gain unauthorized access to a computer. Although laws differ slightly, most laws punish "unauthorized accessing, altering, damaging or destroying of any computer, computer network, computer program, computer service, computer software, or computer system." Additionally, all 50 states have some law or laws punishing identity theft, fraud, or forgery, with Hawaii, Michigan, Virginia, Wyoming, Minnesota, and New Mexico specifically including language about identity theft/fraud using a computer or electronic means. There are 23 states with laws that specifically outlaw internet phishing scams or email fraud scams: Alabama, Arkansas, Arizona, California, Connecticut, Florida, Georgia, Illinois, Kentucky, Louisiana, Michigan, Minnesota, Montana, New Mexico, New York, Oklahoma, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia, and Washington.[17,18,19]

Although there are no official federal laws related to cyberbullying at this time, five states have criminal

statutes that outlaw cyberbullying, specifically Arkansas, Senate Bill 214; Idaho, HH 750; Maryland, Grace's Law; Michigan, Public Act 457; North Carolina, 14-458.1. In Maryland and North Carolina, the statute states that cyberbullying can only be committed toward a minor. Additionally, all states (except for Montana) have a law that requires K-12 public school districts to adopt and enforce a policy to prohibit and punish all forms of on-campus bullying, including cyberbullying, whereas 25 states require that schools address off-campus bullying as well. On-campus versus off-campus bullying is defined as the physical location the perpetrator was occupying while engaging in harassing behavior online. For example, the Alabama Student Harassment Prevention Act – HB 0216[20], and the Texas Education Code § 37.0832[21] outline general and cyber-enabled bullying as intentional behavior that can take place on or off school property.

> Alabama: "A continuous pattern of intentional behavior that takes place on or off of school property, on a school bus, or at a school-sponsored function including, but not limited to, cyberbullying or written, electronic, verbal, or physical acts that are reasonably perceived as being motivated by any characteristic of a student, or by the association of a student with an individual who has a particular characteristic, if the characteristic falls into one of the categories of personal characteristics contained in the model policy adopted by the department or by a local board, and implemented at each school."
>
> Texas: "*Cyberbullying* means bullying that is done through the use of any electronic communication device, including through the use of a cellular or other type of telephone, a computer, a camera, electronic mail, instant messaging, text messaging, a social media application, an Internet website, or any other Internet-based communication tool.
>
> (1) bullying that occurs on or is delivered to school property or to the site of a school-sponsored or school-related activity on or off school property;
>
> (2) bullying that occurs on a publicly or privately owned school bus or vehicle being used for transportation of students to or from school or a school-sponsored or school-related activity; and
>
> (3) cyberbullying that occurs off school property or outside of a school-sponsored or school-related activity if the cyberbullying:
>
> (A) interferes with a student's educational opportunities; or
>
> (B) substantially disrupts the orderly operation of a classroom, school, or school-sponsored or school-related activity."

Finally, 11 U.S. states explicitly allow for suspension or expulsion as punishment for cyberbullying (Alaska, California, Idaho, Illinois, Maine, Nebraska, New Jersey, Ohio, Rhode Island, Texas, Vermont). There are three federal laws that address online threats or harassment. One (18 U.S.C. § 2261A) focuses on online threats in the context of cyberstalking and a larger course of conduct that causes substantial emotional distress. Federal law 18 U.S.C. § 875 prohibits threats via the internet that are specifically intended to extort money or something of value from a person, firm, association, or corporation. Finally, 47 U.S.C. 223 prohibits the use of telecommunication devices (including email) to abuse, threaten, or harass a specific person. However, it specifies that the offending party has not disclosed their identity in the course of the threatening communication. If cyberbullying reaches the threshold for electronic harassment or threat, 44 states and DC, have a criminal harassment sanction that explicitly includes language about harassment or threat via electronic communication. Only 6 states (Maine, Minnesota, Nebraska, New Hampshire, New Mexico, Wyoming) do not explicitly mention electronic communication in their statewide harassment laws.[22]

Across the states with cyber harassment laws, the thresholds for when statements made via electronic communication rise to the level of harassment or threat vary in terms of whether the statements are a crime in and of themselves or must be made in the context of bullying, stalking, or hate crime. As previously discussed, the NAS, ICCS, and NIBRS classification systems utilize the binary yes cyber/no cyber flag indication approach to classifying cybercrime (i.e., they define cybercrime as any already defined traditional crime that occurs via cyber-enabled means). In contrast, state laws differentiate cybercrime via the level of the threat. For example, a minor, non-punishable offense such as bullying might not rise to the level of a prosecutorial offense, while repeated cyberstalking can be prosecuted. How states interpret "level of threat" differs across states. Examples of states with cyber harassment or threat laws that are not tied to other offenses include Illinois, Iowa, and Virginia.[23,24,25,26]

- Illinois 2010 Illinois Code, Chapter 720 Criminal Offense 720 ILCS 135: Harassing and Obscene Communications Act defines harassment through electronic communication as: "making any obscene comment, request, suggestion or proposal with an intent to offend," and "threatening injury to the person or to the property of the person to whom the electronic communication is directed or to any of his family or household members."

- Iowa §708.7 Harassment Law specifies that: "A person commits harassment when, with intent to intimidate, annoy, or alarm another person, the person does any of the following: communicates with another by telephone, telegraph, writing, or via electronic communication without legitimate purpose and in a manner likely to cause the other person annoyance or harm."

- Virginia Section 18.2-152.7:1 "Harassment by Computer," states that, "If any person, with the intent to coerce, intimidate, or harass any person, shall use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act," they have committed harassment by computer. These laws are typically applied in the case of cyberbullying but could apply to other threats that do not involve the power differential that typically distinguishes bullying from other harassment.

In all 50 U.S. states, it is illegal to produce, distribute, or possess "child pornography," or any visual depiction of sexually explicit content involving a minor [18 U.S.C. § 2252]. All states excluding Massachusetts, Mississippi, South Carolina, and Wyoming have a criminal statute that outlaws "revenge porn," or the dissemination of private, intimate, revealing, or nude images without consent (i.e., nonconsensual pornography).[27] Currently, 24 states (Alabama, Arizona, Arkansas, California, Colorado, Georgia, Hawaii, Indiana, Kansas, Kentucky, Maine, Maryland, Missouri, Nevada, New Hampshire, North Carolina, North Dakota, Oklahoma, Rhode Island, Texas, Utah, Vermont, Virginia, West Virginia) have a criminal statute that includes language to punish sexual extortion.[28] In addition, 27 U.S. states have laws that punish minors who create or distribute sexually explicit images/visual depictions of a minor that depicts explicit sexual material (Arizona, Arkansas, Colorado, Connecticut, Florida, Georgia, Hawaii, Illinois, Indiana, Kansas, Louisiana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Dakota, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Vermont, Washington, West Virginia). Only 9 states have laws that explicitly use the term "sexting" (Arkansas, Connecticut, Florida, Louisiana, New Jersey, Rhode Island, South Dakota, Vermont, West Virginia).[29]

Cybercrime may also be charged at the federal level. In 1984, the U.S. passed the Computer Fraud and Abuse Act (CFAA) and many amendments have been made to this law and were codified in 18 U.S.C. §

1030.[30] The law applies to anyone who gains access to a protected computer "without authorization" or in a way that "exceeds authorization." Under the CFAA, a protected computer is defined as (1) any U.S. government computer, (2) a financial institution computer, or (3) a computer used in interstate or foreign commerce. The courts have since ruled that any device connected to the internet is a computer used in interstate or foreign commerce, and thereby constitutes a protected computer (i.e., personal computers, cell phones, etc.), United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007). CFAA focuses on the following types of crimes:[31,32,33]

- accessing a computer and obtaining information (1) in a financial record of a financial institution or a credit card issuer, (2) from any department or agency of the United States, or (3) from any protected computer including one used exclusively by a financial institution or U.S. government, or one which affects interstate or foreign commerce even if located outside of the United States
- obtaining national security information
- trespassing on a government computer
- accessing a computer to defraud and obtain value
- intentionally damaging by knowingly transmitting a code or a program such as a computer virus
- recklessly damaging a protected computer by intentional access
- negligently causing damage and loss to a protected computer by intentional access
- trafficking passwords if the passwords affect commerce or a computer used by the U.S. government
- extortion involving computers.

Federal wire fraud law 18 U.S.C. § 1343 (last updated 2008) is designed to punish any individual "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice."[34] Additionally, federal identity theft law 18 U.S.C. § 1028 (last updated 2006) is designed to punish any individual who "knowingly produces an identification or false document, or possesses documents with intent to defraud," including any identity theft that uses the internet to cross state lines.[35] Further, 15 U.S.C. § 1644 was developed to punish credit card fraud[36], and 15 U.S.C. § 1693 was developed to punish debit card fraud.[37] Finally, federal law 18 U.S.C. § 471 (last updated 2001) states that those with intent to defraud, falsely makes, forges, counterfeits, or alters any obligation or other security of the United States will be punished.[38]

There are also other types of cybercrimes covered under the Electronics Communication Privacy Act (ECPA), which pertains to crimes involving wire, oral, and electronic communications while they are being made, transmitted, or stored on a computer, as well as email and data stored electronically. The federal government has also passed cybercrime laws such as:

- Credit Card Fraud Act, whereby computers and other technology are being used to make fraudulent credit card transactions from cloning credit cards, obtaining credit card access through unauthorized devices and other means to commit credit card fraud.
- Identity Theft Assumption and Deterrence Act, which criminalizes the theft of others' personal data and the impersonation of others in the cyber arena.
- Economic Espionage Act, which deals with the theft of trade secrets and other intellectual property.

- Child Pornography Prevention Act, which criminalizes the digital possession, production, and the distribution of images or videos that depict minors in sexually explicit conduct.
- The Violence Against Women Reauthorization Act, which prohibits the use of computers or electronic communication to harass, threaten, kill, intimidate, or place one under surveillance.[39]

Federal law 18 U.S.C. § 2261A (last updated 2020) focuses on online threats in the context of cyberstalking and a larger course of conduct that causes substantial emotional distress. The statute defines stalking as: "having the intent to kill, injure, harass, intimidate, or place under surveillance another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that—

A. places that person in reasonable fear of the death of or serious bodily injury to a person, a pet, a service animal, an emotional support animal, or a horse described in clause (i), (ii), (iii), or (iv) of paragraph (1)(A); or
B. causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A)."[40]

As of now, there are no federal laws that specifically address bullying, cyberbullying, or trolling. If bullying includes the discrimination/denial of equal opportunity on the basis of race, color, national origin, sex, sexual orientation, gender identity, or disability, it may be punishable under Title IV and Title VI of the Civil Rights Act of 1964; Title IX of the Education Amendments of 1972; Section 504 of the Rehabilitation Act of 1973; Titles II and III of the Americans with Disabilities Act; or Individuals with Disabilities Education Act (IDEA). If cyberbullying reaches the threshold for electronic harassment or threat, it is punishable under Section (b)(2) of federal law 18 U.S.C. § 2261A (see above). Additionally, there is currently no federal law that addresses sexual image-based abuse; however, the SHIELD Act (the Stop Hacks and Improve Electronic Data Security Act) has been proposed (S.3777), which criminalizes the distribution of an "intimate visual depiction of an individual" without consent or reasonable belief that distributing the "depiction touches a matter of public concern."[41]

Federal law 18 U.S.C. § 2252 (last updated 2012) addresses "certain activities relating to material involving the sexual exploitation of minors." The code punishes any individual who receives, possesses, distributes, sells, or accesses with intent to view, any visual depiction of sexually explicit content involving a minor (i.e. child sexual abuse material) "using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer."[42] Federal law 47 U.S.C. 223 (last updated 2013) expands that statute to prohibit the distribution of child pornography via the internet, "(a) uses an interactive computer service to send to a specific person or persons under 18 years of age, or (b) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that is obscene or child pornography, regardless of whether the user of such service placed the call or initiated the communication."[43]

Sexual Extortion or exploitation of a minor is covered under 18 U.S.C. § 2251 (last updated 2008) which punishes "Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual

depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed." And, although there are no federal laws that explicitly describe "sexting," when sexting involving a minor, it is punishable under this statute.[44]

For non-minors, federal law 18 U.S.C. § 875 (last updated 1994) has been used to prosecute sexual extortion, although it does not specifically address sexual content. Section (d) states that:

> "Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both."[45]

These federal and state laws provide a high-level overview of our nation's approach to defining and enforcing laws against cybercrimes and cyber-enabled crimes. The following literature review presents a national and international approach to defining, describing, understanding, and measuring cybercrime.

2.2 Extant Cybercrime Classification and Phillips and Colleagues' (2022) Taxonomy

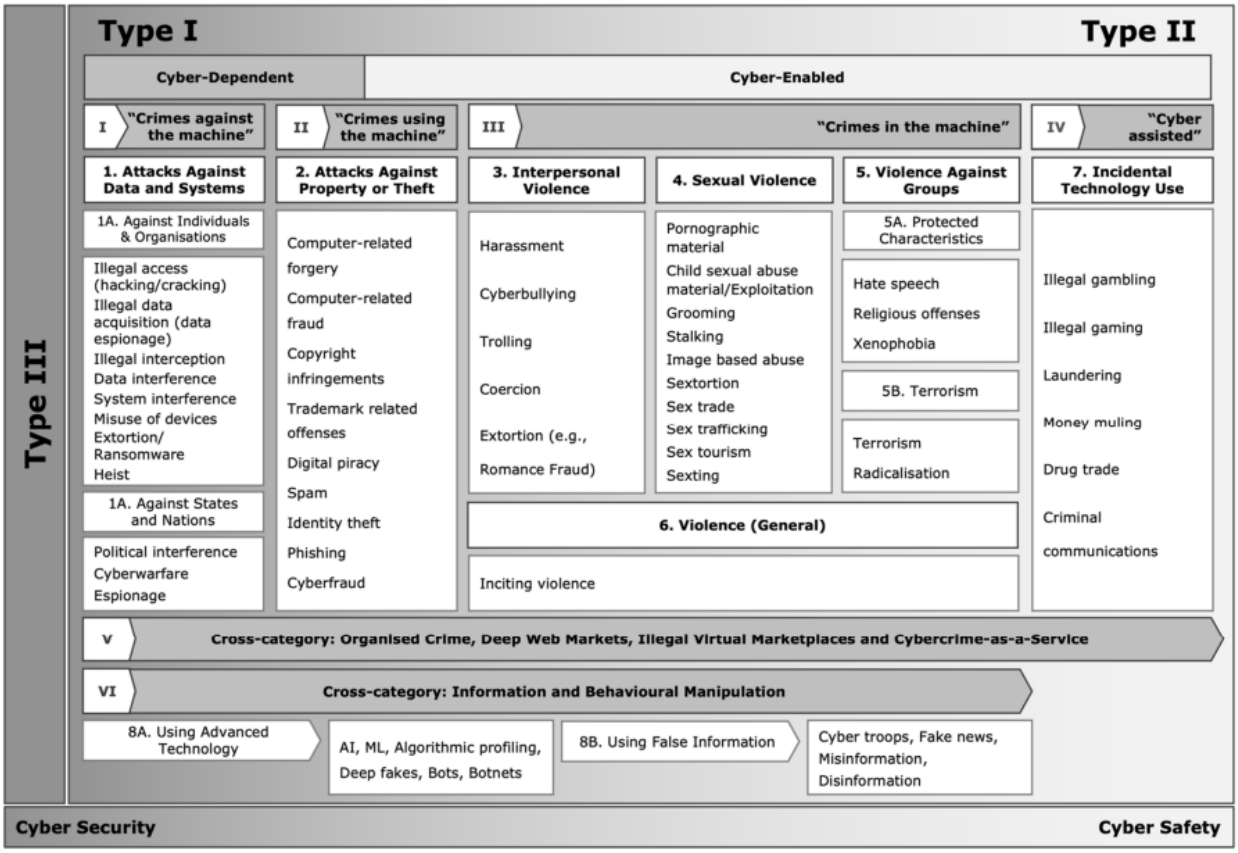
As opposed to the previously described classifications approach, federal and state laws approach cybercrime based on the level of harassment to the victim. The seemingly conflicting approaches regarding how to define and classify cybercrime is reflected in the massive amount of theoretical and empirical research on cybercrime against persons or institutions. Researchers have attempted to mitigate this issue by suggesting various taxonomies for organizing and classifying cybercrime. However, the speed at which cybercrime is evolving, coupled with the variability in terminology and inconsistencies across legislation, has made this difficult and resulted in multiple organizing frameworks and taxonomies. Given this variation in definitions and perspectives, the authors set out to explore meta-analyses, classification systems, taxonomies, and systematic reviews of cybercrime in the extant literature

As noted earlier, since the early 2000s, there have been numerous attempts at defining and classifying cybercrime. The most frequently cited definitions used in the literature come from Thomas and Loader (2000), "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (p. 3)[46] and Gordon and Ford (2006), "any crime that is facilitated or committed using a computer, network, or hardware device" (p. 14).[47] Early in the exploration of cybercrime definitions and typologies, researchers often took a dichotomous approach (i.e., cyber-enabled versus cyber-dependent crime; Paoli et. al., 2018, Sarre et. al., 2018, McGuire et al 2013, and Brenner 2007).[48,49,50,51] However, researchers quickly realized that this two-factor system could not cover all cybercrimes. Thus, Sarre and colleagues (2018) suggested revising the dichotomy to a trichotomy with the adoption of Type I, Type II, and Type III forms of cybercrime. Type 1 cybercrimes are technical (e.g., hacking), Type II cybercrimes involve human communication or interaction (e.g., cyberbullying), and Type III cybercrimes are those perpetuated via Artificial Intelligence

(e.g., bots).

In recent years, researchers have begun exploring a new approach to classifying cybercrime: taxonomies. This approach allows for the categorization of various types of cybercrime without getting hindered by terminologies. As noted previously, given the nearly constant changing nature of cybercrime modes and naming conventions, it is a worthwhile venture to avoid defining cybercrime by terminology. Although not the most frequently cited (due to publication date recency), the most comprehensive taxonomy is that of Phillips and colleagues (2022) (Figure 1). It incorporates the early dichotomy and trichotomy approaches, as well as the previously defined "Type" approaches to cybercrime classification.[52] Additionally, Phillips and colleagues' (2022) taxonomy references the other most frequently cited taxonomies in the literature, including the Council of Europe's (COE) Convention of Cybercrime, widely recognized as "the only globally recognized agreement around cybercrime" (Council of Europe, 2001). Although they were compiled 20 years ago, the Council's recommendations remain a solid foundational classification system on which more recently published authors base their own typologies (Tsakalidis & Vergidis, 2017).[53] Phillips and colleagues' (2022) taxonomy also references and incorporates frequently cited cybercrime taxonomies that diverge from the COE-basis, including the classification system posed by Marcum and Higgins (2019).[54] Thus, as of today, we contend that Phillips and colleagues' (2022) taxonomy is the most comprehensive and responsive to the ever-evolving nature of cybercrime. Of course, the most obvious limitation is the recency of the taxonomy. There has not been enough time to allow dissenting authors/researchers to provide a more comprehensive taxonomy, or a classification system with a different theoretical perspective. Additionally, Phillips and colleagues (2022) made assumptions regarding inclusion or exclusion in their own taxonomy, as we have done in this report.

Figure 1: Phillips and Colleagues' (2022) Cybercrime Taxonomy



This taxonomy is not only representative of the extant literature, but also has the most direct applicability to BJS's National Crime Victimization Survey (NCVS). Although the NCVS does measure cyber-enabled crime (e.g., Identity Theft Supplement, School Crime Supplement), the NCVS has never been revised with the explicit goal of measuring cybercrime victimization. Phillips and colleagues' (2022) taxonomy can potentially serve as a framework on which NCVS revisions and additions can be predicated in an effort to be responsive to both previous classification and measurement attempts and the rapidly and constantly changing nature of cybercrime.

3 Phillips and Colleagues' (2022) Taxonomy and its Applicability to the NCVS's Measurement of Cybercrime

The NCVS already covers a broad range of crime victimization types including nonfatal personal crimes (i.e., rape or sexual assault, robbery, aggravated and simple assault, and personal larceny) and household property crimes (i.e., burglary/trespassing, motor vehicle theft, and other types of theft) both reported and not reported to the police. Yet, the NCVS does not consistently assess victimization experiences committed via cyber-enabled means alongside victimization experiences committed in person for all relevant types covered in the taxonomy. Further, there are some types of cybercrimes that should not be assessed on the NCVS, mostly due to the fact that the NCVS is foremost a survey about crime incidents enacted upon individuals; in contrast, some types of cybercrimes target governments, organizations, etc. Based on Phillips and colleagues' (2022) comprehensive taxonomy, this report

identifies ways that the NCVS currently measures or could be revised to better capture cyber-enabled crimes that are within the scope of the survey (i.e., non-commercial incidents committed against individuals or households).

The following sections of the report organize cybercrime measures into three categories. Section 3.1 details cybercrimes from the taxonomy that are already being measured through the NCVS either partially or fully. For those covered only partially, the report discusses how they are already being measured and any recommended revisions for expanding the scope of those measures. Relevant state or federal laws relating to the crime type are also included. Section 3.2 details crimes from the taxonomy that are not currently assessed in the NCVS, but that should be considered for inclusion in future iterations. Section 3.3 details crimes from the taxonomy not currently assessed in the NCVS that are not recommended to be included in future iterations because they are out of scope for the NCVS. The Appendix presents examples of existing survey measures that can be utilized to develop new recommendations for the NCVS.

3.1 Crimes Currently Assessed on the NCVS, Fully or Partially

Category 1A. Against Individuals and Organizations[*]

- *Illegal access (hacking)*

Tsakalidis and Vergidis (2017) describe "hacking" as, "the offence in which someone knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct aims for personal benefit." All 50 states and Federal Computer Fraud and Abuse Act (CFAA; 18 U.S.C. § 1030) state hacking is a punishable offense.

Although the core NCVS does not ask victims about hacking as a stand-alone offense, hacking is measured in the NCVS Identity Theft Supplement (ITS) as one way an offender might obtain someone's personal information. One of the response options for "How do you think your personal information was obtained?" is "Someone hacked into my computer." This measure only captures hacking done in connection to identity theft. However, it is not recommended that this be expanded to be a stand-alone item on the core survey. If an individual's computer system was hacked without the offender obtaining information, it is unlikely that the respondent would be aware of the hacking and therefore could not report the victimization experience on the NCVS.

Recommendation: no change.

- *Extortion*

There are numerous forms of extortion. When extortion is perpetrated through malware, it is called ransomware. Bhardwaj (2017) describes malicious attacks of ransomware that are perpetrated through various vectors such as browser exploit kits, drive-by freeware apps, malicious email attachments, links offering free software, or advertisements offering free cash and incentives. When the user downloads or opens the file, the virus often encrypts the user data files or even hijacks the system itself, forcing the innocent user into paying up to the ransom demands before having the data files and system restored and released.[55] All 50 U.S. states have a law prosecuting those who gain unauthorized access to a

[*] Category titles and numbering refer to how Phillips and colleagues' (2022) taxonomy is organized.

computer. Although each state's law differs slightly, most laws punish "unauthorized accessing, altering, damaging or destroying of any computer, computer network, computer program, computer service, computer software, or computer system." Further, Section (a)(7)(c) of the Federal Computer Fraud and Abuse Act (CFAA) outlaws unauthorized access to any protected computer "with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion,"[30] which includes any extortion or ransomware.

Romance fraud, which is grouped under extortion in the taxonomy, is discussed in the section below on cyber fraud.

Although the NCVS does not currently include any questions that could be used to measure cyber extortion through ransomware, this type of crime is within the scope of the NCVS. One consideration in adding questions to the NCVS to capture extortion through ransomware is that there are likely a relatively small number of individual victims, since these offenses are more often targeted to businesses and other organizations.

Recommendation: Conduct research on whether extortion can be measured through new items on the NCVS.

Category 2. Attacks Against Property or Theft

- *Computer-related forgery*

Tsakalidis and Vergidis (2017) define forgery as, "…fraud and related activity in connection with identification documents, authentication features, and information. The composing of a document that fraudulently appears to originate from a legitimate author, the modification of an image or video for defamation or as a proof in front of juries, and the alteration of a document or text in order to deceive, are examples of computer-related forgery. Forgery plays a key role in the success of other cybercrimes such as phishing, in which the victim is encouraged to disclose sensitive personal or financial information. This can be achieved by gaining the victim's trust regarding the sender's authenticity with the use of proper forgery techniques."[53] All 50 states have some law or laws punishing forgery-related crimes, and federal wire fraud laws (18 U.S.C. § 1343), federal identity theft laws (18 U.S.C. § 1028), Federal Computer Fraud and Abuse Act (CFAA; 18 U.S.C. § 1030), and federal forgery laws (18 U.S.C. § 471) suggest intentional forgery is punishable at the federal level.

Forgery is partially assessed in the NCVS. Some of the types of identity theft and fraud asked about in the NCVS ITS and the Supplemental Fraud Survey (SFS) could cover forgery. For example, the ITS asks,

> "Has someone used or attempted to use your personal information for some other fraudulent purpose, such as filing a fraudulent tax return, getting medical care, applying for a job or government benefits; giving your information to the police when they were charged with a crime or traffic violation, or something else?"

Forgery is important to consider because it plays a key role in the success of other cybercrimes such as phishing, in which the victim is encouraged to disclose sensitive personal or financial information. We

suggest forgery be considered for inclusion in the NCVS, possibly as an added response option to questions about how identifying information was obtained or how the fraud was committed.

Recommendation: Conduct additional research to examine inclusion of forgery in either the ITS or SFS.

- *Identity theft*

Tsakalidis and Vergidis (2017) explain identity theft as the "assumption of a pre-existing identity (or significant part of it), with or without consent, and regardless of whether the person is dead or alive."[53] Often, the perpetrator illegally obtains personally identifying information about the victim and uses it to purchase items or open new accounts in the victim's name. All 50 states have some law or laws punishing identity theft or fraud; some states specifically include language about identity theft/fraud using a computer or electronic means. Further, Federal Identity Theft laws (18 U.S.C. § 1028) state identity theft is a punishable offense at the federal level.

The NCVS already assesses identity theft in detail in the ITS. For example, it asks,

> "During the past 12 months, that is from [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR] until today, has someone, without your permission, used or attempted to use your personal information to open any NEW accounts such as wireless telephone accounts, credit card accounts, loans, bank accounts, online payment accounts, or something else?"

Because the ITS also asks victims how they think their information was obtained, including options such as "It was stolen during an online purchase/transaction," the survey can be used in its current form to produce estimates of cyber identity theft.

Recommendation: no change.

- *Cyber fraud (i.e., computer-related fraud)*

Smyth and Carleton (2011) define cyber fraud as, "any act of dishonesty or deception carried out through the use of the Internet (or computer technologies) that defrauds the public or any person out of property, money, valuable security or service."[56] Currently, there are 23 states with laws that specifically outlaw internet phishing scams or email fraud scams, and all 50 states have some law or laws punishing identity theft or fraud. Cyber fraud may be punished under Federal wire fraud laws (18 U.S.C. § 1343), Federal Identity Theft laws (18 U.S.C. § 1028), or the federal Computer Fraud and Abuse Act (CFAA; 18 U.S.C. § 1030).

Although the SFS measures fraud, it does not assess cyber fraud explicitly. Example questions include,

> "In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], did you pay money to settle or pay off taxes or a debt, but you found out you were being tricked or lied to and the debt was not real or not yours?"
>
> "In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you donated money to a charity or a charitable cause that later turned out to be fake or that you later suspected was fake?"

> "In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you paid money to get a job or get into a business opportunity but were tricked or lied to about how the money would be used or what you would receive in return?"

Romance fraud is "a type of online grooming and abuse…where the fraudster sets up information early in the communication, which is then relied on to validate later behaviors and requests; 'visceral responses', where the fraudster uses reactions to situations to invoke a protective response from the victim, and 'isolating the victim', where the fraudster uses language to detach the victim from the security and reality of their support network."[57] Although faking romantic interest is not a crime, romance fraud/internet dating fraud may be punishable if the fraud is designed to capture money. All 50 states have some law or laws punishing identity theft or fraud (Hawaii, Michigan, Minnesota, New Mexico, Virginia, and Wyoming specifically include language about identity theft/fraud using a computer or electronic means). In terms of federal laws, similar to the state laws, if the fraud involves money, the crimes may be punished under Federal Identity Theft laws (18 U.S.C. § 1028), Federal wire fraud laws (18 U.S.C. § 1343), or Federal Bank Fraud laws (18 U.S.C. § 1344).

The NCVS currently measures romance fraud in the SFS:

> "In the past 12 months, that is, since [AUTOFILL DATE 1st OF MONTH 1 YEAR PRIOR], have you donated, sent, or otherwise given money to someone who PRETENDED to be or pretended to be calling on behalf of a family member, friend, caregiver, or someone interested in you romantically, but that person was not who they claimed to be?"

We recommend revising the NCVS to account for Phillips and colleagues' (2022) approach to cyber fraud. For each fraud type, questions could be added asking victims how they first learned about the product, service, investment, charity, or other fraudulent offer or promise. Response options of internet, email, or text message would constitute cyber fraud.

Recommendation: Conduct additional research to examine inclusion of cyber fraud in the SFS.

Category 3. Interpersonal Violence

- *Cyber-enabled harassment*

Hazelwood and Koon-Magnin (2013) define cyber-based harassment as, "engaging in an act or behavior that torments, annoys, terrorizes, offends, or threatens an individual via email, instant messages, or other means with the intention of harming that person… Harassing communications encompass all of the events of traditional harassment, but extends the crime into the use of electronic devices to communicate messages that cause a person to feel personally targeted for harm."[58]

The NCVS currently measures harassment in several places including:

> The Crime Incident Report, for example, says, "What actually happened? … Harassed, argument, abusive language"
>
> The School Crime Supplement (SCS), for example, says, "During this school year, has any student from your school… Made fun of you, called you names, or insulted you, in a hurtful way?"

The Supplemental Victimization Survey (SVS), for example, says, "Has anyone sent you unwanted emails or messages using the Internet, for example, using social media apps or websites like Instagram, Twitter, or Facebook?"

However, these measures are not comprehensively capturing cyber harassment and several of these existing measures do not explicitly identify harassment by cyber means rather than through other modes.

Recommendation: Examine measurement of harassment holistically across core and supplemental surveys to determine how to effectively measure for both adults and minors.

- *Cyberbullying*

Cyberbullying, cyber harassment, and cyberstalking involve similar actions, and often, the terms are used interchangeably, but they do differ. Cyberbullying has been defined as "willful and repeated harm inflicted through the medium of electronic text" (Patchin & Hinduja, 2006, p.152).[59] Unlike harassment and stalking, cyberbullying also entails a power differential between the person doing the bullying and the victim. These sorts of behaviors can be carried out using cellular phone text messaging, email, and Internet instant messaging and can take place in chat rooms, on personal websites, on social networking sites such as MySpace, Facebook, Instagram, Snapchat, etc., or on Internet bulletin boards or in other web-based environments. Although in many cases cyberbullying involves traditional bullying behaviors (e.g., name-calling, spreading rumors or lies, and making threats) that are communicated electronically rather than in person, cyberbullying also can include behaviors unique to the Internet that have no corollary in traditional bullying. For example, "bombing" occurs when a bully uses an automated program to flood the victim's email inbox with thousands of messages at once, potentially causing a failure of the email software or of the entire computer system.[60] In more recent years, "doxing" has become prolific, and refers to obtaining and disclosing the personal information of others without their consent.[61]

Five U.S. states have criminal statutes that outlaw cyberbullying (Arkansas, Senate Bill 214; Idaho, HH 750; Maryland, Grace's Law; Michigan, Public Act 457; North Carolina, 14-458.1). In Maryland and North Carolina, the statute specifies that cyberbullying can only be committed toward a minor. Given the extreme measures some young people take in response to cyberbullying, all 49 U.S. states (with the exception of Montana) have responded by instituting a law that requires K-12 public school districts to adopt and enforce a policy to prohibit and punish all forms of bullying that take place when the perpetrator is on campus, including cyberbullying; 25 states require that schools address off-campus bullying (i.e., acts of bullying or harassment when the perpetrator is off-campus); and 11 U.S. states explicitly allow for suspension or expulsion as punishment for cyberbullying (Alaska, California, Idaho, Illinois, Maine, Nebraska, New Jersey, Ohio, Rhode Island, Texas, Vermont). If cyberbullying reaches the threshold for electronic harassment or threat, 44 states have a criminal harassment sanction that explicitly includes language about harassment or threat via electronic communication.

As of now, there are no federal laws that specifically address bullying or cyberbullying. If bullying includes the discrimination/denial of equal opportunity on the basis of race, color, national origin, sex, sexual orientation, gender identity, or disability, it may be punishable under Title IV and Title VI of the Civil Rights Act of 1964; Title IX of the Education Amendments of 1972; Section 504 of the Rehabilitation Act of 1973; Titles II and III of the Americans with Disabilities Act; or Individuals with Disabilities

Education Act (IDEA). If cyberbullying reaches the threshold for electronic harassment or threat, it is punishable under Section (b)(2) of Federal 18 U.S.C. § 2261A.

The SCS on the NCVS already measures cyberbullying against minors.

> "Still thinking about all of the times that you were bullied, where did the bullying occur? Did it occur ... Online or by text?"
>
> "Still thinking about [the time/all of the times] that [another student/other students] did [something/those things] to you, where did [it/they] occur? Did [it/they] occur ... Online or by text?"

We believe the NCVS already assesses cyberbullying sufficiently on the NCVS. BJS should consider only assessing cyberbullying for minors as cyberbullying in adults usually does not rise to the level of a crime unless it involves direct threats. The challenge is delineating the natural gray area between "joking around" and bullying, which is ultimately a subjective determination.

Recommendation: no change.

Category 4. Sexual Violence

- *Cyber-enabled stalking*

In its most basic definition, cyberstalking entails "the repeated pursuit of an individual using electronic or Internet-capable devices."[62] Repeated pursuits include any unwanted electronic communications, and may be threatening, coercive, or intimidating. Ultimately, stalking is a crime that creates a sense of fear, terror, intimidation, stress, or anxiety in the victim. Because of the repetitive nature of cyberstalking, the victim may lose a sense of control over his/her own life, never knowing when the stalker may appear or contact the victim again.[63] In addition to the Federal law, 44 states have criminal harassment sanctions that explicitly include language about harassment or threat via electronic communication. This language includes instances of cyberstalking. The remaining 6 states (Maine, Minnesota, Nebraska, New Hampshire, New Mexico, Wyoming) do not explicitly mention electronic communication in state-wide harassment laws.[64] In regard to Federal statutes pertaining to cyberstalking, Section (b)(2) of Federal 18 U.S.C. § 2261A reports that "anyone with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person, an immediate family member of a person, a spouse or intimate partner of that person, or the pet, service animal, emotional support animal, or horse of that person," is subject to punishment.[65]

If it was part of a pattern or series of such behavior, nearly any act of cyber harassment would constitute cyberstalking. To constitute stalking, the behavior(s) have to be repeated and make the victim feel fearful. This is likely true regardless of the medium (in person, by telephone, or online).

Stalking is already measured in the NCVS, under the SVS.

> "Now I want to ask about unwanted contacts or behaviors using various technologies, such as your phone, the Internet, or social media apps. Again, please DO NOT include bill collectors, solicitors, or other salespeople. In the past 12 months...
>
> > Has anyone spied on you or monitored your activities using technologies such as a listening device, camera, or computer or cell phone monitoring software?
> >
> > Has anyone monitored your activities using social media apps like Instagram, Twitter, or Facebook?"

Recommendation: no change.

- *Cyber-enabled image-based abuse (i.e., non-consensual pornography)*

McGlynn and Rackley (2017) define "image-based sexual abuse" as the "non-consensual creation and/or distribution of private sexual images."[66] Powell and colleagues (2018) note that it involves "non-consensual taking, sharing or threats to share nude or sexual images (photos or videos) of a person. It also includes digitally altered imagery in which a person's face or body is superimposed or 'stitched into' a pornographic photo or video, known as 'fake pornography' (including 'deepfakes' when synthetic images are created using artificial intelligence). Often referred to as 'non-consensual pornography' or 'revenge porn', image-based sexual abuse is an invasion of a person's privacy and a violation of their human rights to dignity, sexual autonomy and freedom of expression."[67]

All states excluding Massachusetts, Mississippi, South Carolina, and Wyoming have a criminal statute that outlaws "revenge porn," or "nonconsensual pornography," involving the dissemination of private, intimate, revealing, or nude images without consent. Currently, there is no federal law that addresses sexual image-based abuse; however, the SHIELD Act has been proposed (S.3777), which criminalizes the distribution of an "intimate visual depiction of an individual" without consent or reasonable belief that distributing the "depiction touches a matter of public concern."[41]

The SCS of the NCVS asks about sharing photos/videos for persons 12-18.

> "Now I have some questions about what students do at school that make you feel bad or are hurtful to you. These could occur in person or using technologies, such as a phone, the Internet, or social media. During this school year, has any student from your school… Purposely shared your private information, photos, or videos in a hurtful way?"

Additionally, the SVS assesses threats of posting pictures or videos on the internet against another's wishes.

> "Now I want to ask about unwanted contacts or behaviors using various technologies, such as your phone, the Internet, or social media apps. Again, please DO NOT include bill collectors, solicitors, or other salespeople. In the past 12 months… Has anyone posted or threatened to post inappropriate, unwanted, or personal information about you on the Internet, including private photographs, videos, or spreading rumors?"

Although image-based abuse, sextortion, and other forms of cyber harassment are related, they differ in terms of their ultimate goal. For example, the goal of sextortion is to obtain something of value from the victim while the goal of image-based abuse is to harm the victim emotionally. We suggest that BJS

consider the inclusion of image-based abuse on the NCVS. This is a growing crime type that is within the scope of a criminal victimization survey.

Recommendation: Conduct additional research to examine inclusion of image-based abuse.

3.2 Crimes Not Assessed on the NCVS that Require Additional Research

Category 2. Attacks Against Property or Theft

- *Phishing*

Tsakalidis and Vergidis (2017) define phishing as, "a form of social engineering through which the attacker obtains sensitive information by fraudulently pretending to be a trustworthy third party. The attack is mainly conducted with the use of spoofed emails, or through the installation of malware on the victims' computers, however, other methods may exist deriving from the attacker's imagination and technical expertise. Consequently, the victims perceive these emails as legitimate providing sensitive information such as credit card and e-banking account numbers and passwords, thus, circumventing every possible security measure."[53] There are 23 states with laws that specifically outlaw internet phishing scams or email fraud scams; however, there is no current federal law that specifically addresses internet phishing scams (but they may be punished under Federal wire fraud laws (18 U.S.C. § 1343) or Federal Identity Theft laws (18 U.S.C. § 1028)).

Although the NCVS does not currently include questions regarding a victim's experience with phishing, we recommend phishing be considered for inclusion on the NCVS due to its inclusion as a crime under some state laws.

Recommendation: Conduct additional research to examine inclusion of phishing.

Category 4. Sexual Violence

- *Cyber-enabled sextortion*

Sextortion differs from image-based abuse (discussed above) in that it involves sharing images or threatening someone to force/coerce them into sexual contact. Researchers define sextortion as, "the threatened dissemination of explicit, intimate, or embarrassing images of a sexual nature without consent, usually for the purpose of procuring additional images, sexual acts, money, or something else."[68] Twenty-six states have a criminal statute that includes language to punish sexual extortion, and all states have an additional clause outlawing "revenge porn," or the dissemination of private, intimate, revealing, or nude images without consent. Finally, sexual exploitation of a minor is punishable under Federal law 18 U.S.C. § 2251, and non-minors under 18 U.S.C. § 875.

Recommendation: Conduct additional research to examine inclusion of sextortion.

3.3 Out-of-Scope Cybercrime Types

From Phillips and colleagues' (2022) taxonomy, the following types of cybercrime are not currently assessed in the NCVS, but we do not recommend including them in future iterations of the survey because they are crimes targeted at states, nations, or institutions, rather than an individual, or they are crimes without a clear victim. Given that the NCVS is designed to assess crimes against individuals,

crimes against organizations or where there is no clear victim cannot be appropriately assessed in the NCVS.

Category 1A. Against Individuals and Organizations

- *Illegal data acquisition (data espionage)*
- *Illegal interception*
- *Data interference*
- *System interference*
- *Misuse of devices*
- *Heist*

Category 1A. Against States and Nations

- *Political interference*
- *Cyberwarfare*
- *Espionage*

Category 2. Attacks Against Property or Theft

- *Copyright infringements*
- *Trademark related offenses*
- *Digital piracy*
- *Spam*

Cybercrimes targeted at states, nations, or institutions are outside the scope of what the NCVS collects.

Category 3: Interpersonal Violence

- *Trolling*

Trolling is not considered criminal unless it involves threats. Currently, there are no state laws that specifically address internet "trolling," although five states have criminal statutes that outlaw cyberbullying. If trolling reaches the threshold for electronic harassment or threat, 44 states have a criminal harassment sanction that explicitly includes language about harassment or threat via electronic communication. Further, there are no federal laws that specifically address internet "trolling." If trolling reaches the threshold for electronic harassment or threat, it is punishable under Section (b)(2) of Federal 18 U.S.C. § 2261A.

- *Coercion*

Most definitions of cyber coercion suggest this is something that occurs between nations rather than individuals.[69]

Category 4. Sexual Violence

- *Child sexual abuse material/exploitation*

Quayle and colleagues (2020) define child sexual abuse material exploitation as, "the production,

dissemination and possession of child sexual abuse images (known in many jurisdictions as child pornography); online grooming of children for sexual purposes; 'sexting'; sexual extortion of children ('sextortion'); revenge pornography; commercial sexual exploitation of children; exploitation of children through online prostitution, and live streaming of sexual abuse."[70] In all 50 states, it is illegal to produce, distribute, or possess "child pornography," or any visual depiction of sexually explicit content involving a minor; this is also reflected at the federal level (18 U.S.C. § 2252).

The inclusion of child sexual abuse is out of scope for the NCVS because the survey does not assess victimization for minors under the age of 12; thus, this assessment would be missing a large component of the population. Further, it may be difficult to measure as minors (or even proxy adults) may not be aware of online material involving them, and a victim may not discover that their image has been used in child pornography within six months of the offense occurring, which is the reference period for the NCVS.

- *Sex trade/sex trafficking/sex tourism*

Although these terms are differentiated in Phillips and colleagues' (2022) taxonomy, we do not find evidence of their differentiation in the literature or in measurement. Therefore, for purposes of discussion, we combined these terms into one category. Sex trafficking is defined by the United Nations Office on Drugs and Crime (UNODC) as, "The recruitment, transportation, transfer, harboring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude or the removal of organs."[71] In recent years, there has been an increase of recruiting and "advertising" related to sex trafficking, thus moving the historically in-person crime to a cybercrime.[72, 73, 74]

However, the NCVS is not well positioned to assess sex trafficking victimization compared to other existing methodologies.[75] There are several reasons for this, including the lack of a universal definition of sex trafficking, which would make creating survey questions difficult. Additionally, household-based surveys, like the NCVS are not ideally situated to measure many types of crime, including crimes against homeless, institutionalized, and trafficked populations, which makes it difficult to provide reliable estimates of sex trafficking victimization.

- *Sexting*

Lounsbury and colleagues (2011) define sexting as, "the creation and transmission of sexual images by minors." They elaborate saying, "The majority of attention has been directed toward sexting via cell phone, but the term can apply to any digital media, such as e-mail, instant messaging, and social networking sites. The term can be used for producing and sending images of oneself, receiving images directly from the producer, or forwarding received images to other people."[76] Twenty-seven states have laws that punish minors who create or distribute sexually explicit images/visual depictions of a minor that depicts explicit sexual material (Arizona, Arkansas, Colorado, Connecticut, Florida, Georgia, Hawaii, Illinois, Indiana, Kansas, Louisiana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Dakota, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Vermont,

Washington, West Virginia), but only 9 states have laws that explicitly use the term "sexting" (Arkansas, Connecticut, Florida, Louisiana, New Jersey, Rhode Island, South Dakota, Vermont, West Virginia). Twenty-three states have laws that punish minors who receive sexually explicit images or visual depictions of a minor that depicts explicit sexual material (Arizona, Arkansas, Colorado, Florida, Georgia, Hawaii, Indiana, Kansas, Louisiana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Dakota, Pennsylvania, South Dakota, Tennessee, Texas, Utah, Vermont, Washington, West Virginia). Additionally, all states, excluding Massachusetts, Mississippi, South Carolina, and Wyoming, have a criminal statute that outlaws "revenge porn," or the dissemination of private, intimate, revealing, or nude images without consent. There are no federal laws that explicitly address "sexting;" however, when sexting involves a minor, the act becomes punishable by federal sexual extortion laws (18 U.S.C. § 2251) or federal child sexual abuse material laws (18 U.S.C. § 2252).

One challenge with measuring sexting as a crime is that sexting is usually consensual by both parties. It becomes a crime when it involves a minor or when one (or both) parties share that information elsewhere. When sexting includes a minor, this crime becomes punishable under the same laws as child sexual abuse material distribution/exploitation (see above). Finally, an added challenge is that affirmative responses to questions would require a respondent to implicate themselves in the act.

- *Pornographic materials*
- *Grooming*

These acts are not considered criminal unless they involve a minor.

Category 5. Violence Against Groups - 5a. Protected Characteristics

- *Hate speech*
- *Religious offenses*
- *Xenophobia*

The SCS on the NCVS asks about online or text-based bullying motivated by bias, religious bias, or by ethnicity or origin bias, for persons 12-18 (but does not specify bias due to being from another country). However, we do not recommend revision to the NCVS as none of these biases are considered criminal unless involving a direct threat.

Category 5. Violence Against Groups - 5b. Terrorism

- *Radicalization*
- *Terrorism*

Although radicalization and terrorism are serious problems and are perpetuated extensively online, there is no clear victim in radicalization-related crimes. Regarding terrorism, there will likely be a small number of victims and measurement may be difficult. Thus, we do not recommend inclusion on the NCVS.

Category 6. Violence (General)

- *Inciting violence*

Category 7. Incidental Technology Use

- *Illegal gambling*
- *Illegal gaming*
- *Laundering*
- *Money muling*
- *Drug trade*
- *Criminal communications*

Category 8a. Using Advanced Technology

- *Artificial intelligence*
- *Machine learning*
- *Algorithmic profiling*
- *Deepfakes*
- *Bots*
- *Botnets*

Category 8b. Using False Information

- *Cyber troops*
- *Fake news*
- *Misinformation*
- *Disinformation*

4 Recommendations for Future Measurement of Cybercrime on the NCVS

The table below summarizes the cybercrime types, applicability to the NCVS, and assessment of coverage within the core and supplemental surveys.

Cybercrime Type	Currently captured by NCVS	Recommendation
Illegal access (hacking)	Yes	No change
Extortion	No	Further research
Computer-related forgery	Partially	Further research
Identity theft	Yes	No change
Cyber fraud	Partially	Further research
Harassment	Partially	Further research
Cyberbullying	Yes	Further research

Stalking	Yes	No change
Image-based abuse	Yes	Further research
Phishing	No	Further research
Sextortion	No	Further research
Illegal data acquisition	No	Out of scope
Illegal interception	No	Out of scope
Data interference	No	Out of scope
System interference	No	Out of scope
Misuse of devices	No	Out of scope
Heist	No	Out of scope
Political interference	No	Out of scope
Cyberwarfare	No	Out of scope
Espionage	No	Out of scope
Copyright infringements	No	Out of scope
Trademark related offenses	No	Out of scope
Digital piracy	No	Out of scope
Spam	No	Out of scope
Trolling	No	Out of scope
Coercion	No	Out of scope
Child sexual abuse material/exploitation	No	Out of scope
Sex trade/sex trafficking/sex tourism	No	Out of scope
Sexting	No	Out of scope
Inciting violence	No	Out of scope
Pornographic materials	No	Out of scope
Grooming	No	Out of scope
Hate speech	Partially	Out of scope
Religious offenses	No	Out of scope
Xenophobia	No	Out of scope

Radicalization	No	Out of scope
Terrorism	No	Out of scope
Illegal gambling	No	Out of scope
Illegal gaming	No	Out of scope
Laundering	No	Out of scope
Money muling	No	Out of scope
Drug trade	No	Out of scope
Criminal communications	No	Out of scope
Artificial intelligence	No	Out of scope
Machine learning	No	Out of scope
Algorithmic profiling	No	Out of scope
Deepfakes	No	Out of scope
Bots	No	Out of scope
Botnets	No	Out of scope
Cyber troops	No	Out of scope
Fake news	No	Out of scope
Misinformation	No	Out of scope
Disinformation	No	Out of scope

For each of the cybercrime types included in the table above, additional research on definitions, measurement, and survey items will inform the next phase of research.

Additionally, whether estimates should be presented individually by cybercrime type or aggregately as a composite measure that reflects total cybercrime victimization was examined. An aggregate measure could be created through the development of a single survey question or a short series of questions used to generate a single estimate of cybercrime, or by aggregating across multiple cyber-enabled measures as is done to create composite measures for violent and property crime. However, there are several challenges with this approach. These include, but are not limited to:

- the range of victimization experiences included under the heading of cybercrime is diverse enough that it might be difficult to effectively define the various crime types in the context of one question or a few questions;
- the ages of focus for the cybercrime types vary (i.e., cyberbullying is currently measured for persons 12-18; identity theft is only asked of people 16 or older);

- some of cybercrime types overlap or could occur in the context of the same incident (cyber fraud and forgery; stalking and nonconsensual porn), but there would not be a way to parse this out to the same extent the NCVS does this currently;
- the NCVS supplements, some of which cover some of the cybercrime types, have different reference periods than the core NCVS, focus on producing prevalence rates rather than incident rates, do not have a bounding adjustment, have different rules related to proxy respondents, and have different weights.

These differences make combining estimates from the supplements and core somewhat problematic. It is recommended that BJS focus on measuring individual types of cybercrime, rather than use an aggregate or composite approach.

Appendix

Survey Name (if applicable)	Related Construct(s)	Content Summary	Example Item(s)	Reference
N/A	Phishing	Predicting future phishing victimization	Have you fallen for phishing emails in the past? It is likely that I will become victimized by phishing attacks.	Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. Decision Support Systems, 133, 113287.
Adolescent Cyber-Victimization Scale (CYBVICS)	Extortion	This scale is composed of 18 items that assess direct and indirect cyber-victimization.	Someone used threats to make me do things on the Internet or smartphone that I did not want to do (like recording myself on video, giving money, doing bad things)	Buelga, S., Martínez-Ferrer, B., Cava, M. J., & Ortega-Barón, J. (2019). Psychometric properties of the CYBVICS cyber-victimization scale and its relationship with psychosocial variables. Social Sciences, 8(1), 13.
N/A	Extortion	Item assessment of ransomware (type of extortion)	Have you ever been a victim of a ransomware attack? Ransomware is a type of malicious software, or malware, that denies access to a computer system or data until a ransom is paid.	Yilmaz, Y., Cetin, O., Grigore, C., Arief, B., & Hernandez-Castro, J. (2022). Personality Types and Ransomware Victimisation. Digital Threats: Research and Practice.
Cyber Victimization Scale	Forgery	Thirty-five-item cybercrime measure	My personal information on social networking profiles was used for fraudulent act	Riaz, N., Iram, H., Iqbal, N., & Hassan, B. (2022). Development and Validation of Cyber Victimization Scale (CVS). Foundation University Journal of Psychology, 6(2).

Adolescent Cyber-Victimization Scale (CYBVICS)	Fraud	This scale is composed of 18 items that assess direct and indirect cyber-victimization.	Someone created a false profile on the Internet with my personal data in order to impersonate me saying or doing bad things	Buelga, S., Martínez-Ferrer, B., Cava, M. J., & Ortega-Barón, J. (2019). Psychometric properties of the CYBVICS cyber-victimization scale and its relationship with psychosocial variables. Social Sciences, 8(1), 13.
FINRA Foundation Fraud Survey	Fraud	Includes measures of fraud prevalence and the mode of fraud commission	How did you find out about the person, product, service, job, charity, or company you gave your money to? (Select all that apply) I found out from browsing the Internet I found out through an email I found out through a text message or direct message on my mobile phone I received something in the mail I found out through a TV commercial or Radio advertisement I was called directly by someone on the telephone I attended a presentation or seminar I found out through word-of-mouth or face-to-face from the person who took my money	DeLiema, M., Mottola, G. R., & Deevy, M. (2017). Findings from a pilot study to measure financial fraud in the United States. Available at SSRN 2914560.

Youth Internet Safety Study	Harassment, image-based abuse	Measures of online harassment, unwanted sexual acts, exposure to porn, and sexting	In the past year, did anyone on the Internet ever ask you to do something sexual that you did not want to do? In the past year, did anyone ever use the Internet to threaten or embarrass you by posting or sending messages about you for other people to see? Has someone else ever taken nude or nearly nude pictures or videos of you?	Mitchell, K. J., & Jones, L. M. (2011). Youth Internet Safety Study (YISS): Methodology Report.
Nationwide online study of nonconsensual porn victimization and perpetration	Image-based abuse	Measures the prevalence of having sexual graphic images distributed without consent	Has anyone ever shared or threatened to share a sexually-explicit image or video of you without your consent?	Eaton, A., Jacobs, H., & Ruvalcaba, Y. (2017). 2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration.
Adolescent Cyber-Victimization Scale (CYBVICS)	Image-based abuse	This scale is composed of 18 items that assess direct and indirect cyber-victimization.	To make fun of me, someone made or manipulated videos or photos of me and uploaded or distributed them on social networks or by smartphone. Someone stole my photos, videos, or private conversations and uploaded them or sent them to others.	Buelga, S., Martínez-Ferrer, B., Cava, M. J., & Ortega-Barón, J. (2019). Psychometric properties of the CYBVICS cyber-victimization scale and its relationship with psychosocial variables. Social Sciences, 8(1), 13.

National Sextortion Survey Among U.S. Youth	Sextortion	Measures prevalence of sextortion among middle and high school students		https://journals.sagepub.com/doi/full/10.1177/1079063218800469#bibr24-1079063218800469
Sextortion Study	Sextortion	Online survey of persons 18-25 who experienced sextortion	Did the person who threatened you ever contact you on or direct you to use any of the following types of websites or apps? How long had you known them or interacted with them online before they got the first image?	https://www.thorn.org/wp-content/uploads/2016/08/Sextortion_Report.pdf
Cyber Victimization Scale	Sextortion	Thirty-five item cybercrime measure	Someone has pressurized me to share my naked photos	Riaz, N., Iram, H., Iqbal, N., & Hassan, B. (2022). Development and Validation of Cyber Victimization Scale (CVS). Foundation University Journal of Psychology, 6(2).
Adolescent Cyber-Victimization Scale (CYBVICS)	Cyber harassment and bullying	This scale is composed of 18 items that assess direct and indirect cyber-victimization.	Someone insulted or ridiculed me in social networks or groups like WhatsApp to really hurt me. Someone used threats to make me do things on the Internet or smartphone that I did not want to do (like recording myself on video, giving money, doing bad things) To make fun of me, someone made or manipulated videos or photos of me and	Buelga, S., Martínez-Ferrer, B., Cava, M. J., & Ortega-Barón, J. (2019). Psychometric properties of the CYBVICS cyber-victimization scale and its relationship with psychosocial variables. Social Sciences, 8(1), 13.

			uploaded or distributed them on social networks or by smartphone. Someone stole my photos, videos, or private conversations and uploaded them or sent them to others.	

5 References

[1] Text - S.2629 - 117th Congress (2021-2022): Better Cybercrime Metrics Act. (2022, May 5). https://www.congress.gov/bill/117th-congress/senate-bill/2629/text

[2] Black, A., Lumsden, K., & Hadlington, L. (2019). 'Why Don't You Block Them?' Police Officers' Constructions of the Ideal Victim When Responding to Reports of Interpersonal Cybercrime. In Online Othering (pp. 355-378). Palgrave Macmillan, Cham.

[3] Viano, E. C. (2017). Cybercrime, organized crime, and societal responses. *Int. approaches*, Basel, 1103

[4] Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change, 70*(4), 397-420.

[5] Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: current trends. *Police practice and research, 19*(6), 515-518.

[6] Donalds, C., & Osei-Bryson, K. M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior, 92*, 403-418.

[7] Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review, 34*(6), 1180-1196.

[8] NAS, an independent entity charged with providing objective advice to the nation on matters related to science and technology.

[9] National Academies of Sciences, Engineering, and Medicine. (2016). *Modernizing crime statistics: Report 1: Defining and classifying crime*. National Academies Press.

[10] National Academies of Sciences, Engineering, and Medicine. (2018). *Modernizing crime statistics: Report 2: New systems for measuring crime*. National Academies Press.

[11] United Nations Office on Drugs and Crime. (2015). International Classification of Crime for Statistical Purposes (ICCS)—Version 1.0.

[12] Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change, 70*(4), 397-420.

[13] Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: current trends. *Police practice and research, 19*(6), 515-518.

[14] McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75, 1-35.

[15] Brenner, S. (2007) 'Cybercrime: Re-thinking Crime Control Strategies', in Y. Jewkes (ed.), Crime Online. Cullompton: Willan Publishing

[16] National Incident-Based Reporting System User Manual. (2021). Criminal Justice Information Services Division Global Law Enforcement Support Section Crime Statistics Management Unit. https://bjs.ojp.gov/sites/g/files/xyckuh236/files/sarble/data_common/nibrs-user-manual-2021-1041521.pdf

[17] https://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx

[18] Anti-Phishing Laws & Regulations (2017. InfoSec. https://resources.infosecinstitute.com/topic/anti-phishing-laws-regulations/

[19] Computer Crime Statues. National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx

[20] https://cyberbullying.org/bullying-laws/alabama

[21] Tex. Educ. Code § 37.0832. https://casetext.com/statute/texas-codes/education-code/title-2-public-education/subtitle-g-safe-schools/chapter-37-discipline-law-and-order/subchapter-c-law-and-order/section-370832-bullying-prevention-policies-and-procedures#:~:text=(a%2D1)%20This%20section,of%20students%20to%20or%20from

[22] https://cyberbullying.org/bullying-laws

[23] Extortion: Laws, Penalties, and Sentencing. https://www.criminaldefenselawyer.com/crime-penalties/federal/Extortion.htm

[24] Federal Civil Action for Disclosure of Intimate Images: Free Speech Considerations (2022). Congressional Research Service. https://crsreports.congress.gov/product/pdf/LSB/LSB10723

[25] https://www.ncsl.org/Portals/1/Documents/legisbriefs/2019/AugustLBs/Revenge-Porn-and-Sextortion_29.pdf

[26] STATE ANTI-TERRORISM LAWS. International Association of Chiefs of Police. https://www.theiacp.org/sites/default/files/all/k-m/ModelStatutesTerrorism2002.pdf

[27] https://cyberbullying.org/sexting-laws

[28] https://www.ncsl.org/Portals/1/Documents/legisbriefs/2019/AugustLBs/Revenge-Porn-and-Sextortion_29.pdf

[29] https://cyberbullying.org/sexting-laws

[30] https://www.law.cornell.edu/uscode/text/18/1030

[31] https://www.sciencedirect.com/topics/computer-science/computer-fraud-and-abuse-act

[32] Sharton, B. (2018). Key Issues in Computer Fraud and Abuse Act (CFAA) Civil Litigation. Practical Law. https://www.goodwinlaw.com/-/media/files/publications/10_01-aa-key-issues-in-computer-fraud-and-abuse.pdf

[33] https://www.justice.gov/jm/jm-9-48000-computer-fraud

[34] https://www.law.cornell.edu/uscode/text/18/1343

[35] https://www.law.cornell.edu/uscode/text/18/1028

[36] https://www.govinfo.gov/app/details/USCODE-2010-title15/USCODE-2010-title15-chap41-subchapI-partB-sec1644

[37] https://www.law.cornell.edu/uscode/text/15/chapter-41/subchapter-VI

[38] https://www.law.cornell.edu/uscode/text/18/471

[39] HOW THE EXPANSION OF FEDERAL CYBERCRIME LAWS AFFECTS YOU. Bruno Law. https://brunolaw.com/resources/general-criminal-law/the-expansion-of-federal-cybercrime-laws-and-how-it-affects-you

[40] https://www.law.cornell.edu/uscode/text/18/2261A

[41] S.3777 - 117th Congress (2021-2022): SHIELD Act of 2022. (2022, March 8). https://www.congress.gov/bill/117th-congress/senate-bill/3777

[42] https://www.law.cornell.edu/uscode/text/18/2252

[43] https://www.law.cornell.edu/uscode/text/47/223

[44] Sextortion - Should It Be a Federal Crime? https://www.hg.org/legal-articles/sextortion-should-it-be-a-federal-crime-53756

[45] https://www.law.cornell.edu/uscode/text/18/875

[46] Thomas, D. and Loader, B. (2000) 'Introduction – cyber crime: law enforcement, security and surveillance in the information age', in: D. Thomas and B. Loader (Eds.), Cyber crime: Law Enforcement, Security and Surveillance in the Information Age, London: Routledge.

[47] Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in computer virology, 2(1), 13-20.

[48] Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change, 70*(4), 397-420.

[49] Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: current trends. *Police practice and research, 19*(6), 515-518.

[50] McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75, 1-35.

[51] Brenner, S. (2007) 'Cybercrime: Re-thinking Crime Control Strategies', in Y. Jewkes (ed.), Crime Online. Cullompton: Willan Publishing

[52] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2(2), 379-398.

[53] Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(4), 710-729.

[54] Marcum, C. D., & Higgins, G. E. (2019). Cybercrime. In Handbook on crime and deviance (pp. 459-475). Springer, Cham.

[55] Bhardwaj, A. (2017). Ransomware: A rising threat of new age digital extortion. In Online banking security measures and data protection (pp. 189-221). IGI Global.

[56] Smyth, S. M., & Carleton, R. (2011). Measuring the extent of cyber-fraud: A discussion paper on potential methods and data sources.

[57] Carter, E. (2021). Distort, extort, deceive and exploit: exploring the inner workings of a romance fraud. The British Journal of Criminology, 61(2), 283-302.

[58] Hazelwood, S. D., & Koon-Magnin, S. (2013). Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. International Journal of Cyber Criminology, 7(2), 155.

[59] Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. Youth Violence and Juvenile Justice, 4(2), 148–169.

[60] Burgess-Proctor, A., Patchin, J. W., & Hinduja, S. (2009). Cyberbullying and online harassment: Reconceptualizing the victimization of adolescent girls. Female crime victims: Reality reconsidered, 162, 176.

[61] Chen, M., Cheung, A. S. Y., & Chan, K. L. (2019). Doxing: What adolescents look for and their intentions. International journal of environmental research and public health, 16(2), 218.

[62] Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. Deviant behavior, 33, 1- 25. doi: 10.1080/01639625.2010.538364

[63] Hazelwood, S. D., & Koon-Magnin, S. (2013). Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. International Journal of Cyber Criminology, 7(2), 155.

[64] https://cyberbullying.org/bullying-laws

[65] https://www.govinfo.gov/content/pkg/USCODE-2013-title18/pdf/USCODE-2013-title18-partI-chap110A-sec2261A.pdf

[66] McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. Oxford Journal of Legal Studies, 37(3), 534-561.

[67] Powell, A., Henry, N., & Flynn, A. (2018). Image-based sexual abuse. In Routledge handbook of critical criminology (pp. 305-315). Routledge.

[68] Patchin, J. W., & Hinduja, S. (2020). Sextortion among adolescents: Results from a national survey of U.S. youth. Sexual Abuse, 32(1), 30-54.

[69] Hodgson, Q. E., Ma, L., Marcinek, K., & Schwindt, K. (2019). Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.

[70] Quayle, E. (2020, December). Prevention, disruption and deterrence of online child sexual exploitation and abuse. In Era Forum (Vol. 21, No. 3, pp. 429-447). Springer Berlin Heidelberg.

[71] United Nations Office on Drugs and Crime (UNODC). 2004. United Nations Convention Against Transnational Organized Crime and the Protocols Thereto. New York.

[72] Hickle, K. (2017). Victims of sex trafficking and online sexual exploitation. In Cybercrime and its Victims (pp. 94-107). Routledge.

[73] Greiman, V., & Bain, C. (2013). The emergence of cyber activity as a gateway to human trafficking. Journal of Information Warfare, 12(2), 41-49.

[74] Chung, W., Mustaine, E., & Zeng, D. (2017, July). Criminal intelligence surveillance and monitoring on social media: Cases of cyber-trafficking. In 2017 IEEE international conference on intelligence and security informatics (ISI) (pp. 191-193). IEEE.

[75] https://www.acf.hhs.gov/sites/default/files/documents/otip/adult_human_trafficking_screening_tool_and_guide.pdf

[76] Lounsbury, K., Mitchell, K. J., & Finkelhor, D. (2011). The True Prevalence of "Sexting."