

# Comparative study on the metric of cybercrime between the U.S. and South Korea

Seokbeom Kim·Yunsik Jang·Alice Elizabeth Perry·Youngoh Jo



**KiC**

KOREAN INSTITUTE OF CRIMINOLOGY





# Table of Contents

## Chapter 1 Seokbeom Kim · Youngoh Jo

<b>INTRODUCTION</b> .....	<b>1</b>
Section 1 Connectivity and Cybercrime .....	3
Section 2 Contemporary Cybercrime .....	7
Section 3 Issues in Measuring Cybercrime .....	12
1. Difficulty in Establishing the Definition of Cybercrime .....	12
2. Problem with Counting Cybercrime .....	13
3. Estimating the Financial Costs of Cybercrime .....	14
4. Limitation of Official Crime Statistics and Victimization Survey .....	16
Section 4 Scope of Research .....	19
Section 5 Methodology .....	20

## Chapter 2 Seokbeom Kim · Yunsik Jang

<b>DEFINITION OF CYBERCRIME</b> .....	<b>23</b>
Section 1 Overview .....	25
Section 2 UNODC .....	25
Section 3 E.U. ....	26
Section 4 The United States of America .....	27
Section 5 South Korea .....	34

**Chapter 3** Seokbeom Kim · Alice Elizabeth Perry · Yunsik Jang

**MEASURING CYBERCRIME** ..... 35

Section 1 Introduction	37
1. Official Crime Statistics	38
2. Victimization Survey	39
3. Self-Reporting	41
4. Crime Cost	43
5. Fear of Crime	44
Section 2 Current Practices within South Korean Law	
Enforcement	45
1. Investigative Procedure	45
2. Official Cybercrime Statistics	47
3. Other Cybercrime Statistics	49
4. Self-Reporting	52
5. Victimization Survey	54
6. Summary	57
Section 3 Current Practices in the U.S. Law Enforcement	57
1. Federal and State Criminal Jurisdiction in the U.S.	57
2. Cybercrime in the U.S.	62
3. Cybercrime Statistics	78
4. Summary	101

**Chapter 4** Seokbeom Kim · Youngoh Jo

**CONCLUSION** ..... 105

Section 1 Comparison of the Metrics of Cybercrime	107
1. The Cyber-policing Organization	107
2. Definition and Classification of Cybercrime	109
3. The Kind of Data Collected	111
4. The Levels of Data Collected	113

Section 2 Policy Implication .....	115
1. Developing Index Cybercrime .....	115
2. Adopting Alternative Measures of Cybercrime .....	116
3. Enhancing the Reliability of Official Cybercrime Statistics .....	116
4. Publicize Detailed Official Cybercrime Data .....	117
 References .....	 119



# List of Figures and Tables

## 【Figures】

[Figure 1-1-1] Share of the Internet User among Population, 1990 to 2017 .....	4
[Figure 1-1-2] U.S. Perception towards Police Response to Fight Cybercrime 2018 5	
[Figure 1-2-1] Violent Crime Trends in the U.S. (UCR: 1960-2016) .....	7
[Figure 1-2-2] Property Crime Trends in the U.S. (UCR: 2014-2018) .....	8
[Figure 1-2-3] Violent and Property Crime Trends in the U.S. (NCVS) .....	8
[Figure 1-2-4] Number of Data Breaches and Records Exposed in the U.S. (in millions) .....	9
[Figure 1-2-5] Reported Monetary Damage in the U.S. (in millions) .....	10
[Figure 1-2-6] The Rise in Opioid Overdose Deaths .....	10
[Figure 1-2-7] The Synthetic Opioid Transaction via Dark Web .....	11
[Figure 1-4-1] Traditional and Digital Crime Evidence .....	20
[Figure 3-1-1] Trend in Self-reporting of Cybercrime Victimization in Australia .....	42
[Figure 3-1-2] Self-reported Cybercrime in Australia (2019.7.1~2020.6.30) .....	43
[Figure 3-2-1] Cybercrime Reporting System 1 .....	45
[Figure 3-2-2] Cybercrime Reporting System 2 .....	46
[Figure 3-2-3] Official Cybercrime Registering System (KICS) .....	47
[Figure 3-3-1] Total Caseload for State Courts in United States .....	60
[Figure 3-3-2] Criminal Caseload Composition in 32 States .....	61
[Figure 3-3-3] Felony and Misdemeanor Criminal Caseload Composition in 21 States (including Massachusetts) .....	62
[Figure 3-3-4] Monetary Loss to Victims from Cybercrime in United States by Top States 2019 (in millions) .....	83
[Figure 4-1-1] Organization Chart of the Cybersecurity Bureau in the Korean National Police Agency .....	107
[Figure 4-1-2] Workflow Chart of the Cybercrime Investigation in Massachusetts .....	108

[Figure 4-1-3] Reported Monetary Damage in the U.S. (in millions) .....	111
[Figure 4-1-4] The Flowchart of Reporting Cybercrime in South Korea .....	113
[Figure 4-1-5] The Flowchart of Reporting Cybercrime in the U.S. ....	114
[Figure 4-2-1] Trend in Reported Cybercrime in South Korea .....	117

**【Tables】**

[Table 1-1-1] 2018 Gallup Survey ..... 4

[Table 1-1-2] Reported Cybercrime Cases in South Korea (2010~2018) ..... 6

[Table 1-1-3] Perceived Safety Survey of 2018 (South Korea) ..... 6

[Table 1-3-1] Prior Research on Cybercrime Classification ..... 12

[Table 1-3-2] Major Data Breach Cases in the U.S. .... 14

[Table 1-3-3] Estimated Financial Cost of Cybercrime ..... 15

[Table 1-3-4] Summary of Selected Cyberstalking Victimization Studies ..... 16

[Table 1-3-5] Reported Cybercrime in the South Korean ..... 17

[Table 2-2-1] Cybercrime Classification in UNODC ..... 26

[Table 2-4-1] Group “A” Offenses in NIBRS ..... 27

[Table 2-4-2] Group “B” Offenses in NIBRS ..... 30

[Table 2-4-3] Offense Lookup Table in NIBRS ..... 31

[Table 2-4-4] The Definitions of Fraud Offense by NIBRS ..... 33

[Table 2-5-1] Cybercrime Classification in South Korean ..... 34

[Table 3-1-1] Phishing Victimization in 2008 ..... 39

[Table 3-1-2] Cybercrime Victimization Survey of 2019 CSEW ..... 40

[Table 3-1-3] Cybercrime Victimization Survey in the U.S. .... 41

[Table 3-1-4] Self-reporting Categories of Cybercrime in Australia ..... 41

[Table 3-2-1] Types of Reported Cybercrime (South Korea) ..... 47

[Table 3-2-2] Reported/Arrested Cases by the Types of Cybercrime ..... 48

[Table 3-2-3] Reported/Arrested cases by the Types of Traditional Crime ..... 49

[Table 3-2-4] Institutions with Online Cybercrime Reporting System ..... 50

[Table 3-2-5] Trends in Malware Damage and Hacking Incidents in South Korea · 51

[Table 3-2-6] Deletion and Cancellation of Contents Harmful to Juveniles ..... 52

[Table 3-2-7] Copyright Violation Incidents ..... 52

[Table 3-2-8] Self-Reporting Victimization Survey of 2013 ..... 53

[Table 3-2-9] Self-Reporting Victimization Survey of 2014(N=1,000) ..... 54

[Table 3-2-10] Information Protection Survey of 2013 ..... 55

[Table 3-2-11] Information Statistics Collection 1 ..... 55

[Table 3-2-12] Information Statistics Collection 2 ..... 56

[Table 3-3-1] Massachusetts Statewide Criminal Caseloads by Year ..... 59

[Table 3-3-2] Reported Internet-facilitated Fraud and Financial Losses (2015-2019)	79
[Table 3-3-3] Recovery Rate of Financial Losses by the RAT (2018-2019)	79
[Table 3-3-4] Victim by Age Group (2018-2019)	79
[Table 3-3-5] Cybercrime Types by Victim Count (2018-2019)	80
[Table 3-3-6] Number of Complaints within the American Territory (2018-2019)	81
[Table 3-3-7] Crimes Reported to NIBRS 2018 for All Cities and Towns in Massachusetts	85
[Table 3-3-8] Total Arrests in Massachusetts by Year	94
[Table 3-3-9] The Number of Offenses regarding Crimes Against Property Offenses in 2019	95
[Table 3-3-10] 2019 Crime Against Property Arrests by Offense in Massachusetts	97
[Table 3-3-11] Massachusetts State Police Cybercrime cases (2017-2019)	98
[Table 3-3-12] Worcester Police Department Total Cybercrime Cases (2017-2020)	99
[Table 3-3-13] The NIBRS Systems of the Springfield Police Department	99
[Table 3-3-14] Cybercrimes Handled by Massachusetts Attorney General's Office (2017-2019)	101
[Table 3-3-15] Summary of Massachusetts Cybercrime Statistics	103
[Table 4-1-1] Comparison of the Official Classification of Cybercrime	110
[Table 4-1-2] Cybercrime Type by Victim Count	112
[Table 4-1-3] Comparison of the Kind of Cybercrime Data Collected	113



## Chapter 1

Comparative Study on the metric of cybercrime  
between the U.S. and South Korea

# INTRODUCTION

Seokbeom Kim · Youngoh Jo



## Chapter 1

# INTRODUCTION

### Section 1 | Connectivity and Cybercrime

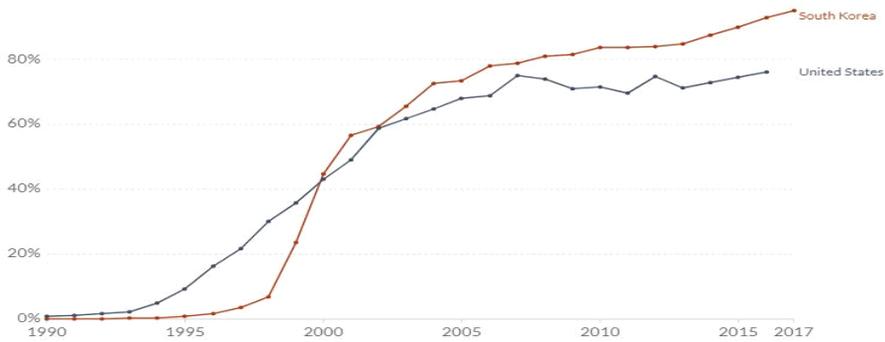
The Internet is now one of the fastest-growing technologies, with its users increasing from 413 million back in 2000 to over 3.4 billion in 2016 and an average of 640,000 new users spring up annually (Roser, Ritchie & Ortiz-Ospina, 2015). Consequently, we can observe in both the U.S. and South Korea's data that the percentage of all individuals who have used the Internet in the last three months among the population skyrocketed since the mid-1990s. Precisely, the graph below displays that South Korea started observing a sharp increase in 1998 and the U.S. in 1994. As of 2017, almost 90% of South Korean and nearly 80% of the Americans use the Internet via a computer, mobile phone, digital T.V., games box, personal digital assistant, etc.(World Bank, 2020). This trend correlated with technological advancements.

The technological advancements allowed the Internet to be faster, cheaper, and easily accessible, enabling cybercriminals to have a great opportunity to be involved with cybercrimes beyond their geographical limits (Baylon & Antwi-Boasiako, 2016). For example, due to the recent COVID-19 pandemic in the U.S., almost 43 million employees lost their job, and qualified laid-off employees filed for unemployment benefits. However, Washington state in the U.S. paid hundreds of millions of dollars to the fake claims, which were filed by the Nigerian hacking

#### 4 Comparative Study on the metric of cybercrime between the U.S. and South Korea

ring, who used stolen identities from prior personal data breaches (“Scammers steal,” 2020).

»» [Figure 1-1-1] Share of the Internet User among Population, 1990 to 2017



Source: World Bank (2020)

Reported cybercrime and the levels of perceived cybercrime in South Korea as well as in the U.S. are very high. According to the “2019 Internet Crime Report,” more than 467 thousand cybercrime cases were reported in 2019, an increase of nearly 33% compared to the previous year (FBI, 2019). Therefore, the general populous of the United States fear the most about the ‘violation of personal information due to cyberattack,’ which were the only two categories hate crime and violation of personal information due to cyberattack that increased compared to their historical averages (Brenan, 2018).

»» [Table 1-1-1] 2018 Gallup Survey

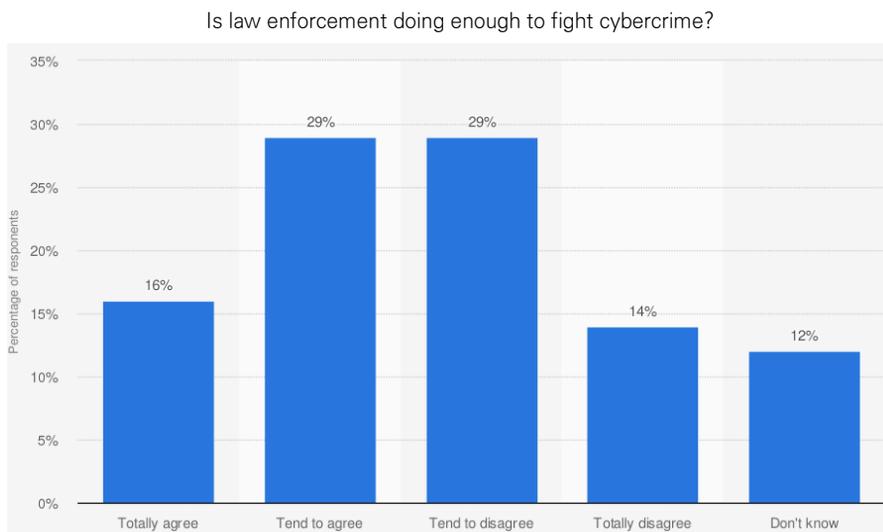
[Question] How often do you, yourself, worry about the following things?(frequently/occasionally/rarely/never) (unit: %)		
	2018	Historical average
Violation of personal information due to cyberattack	71	69
Identity theft	67	68
Burglar	40	45
Car steal	37	43
Terrorism	24	34
Hate crime	22	18
Sexual crime	20	20
Murder	17	18

Source: Cybercrimes Remain Most Worrisome to Americans (Brenan, 2018)

Note: % indicates the sum of ‘frequently’ and ‘occasionally’ responses.

American feels very vulnerable to cybercrime, and thus their levels of satisfaction with low enforcement were shallow. According to the ESET Cybersecurity Barometer USA 2018, only 16 percent of 2,500 respondents was satisfied with the police and other law enforcement authorities' activities against cybercrime (Clement, 2019c).

»» [Figure 1-1-2] U.S. Perception towards Police Response to Fight Cybercrime 2018



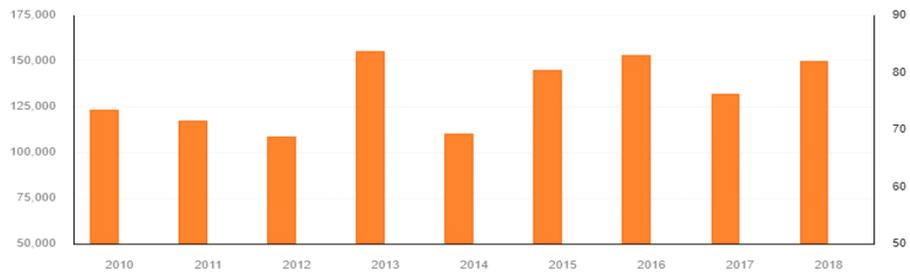
Source: Clement (2019)

Note: 2,500 respondents; 18 years and older; Computer-assisted web interviews (CAWI)

South Korea is also under the threat of cybercrime as advancements in technology and increased usage of mobile communication sparked from widespread usage of smart devices. A threat of cybercrime in Korea ranges from national security, including but not limited to cyberattacks from the People's Republic of Korea (North Korea) or social issues such as cybersex crime. In 2018, the South Korean national police agency reported approximately 150 thousand cases of cybercrime, a 10.2% increase compared to the previous decade.

## 6 Comparative Study on the metric of cybercrime between the U.S. and South Korea

»» [Table 1-1-2] Reported Cybercrime Cases in South Korea (2010~2018)



	2010	2011	2012	2013	2014	2015	2016	2017	2018
Reported Case	122,902	116,961	108,223	155,366	110,109	144,679	153,075	131,734	149,604
% Increase		-4.8%	-7.5%	43.6%	-29.1%	31.4%	5.8%	-13.9%	13.6%

Source: Statistics Korea, e-Nara Indicators (2019)

The Ministry of the Interior and Safety administered ‘Perceived Safety Survey of 2018’ for people above thirteen and field experts, respectively. Among thirteen different disaster categories, ‘cyber threat’ took the second-lowest place only after ‘environmental pollution,’ yet was ranked higher concerning aspect than traditional, physical crimes.

»» [Table 1-1-3] Perceived Safety Survey of 2018 (South Korea)

Perceived Safety		General Population			Expert		
		1 <sup>st</sup> half	2 <sup>nd</sup> half	Difference	1 <sup>st</sup> half	2 <sup>nd</sup> half	Difference
Residential area		3.45	3.39(↓)	-0.06	3.52	3.48(↓)	-0.04
SpecificCriteria	Crime	2.61	2.52(↓)	-0.09	2.96	2.78(↓)	-0.18
	Traffic Accident	2.46	2.42(↓)	-0.04	2.62	2.56(↓)	-0.06
	Sexual Crime	2.44	2.33(↓)	-0.11	2.55	2.54(↓)	-0.01
	Cyber Threat	2.31	2.31(-)	0	2.40	2.42(↑)	0.02
	EnvironmentalPollution	2.27	2.30(↑)	0.03	2.44	2.52(↑)	0.08

Source: Ministry of the Interior and Safety, 2018.

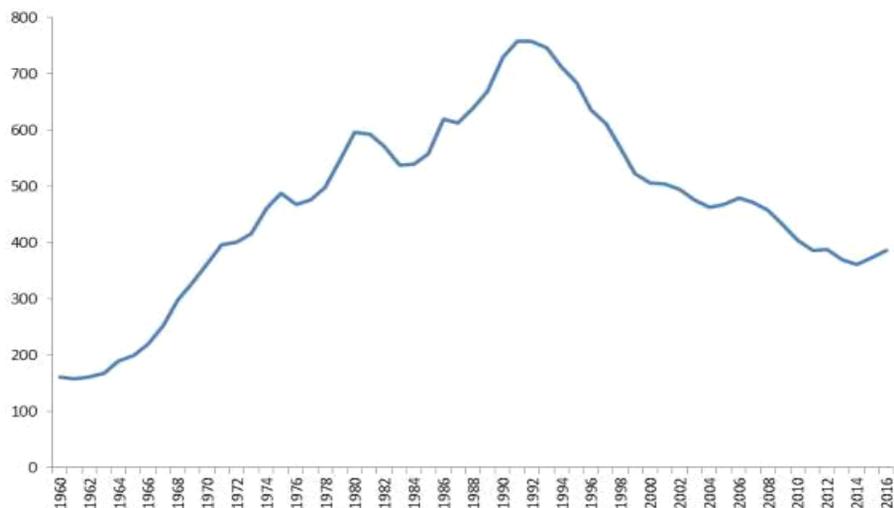
Note: 5-point Likert responses (Very threatened-Threatened-Neutral-Safe-Very Safe)

## Section 2 | Contemporary Cybercrime

Traditionally, crimes were relatively strictly categorized into online and offline crimes. However, increased connectivity caused by the development of Internet and information technologies provides cybercriminals an opportunity to change their modus operandi, and thus old crimes such as fraud, stalking, and harassment evolve into the new forms of crime online.

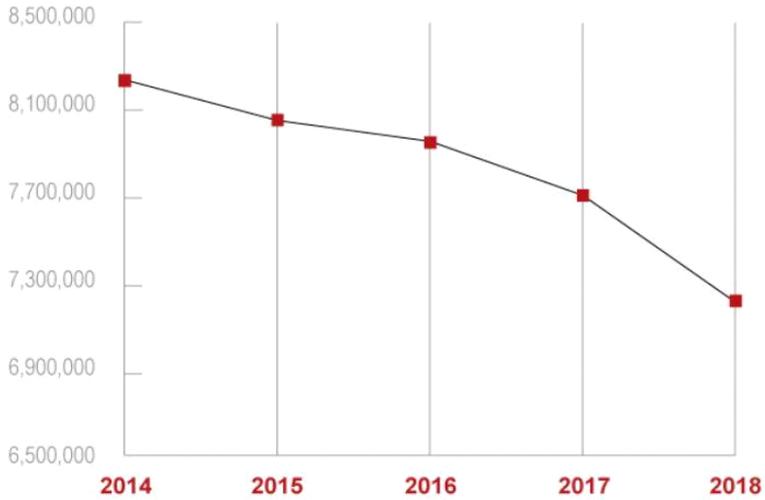
Based on Uniform Crime Reports (UCR) and National Crime Victimization Survey (NCVS), it is a commonly accepted fact that the rate of serious violent crime and property crime has shown a downward trend since the early 1990s (Rosenfeld & Weisburd, 2016).

»» [Figure 1–2–1] Violent Crime Trends in the U.S. (UCR: 1960–2016)



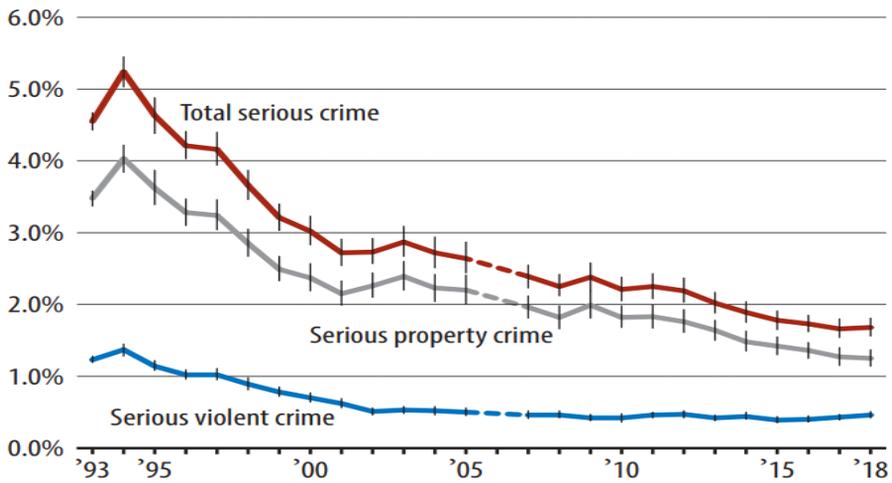
Source: FBI Uniform Crime Reports 1960–2016 (James, 2018)

»» [Figure 1-2-2] Property Crime Trends in the U.S. (UCR: 2014-2018)



Source: FBI Uniform Crime Reports 2018

»» [Figure 1-2-3] Violent and Property Crime Trends in the U.S. (NCVS)



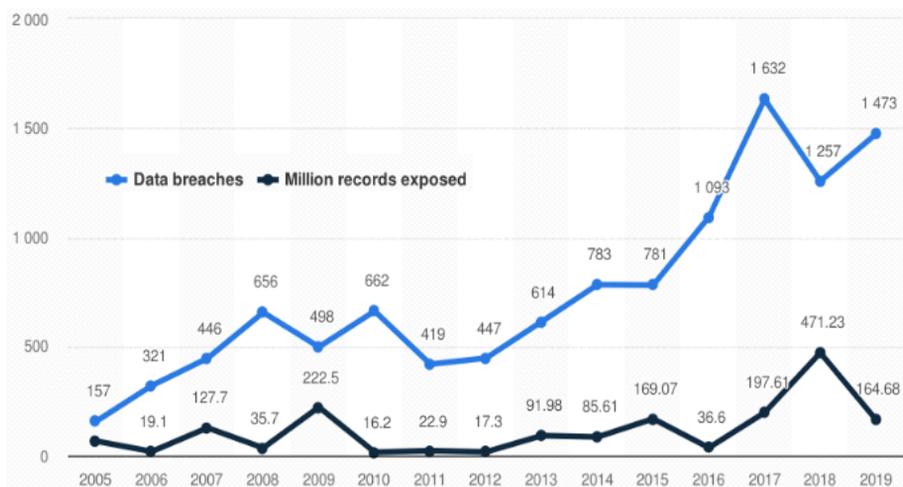
Source: Bureau of Justice Statistics, NCVS 1993-2018 (Morgan & Oudekerk, 2019)

Note: Percent of U.S. residents age 12 or older who were victims of total serious, serious violent, and serious property crime

However, this downward trend in crime is merely a façade, as the U.S. index crime rates did not capture the reality of the dramatic increases in crime directly or indirectly related to cyberspace. For example, while the property crime has

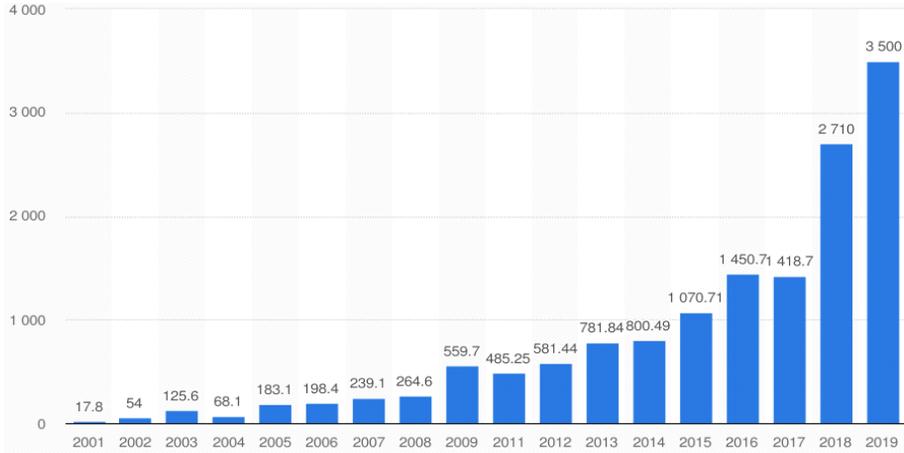
declined significantly, the annual number of sensitive digital data breaches have surged with increasing financial losses incurred by such breaches. In 2019, there were a total of 1,473 cases of data breaches, which exposed 164.68 million sensitive individual records combined. According to the Internet Crime Complaint Center (IC3), the monetary damage caused by cybercrime was estimated at 3.5 billion dollars in 2019. Another study showed that a threat of cybercrime is at an accelerating trend, and it is estimated that the cost of cybercrime would spike from 3 trillion in 2015 to 6 trillion in 2020 (Morgan, 2019). The White House Council of Economic Advisers also predicted that the United States is losing more than 109 billion dollars due to cybercrime annually (the United States White House, 2018). However, under current official crime statistics, the reality of cybercrime and financial losses have not been measured to represent the gravity of these issues.

»» [Figure 1-2-4] Number of Data Breaches and Records Exposed in the U.S. (in millions)



Source: Identity Theft Resource Center (ITRC) End-Year Data Breach Report 2005-2019 (Clement, 2020a)

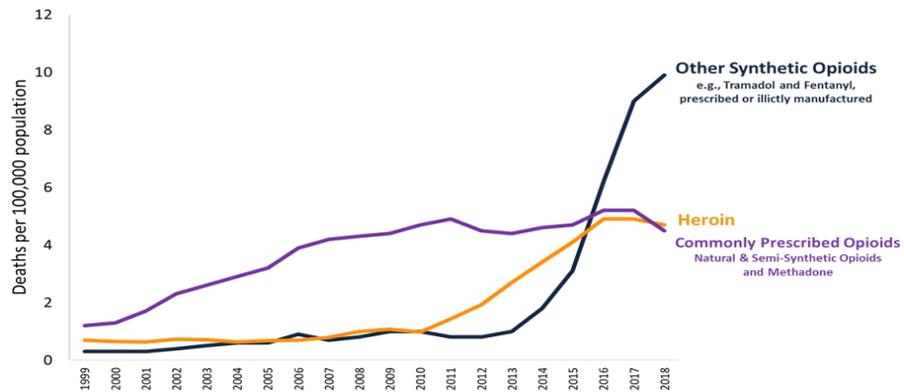
»» [Figure 1–2–5] Reported Monetary Damage in the U.S. (in millions)



Source: IC3 annual report 2001–2019 (Clement, 2020b)

Another example would be related to violent crime. Regarding why the violent crime rates have plunged dramatically since the early 1990s, many scholars believed that a consequence of the end of the 1980’s crack epidemic is one of the most influential factors (Rosenfeld & Weisburd, 2016). Deaths of opioid overdoses are not new in the United States. However, a new phase of the opioid epidemic – specifically Fentanyl-linked overdose, has been reported since 2013, concentrated on the New England area in the U.S. (Bebinger, 2019).

»» [Figure 1–2–6] The Rise in Opioid Overdose Deaths



Source: IC3 annual report 2001–2019 (Clement, 2020b)

Fentanyl is a synthetic opioid that gained a surge of popularity in the U.S. back in the end of 2013. This drug is said to be 50 to 100 times stronger, which can lead to immediate death when in contact (Centers for Disease Control and Prevention, 2017). During 2017 alone, approximately 30,000 people died due to Fentanyl overdose (CDC, 2018). According to the U.S. Drug Enforcement Administration (DEA), "illicit Fentanyl, fentanyl analogues, and their immediate precursors are often produced in China. From China, these substances are shipped primarily through express consignment carriers or international mail directly to the United States" (DEA, 2018, p.1).

»» [Figure 1–2–7] The Synthetic Opioid Transaction via Dark Web



Source: DEA(2018), Zezima(2017)

Opioids addicts or criminals use the Dark Web to order illegal drugs such as Fentanyl over eBay-like illicit markets (Zezima, 2017). These transactions are usually made using cryptocurrencies, digital assets that are not easily traceable. The ordered drugs are shipped via international packages, becoming harder to prevent such activities. Therefore, the first responders are postal inspection officers who lack the professional training to deal with such incidents, rather

than the DEA agents (Zezima, 2017). Although the FBI eventually shut down the illicit Dark Web market (Silk Road in 2013 and Alphabay in 2017), it is important to note that if someone can turn a profit, similar websites will proliferate. Given that the end of the 1980’s crack epidemic turned the violent crime rates downwards (Rosenfeld & Weisburd, 2016), it is too early to call that the Fentanyl epidemic will forecast significant upward trends in violent crime since 2013. However, it is clear that criminals’ modus operandi (MO) has changed.

Is crime migrating from offline to online? Little evidence exists so far (Wall, 2015). However, the lack of cybercrime data deters further research that is urgently needed to address the evolving nature of cybercriminal behavior.

## Section 3 | Issues in Measuring Cybercrime

### 1. Difficulty in Establishing the Definition of Cybercrime

It is very difficult to establish a specific definition of cybercrime, as there has not been a single definition agreed upon by scholars.

»» [Table 1–3–1] Prior Research on Cybercrime Classification

David Wall(2001)	Cyber-trespass	Hacking
	Cyber-deception/theft	Digital intellectual property right infringement
	Cyber-porn/obscenity	
	Cyber-violence	Cyberbullying
McGuire & Dowling(2013)	Cyber-enabled crime	Typically considered as a traditional offline crime which uses the Internet as its method of crime <ul style="list-style-type: none"> <li>• Cyberbullying</li> <li>• Cyberstalking</li> </ul>
	Cyber-dependent crime	‘Pure’ cybercrime (Cybercrime which cannot be committed without the Internet) <ul style="list-style-type: none"> <li>• Hacking</li> <li>• Malware</li> <li>• Distributed denial of service(DDos)</li> </ul>

Tcherni et. al.(2015)	Traditional offline crime	
	Hybrid crime	Combination of online-offline crime
	Cybercrime	Only possible through cyberspace

Delving into a few reports related in this matter, McGuire and Dowling (2013) categorizes cybercrime into two categories: 'Cyber-enabled crime' and 'cyber-dependent crime.' 'Cyber-enabled crime' can be considered as one of the traditional crime or crimes with internet MO, including but not limited to cyber bullying and internet fraud. 'Cyber-dependent crime' on the other hand is crime that cannot be committed without the Internet, such as hacking or virus attacks. Based on McGuire and Dowling's crime categorization, Tcherni and his colleges (2016) further expanded the categorization into 'offline crimes,' 'online crimes,' and 'hybrid crimes' that encompasses the both aforementioned. An example of a hybrid crime is cyberbullying, which the crime prevails online, but it leads to a series of offline bullying in physical spaces. Another example is online identity theft, which the criminals would obtain the victim's identity through dumpster diving.

In conclusion, many scholars have suggested a variety of classifications of cybercrimes, but yet to have found one that generally applied to all types of cybercrime, making it challenging to find suitable preventive measures of these crimes.

## 2. Problem with Counting Cybercrime

In order to accurately measure the effectiveness of prevention policies of cybercrime, there must be a specific guideline to count the occurrence of cybercrime. For example, Equifax, one of the major credit bureaus in the U.S., announced in 2017 that about 147.9 million consumers' data - such as Social security number, driver license number, and credit card number - were breached due to the Hacking. The data breach of Equifax exposed almost half of the American's credentials.

## 14 Comparative Study on the metric of cybercrime between the U.S. and South Korea

The question arises from whether we should consider these data breaches as one incident or 147.9 million cases because the crime occurrence rate largely depends on the methods of counting. In particular, in counting the number of victims per 100,000, there is a problem in that the measurement of performance varies greatly on how the number of cybercrime victims is defined.

»» [Table 1–3–2] Major Data Breach Cases in the U.S.

	Year	# of affected users	Details
Adobe	2013	153 million	<ul style="list-style-type: none"><li>• 3 million credit card records, login data</li><li>• Internationally affected</li></ul>
Target	2013	41 million	<ul style="list-style-type: none"><li>• Credit card verification codes and other sensitive data</li></ul>
Yahoo	2014	3 billion	<ul style="list-style-type: none"><li>• 500 million users (the real names, email addresses, dates of birth and telephone numbers)</li><li>• Internationally affected</li></ul>
eBay	2014	145 million	<ul style="list-style-type: none"><li>• Name, date of birth, password</li><li>• Internationally affected</li></ul>
Equifax	2017	148 million	<ul style="list-style-type: none"><li>• Social security number, driver license number, credit card number</li></ul>
Marriot International	2018	500 million	<ul style="list-style-type: none"><li>• Passport number, credit card number, and other sensitive data (travel &amp; personal information)</li><li>• Internationally affected</li></ul>

Source: CSO (2020)

Note: Estimated 2019 U.S. Population is 328 million (U.S. Census Bureau, 2019)

### 3. Estimating the Financial Costs of Cybercrime

According to the FBI (2019), the financial cost due to property crimes in 2018 (Burglary, Larceny-theft, Motor vehicle theft) is estimated to be approximately \$16.4 billion. Compared to this metric, according to the White House (2018), financial cost due to cybercrime is estimated to be \$109 billion, which is eight times more than FBI's traditional property crime cost of 16.4 billion.

However, one of the characteristics of cybercrime is that it is hard to estimate its financial costs, and therefore the metric depends on each institute. Similar

to those mentioned earlier, the reason why the financial costs differ stems from the fact that the methodological void of current crime statistics. This gap is well represented in the major data breach cases. For example, in cases of the breach of sensitive personal information due to Hacking, malware, or virus, it is hard to decide whether one should consider just the data loss or also the time and physical efforts to restore them. The scale of damage solely depends on what one decides to consider as financial costs. Also, in the case of cyber fraud, the financial cost measures can drastically change based on whether one decides only to consider immediate financial losses or also the aftermath as damage.

»» [Table 1–3–3] Estimated Financial Cost of Cybercrime

	Year	Estimated Cost(USD)	Details
Cybercrime	2019	3.5 billion	Internet Crime Complaint Center (2019) U.S. estimate
Cybercrime	annually	6 trillion	Morgan (2019) 3trillion (2016) →6 trillion (2020) International estimate
Cybercrime	annually	109 billion	United States White House (2018) U.S. estimate
Ransomware	annually	1 billion	FBI (2017) Global ransom payment estimates
Ransomware	2015	5 billion	Morgan (2019) Global ransomware damage estimated costs
Global Information Security Spending	2018	124 billion	Aitken (2019) International estimate
Global spending on cybersecurity	2017~2021	1 trillion	Morgan (2019) International estimate
Property crimes	2018	16.4 billion	FBI (2019) Burglary, Larceny–theft, Motor vehicle theft

#### 4. Limitation of Official Crime Statistics and Victimization Survey

Official cybercrime rates are generally criticized for underestimating the actual crime (Dupont, 2016). Taking the U.S. as an example, the Bureau of Justice Statistics (BJS) in 2012 reported that the estimated number of victims of cyberstalking is 0.035% among persons age 18 or older. However, studies showed that the estimates of cyberstalking victimization lie between 7.2% and 21.6%, with examples including unsolicited emails and harassment that cause one to be fearful.

»» [Table 1–3–4] Summary of Selected Cyberstalking Victimization Studies

Study	Operationalization of Cyberstalking	Estimate victimization Rate
Sheridan & Grant (2007)	Unsolicited emails and harassment via the Internet, which last less than four weeks on less than ten occasions	7.2%
Holt & Bossler (2009)	Online harassment through chatting in the last 12 months	18.9%
Baum et al. (2009)	Behavior which causes respondent to be fearful via unwanted or unsolicited emails	21.6% (among stalking victims)
Kraft & Wang (2010)	Repeated harassment through online communications that causes the victim to be fearful	9%

Like other cybercrime, the variations in cyberstalking victimization rate may be due to the lack of a unified definition of cyberstalking. There exist several U.S. federal laws, which prohibit cyberstalking. Example are shown below:

- 1) 18 U.S. Code §2261A. (Stalking): with intent to injure, harass, or intimidate another person, using any interactive computer service or electronic communication service or electronic communication system of interstate 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
- 2) 18 U.S. Code. §875 (Interstate communications): Whoever transmits in interstate or foreign commerce any communication containing any demand or request for a ransom or reward for the release of any kidnapped person.

- 3) 47 U.S. Code §223 (Telecommunications): Whoever, by means of a telecommunications device knowingly, makes, creates, or solicits, and initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene or child pornography, with intent to abuse, threaten, or harass another person

Some scholars even coined a Technology-Facilitated Sexual Violence (TFSV), which refers to “a range of behaviors where digital technologies are used to facilitate both virtual and face-to-face sexually based harms” (Henry & Powell, 2018, p.1). There exist several dimensions of TFSV and cyberstalking is related to the cyber-obsessive pursuit (Henry & Powell, 2018).

- 1) Online sexual harassment
- 2) Gender-and sexuality-based harassment
- 3) Cyber-obsessive pursuit (cyberstalking)
- 4) Image-based sexual exploitation
- 5) The use of a carriage service to perpetrate a sexual assault or coerce an unwanted sexual experience

Ostensibly, Korean official cybercrime statistics collect a large number of credible cases, even greater than some first-world countries. However, its credibility is not questioned enough due to inapplicable cybercrime definition and classification, inappropriate counting method, and unduly underestimates.

»» [Table 1-3-5] Reported Cybercrime in the South Korean

Field	Category	Group	Case Reported	Rate(%)
			149,604	100
Infringement of Cyber-network	Hacking	Identity theft, Information leak, Information pollution	2,178	1.9
	Denial-of-service attack		20	
	Malware		119	

18 Comparative Study on the metric of cybercrime between the U.S. and South Korea

Field	Category	Group	Case Reported	Rate(%)
	Others	Business interruption through computer	571	
Criminal Use of Cyber-network	Internet scam	Direct transaction scam, Cybermall scam, Video game scam	112,000	82.7
	Cyber Financial Crime	Phishing, Pharming, SMS phishing	5,621	
	Infringement of personal location data		246	
	Infringement of copyright		3,856	
	Others	Spam mail, Computer Scam	1,951	
Use of Illegal Contents	Cyber porn	Porn, Child porn	3,833	15.4
	Cyber gambling	Sports ToTo, Racing	3,012	
	Cyberstalking		20	
	Cyber defamation		15,926	
	Others	Production of false social security number	208	

Source: National Police Agency Internal Report, 2019

Information Protection Survey of 2018 reported that individuals' personal information infringement experience rate has been greater than 10% of the total sample size until 2018. Although the victimization rate of personal information infringement drastically decreased to 4.6% in 2018, this rate far exceeds the National Police Agency's official statistics, which reported to be 1.9%. Furthermore, the reported cyberstalking in South Korea is only 0.000134% (20/149,604 offenses) of the total cybercrime, which is far below the victimization rate in the U.S. These aspects of lacking the universal definition of cybercrime, as an example of cyberstalking, hinders the systematic measurement of cybercrime.

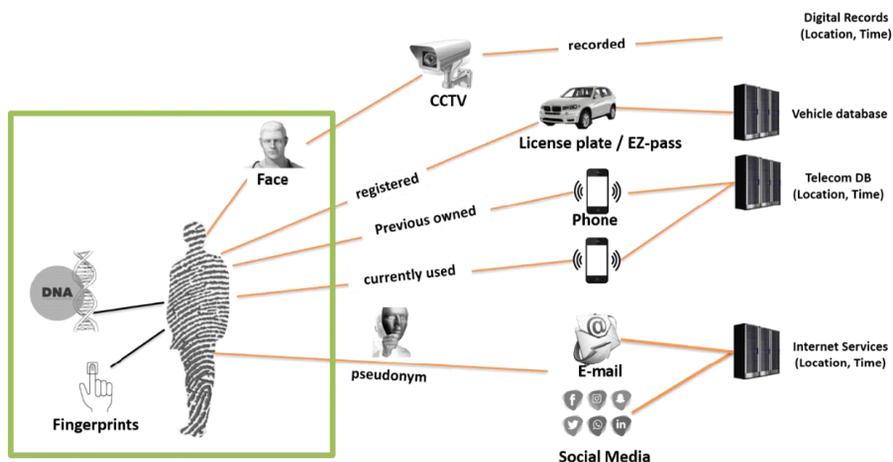
There are various reasons why the victims ultimately do not report the cybercrimes that they encounter. In many cases, the crime goes unreported if and when the financial loss is negligible, the victim believes the damage cannot be recovered, and the victim has low trust in the police.

## Section 4 | Scope of Research

First, to improve the current South Korean metric of cybercrime, this study will examine the wide range of the definition and the classification criterion of cybercrime, including UNODC, E.U., and the U.S. In addition, the alternative metric of cybercrime such as cybercrime victimization survey, self-reporting survey, and cybercrime cost analysis will be explored in the U.S. context. Importantly, this study will interview and survey cybercrime experts to examine what kind of cybercrime data has been used to develop policies and procedures to help law enforcement effectively cope with cybercrime. This study will provide policy implications for South Korean law enforcement on how to gather and interpret the cybercrime statistics.

Second, even traditional offline criminal, such as murder, now uses cyberspace as a part of its crime method. Therefore, it is a common thing for law enforcement to acquire digital evidence to solve the criminal case, along with securing physical evidence like DNA and fingerprints. As the digital evidence which provides time and location of criminal or crime has become an investigation standard, the traditional law enforcement system to separate police force for online/offline has become questionable. Furthermore, according to the deterrence theory, certainty criminals will be eventually caught and brought to justice is the essential factor for deterring crime. If current technology fails to identify criminals, law enforcement usually waits until new technology provides interpretations of previous evidence. This is why keeping up with technological advances is vital to law enforcement and why the reformation of law enforcement education and training system is necessary to respond to the increasing rate of hybrid crime that combines both online and offline criminal methods.

»» [Figure 1-4-1] Traditional and Digital Crime Evidence



In regard to the fusion of traditional offline crime and online crime (hybrid crime), this study will interview and survey experts in the United States law enforcement, asking about education and training. This study will provide suggestions for South Korean law enforcement on how to strengthen their cybercrime response capability.

## Section 5 | Methodology

We conducted personal interviews with law enforcement personnel from U.S. and South Korea. We were interested in how cybercrime data were defined, categorized, and collected. The interview was conducted in the period from July to October 2020. In the U.S., Massachusetts local police departments were contacted to recruit interviewees. We listed the top 10 local police departments, which cover the most populated county. Finally, Boston, Worcester, and Springfield local police department consented to the interview. Besides, state police and

Massachusetts Attorney's general office were contacted and willingly participated in the interview. Initially, face-to-face in-depth interviews were planned. But, due to the COVID-19 pandemic, most interviews were conducted via email or phone. Other than the interview, we gather publicized official data and internal cybercrime data from both South Korea and the U.S.



## Chapter 2

Comparative Study on the metric of cybercrime  
between the U.S. and South Korea

# DEFINITION OF CYBERCRIME

Seokbeom Kim · Yunsik Jang



## Chapter 2

# DEFINITION OF CYBERCRIME

---

### Section 1 | Overview

There exists no globally accepted definition of cybercrime so far because cybercrime is an interdisciplinary subject (UNODC, 2019). Therefore, the interpretation of cybercrime highly depends on the academic or professional point of view. For example, scientists focus on the use of technology in criminal activity, while criminal justice expert pivots on modus operandi or how the crime was conducted (UNODC, 2019).

### Section 2 | UNODC

UNODC produces and disseminates statistics on drugs, crime, and criminal justice at the international level. UNODC also works to strengthen national capacities to produce and distribute criminal justice statistics within the framework of official statistics. It develops several statistical standards and recommendations in the field of criminal justice in collaboration with international experts and relevant international organizations.

UNODC suggests cybercrime into three major categories, and the types of

cybercrimes included within each group. The criteria for this classification is “act descriptions” (UNODC, 2019).

- 1) Offenses against the confidentiality, integrity, and availability of computer data and systems are related to crime conducted to harm the operational capability and credentials of the cyber network system.
- 2) Computer-related offenses refer to crimes aimed to cause either private or economic advantage or damage.
- 3) Content-related offenses incorporate any criminal act committed through cyberspace involving illegal contents, ranging from child sexual abuse material to information related to the act of terrorism.

Each category includes several types of cybercrime.

»» [Table 2-2-1] Cybercrime Classification in UNODC

Types of Cybercrime	Examples
Offenses against the confidentiality, integrity, and availability of computer data and systems	① Hacking ② Denial of Service Attacks ③ Distributed Denial of Service Attacks ④ Defacement of website
Computer-related offenses	① Computer-related fraud or forgery ② Computer-related identity offenses ③ Spamming ④ Computer-related copyright/trademark offenses
Content-related offenses	① Child sexual abuse material ② Commercial sexual exploitation ③ Racist and xenophobic material ④ Act of terrorism material

Source: UNDOC (2013)

## Section 3 | E.U.

E.U., specifically Cybercrime Programme Office of the Council of Europe (C-PROC), is currently working on establishing the classification of cybercrime

under the project name of ‘global action on cybercrime extended (GLACY+).’ The main objective of this project is to set the guidelines for criminal justice statistics on cybercrime and electronic evidence (C-PROC, 2019). This report will update the E.U.’s definition or classification of cybercrime based on the progress of the draft.

## Section 4 | The United States of America

According to the National Incident-Based Reporting System (NIBRS) user manual, all offenses are categorized ‘Group A offenses’ and ‘Group B offenses’ (FBI, 2020). There are 28 Group A crime categories made up of total 71 Group A offenses; therefore, there are 71 Group A Offense Codes. The offense categories are listed below in alphabetical order (FBI, 2020). Identity Theft and Hacking/Computer Invasion were included as the types of fraud offenses on April 28, 2014.

»» [Table 2–4–1] Group “A” Offenses in NIBRS

NIBRS Offenses	NIBRS Codes	Crime Against
<b>Animal Cruelty</b>	720	Society
<b>Arson</b>	200	Property
<b>Assault Offenses</b>		
• Aggravated Assault	13A	Person
• Simple Assault	13B	Person
• Intimidation	13C	Person
<b>Bribery</b>	510	Property
<b>Burglary/Breaking &amp; Entering</b>	220	Property
<b>Commerce Violations</b>		
• Import Violations	58A	Society
• Export Violations	58B	Society
• Federal Liquor Offenses	61A	Society
• Federal Tobacco Offenses	61B	Society

28 Comparative Study on the metric of cybercrime between the U.S. and South Korea

NIBRS Offenses	NIBRS Codes	Crime Against
• Wildlife Trafficking	620	Society
<b>Counterfeiting/Forgery</b>	250	Property
<b>Destruction/Damage/Vandalism of Property</b>	290	Property
<b>Drug/Narcotic Offenses</b>		
• Drug/Narcotic Violations	35A	Society
• Drug Equipment Violations	35B	Society
<b>Embezzlement</b>	270	Society
<b>Espionage</b>	103	Society
<b>Extortion/Blackmail</b>	210	Property
<b>Fraud Offenses</b>		
• False Pretenses/Swindle/ Confidence Games	26A	Property
• Credit Card/Automatic Teller Machine Fraud	26B	Property
• Impersonation	26C	Property
• Welfare Fraud	26D	Property
• <b>Wire Fraud</b>	<b>26E</b>	<b>Property</b>
• <b>Identity Theft</b>	<b>26F</b>	<b>Property</b>
• <b>Hacking/Computer Invasion</b>	<b>26G</b>	<b>Property</b>
• Money Laundering	26H	Property
<b>Fugitive Offenses</b>		
• Harboring Escapee/Concealing from Arrest	49A	Society
• Flight to Avoid Prosecution	49B	Society
• Flight to Avoid Deportation	49C	Society
<b>Gambling Offenses</b>		
• Betting/Wagering	39A	Society
• Operating/Promoting/ Assisting Gambling	39B	Society
• Gambling Equip. Violations	39C	Society
• Sports Tampering	39D	Society
<b>Homicide Offenses</b>		
• Murder/Non-Negligent Manslaughter	09A	Person
• Negligent Manslaughter	09B	Person
• Justifiable Homicide	09C	Not a Crime
<b>Human Trafficking</b>		
• Commercial Sex Acts	64A	Person
• Involuntary Servitude	64B	Person
<b>Immigration Violations</b>		
• Illegal Entry into the United States	30A	Society
• False Citizenship	30B	Society

NIBRS Offenses	NIBRS Codes	Crime Against
• Smuggling Aliens	30C	Society
• Re-entry after Deportation	30D	Society
<b>Kidnapping/Abduction</b>	100	Person
<b>Larceny/Theft Offenses</b>		
• Pocket Picking	23A	Property
• Purse Snatching	23B	Property
• Shoplifting	23C	Property
• Theft from Building	23D	Property
• –Theft from Coin-Operated Machine or Device	23E	Property
• Theft from Motor Vehicle	23F	Property
• Theft of Motor Vehicle Parts or Accessories	23G	Property
• All Other Larceny	23H	Property
<b>Motor Vehicle Theft</b>	240	Property
<b>Pornography/Obscene Material</b>	370	Society
<b>Prostitution Offenses</b>		
• Prostitution	40A	Society
• Assisting or Promoting Prostitution	40B	Society
• Purchasing Prostitution	40C	Society
<b>Robbery</b>	120	Property
<b>Sex Offenses</b>		
• Forcible Rape	11A	Person
• Forcible Sodomy	11B	Person
• Sexual Assault with An Object	11C	Person
• Forcible Fondling	11D	Person
• Incest	36A	Person
• Statutory Rape	36B	Person
• Failure to Register as a Sex Offender	360	Society
<b>Stolen Property Offenses</b>	280	Property
<b>Treason</b>	101	Society
<b>Weapon Law Violations</b>		
• Weapon Law Violations	520	Society
• Violation of National Firearm Act of 1934	521	Society
• Weapons of Mass Destruction	522	Society
• Explosives	526	Society

Source: FBI, 2020

There are 13 Group B offense categories. They encompass all of the crimes for which the national UCR Program collects data that are not considered Group A offenses (FBI, 2020). The Group B offense categories listed below are in alphabetical order.

»» [Table 2-4-2] Group “B” Offenses in NIBRS

NIBRS Offenses	NIBRS Codes
<b>Bad Checks</b>	90A
<b>Bond Default (Failure to Appear)</b>	90K
<b>Curfew/Loitering/Vagrancy Violations</b>	90B
<b>Disorderly Conduct</b>	90C
<b>Driving Under the Influence</b>	90D
<b>Drunkenness</b>	90E
<b>Family Offenses, Nonviolent</b>	90F
<b>Federal Resource Violations</b>	90L
<b>Liquor Law Violations</b>	90G
<b>Peeping Tom</b>	90H
<b>Perjury</b>	90M
<b>Trespassing of Real Property</b>	90J
<b>All Other Offenses</b> • All crimes that are not Group A offenses and not included in one of the specifically named Group B crime categories listed previously	90Z

Source: FBI, 2020

The FBI overhauled its cybercrime measurement system in 2000. The key determinant of measuring cybercrime is whether a computer was used in the commission of the crime (Holt & Bossler, 2016; FBI, 2000). Therefore, according to the ‘Offense Lookup Table’ in the NIBRS manual (FBI, 2020, p. 53), cybercrimes such as identity theft, hacking, and online scams are categorized under ‘Fraud Offenses’ while remaining cybercrime would be placed under substantive offense.

»» [Table 2-4-3] Offense Lookup Table in NIBRS

Offense	Group A or B	Corresponding NIBRS crime category and notes	NIBRS Offense Code
Computer Crime	A or B	Classify same as substantive offense, e.g., Larceny/Theft, Embezzlement, or Fraud Offenses	Depends on circumstances
Fraud, Automated Teller Machine (ATM)	A	Fraud Offenses (Credit Card/Automated Teller Machine Fraud)	26B
Fraud, Credit Card	A	Fraud Offenses (Credit Card/Automated Teller Machine Fraud)	26B
Fraud, Hacking/Computer Invasion	A	Fraud Offenses (Hacking/Computer Invasion)	26G
Fraud, Identity Theft	A	Fraud Offenses	26F
Fraud, Mail	A	Fraud Offenses (False Pretenses/Swindle/Confidence Game)	26A
Fraud, Telephone	A	Fraud Offenses (Wire Fraud)	26E
Fraud, Wire	A	Fraud Offenses (Wire Fraud)	26E
Impersonation	A	Fraud Offenses (Impersonation) or Human Trafficking	26C, 26F, 64A, or 64B
Incendiary Device Offenses	A	Classify same as substantive offenses committed, e.g., Arson, Homicide, Aggravated or Simple Assault, Weapon Law Violations, or Destruction/Damage/Vandalism of Property	Depends on circumstances
Libel, Criminal	B	All other offenses	90Z
Lottery, Unlawful	A	Gambling Offenses (Betting/Wagering)	39A
Mail Fraud	A	Fraud Offenses (False Pretenses/Swindle/Confidence Game)	26A
Obscene Communication	B	All other offenses	90Z
Obscene Material	A	Pornography/Obscene Material	370
Obscene Telephone Call	B	All other offenses	90Z
Pornography	A	Human Trafficking (Commercial Sex Acts) or Pornography/Obscene material	64A or 370
Privacy, Invasion of	B	All other offenses	90Z
Slander, Criminal	B	All other offenses	90Z
Stalking	A	Assault Offenses (Intimidation)	13C
Swindle	A	Fraud Offenses or Human Trafficking	26A, 64A, or 64B

32 Comparative Study on the metric of cybercrime between the U.S. and South Korea

Offense	Group A or B	Corresponding NIBRS crime category and notes	NIBRS Offense Code
Telephone Fraud	A	Fraud Offenses (Wire Fraud)	26E
Threatening Telephone Call	A	Assault Offenses (Intimidation)	13C
Threatening Words or Statement	A	Assault Offenses (Intimidation)	13C
Transmitting Wagering Information	A	Gambling Offenses (Operating/Promoting/Assisting Gambling)	39B
Uttering	A or B	Fraud Offenses (False Pretenses Swindle/Confidence Game, Impersonation, or Welfare Fraud), Counterfeiting/Forgery, or Bad Checks	26A, 26B, 26D, 26F, 250, or 90A (Depends on circumstances)

Sometimes, NIBRS require the specification of location by the offender’s intent during the commission of the crime. If the crime location is related to ‘a virtual or internet-based network of two or more computers in separate locations which communicate either through wireless or wire connections,’ then the location of crime is coded as ‘Cyberspace’ (FBI, 2020, p. 95), which was added as a location code on the fall 2014. The suggested examples by NIBRS are shown below (FBI, 2020, p. 96).

[Example 1] Police received a phone call from an individual who reported he recently received a letter from a local business informing him the business’ computers were recently hacked from an external source and the customer’s personal information might have been compromised. The individual then reported he noticed someone had opened credit cards and other loans in his name. The agency should enter data value *26F = Identity Theft* into Data Element 6 (UCR Offense Code), since the individual’s personal information had been taken from the victim business and new accounts had been opened in the individual’s name. Because the data was obtained by the perpetrator through the use of the internet, data value *58 = Cyberspace* should be entered into Data Element 9 (Location Type). Had the internet not been available, then this crime could not have been committed in the matter upon which it occurred.

[Example 2] Police received a phone call from a business that reported their computers were recently hacked based on information identified by its information technology staff. The business reported the hacking/invasion offense appeared to have come from an internet address located in Iran. The LEA should enter data value *26G = Hacking/Computer Invasion* into Data Element 6 (UCR Offense Code). Data value *58 = Cyberspace* should be entered into Data Element 9 (**Location Type**) because *this crime could not have been committed if cyberspace had not been available.*

The specific definition of each offense is shown as below. (FBI, 2020, p. 33-34)

» [Table 2-4-4] The Definitions of Fraud Offense by NIBRS

False Pretenses/Swindle/ Confidence Games	The intentional misrepresentation of existing fact or condition or the use of some other deceptive scheme or device to obtain money, goods, or other things of value E.g.) – Renting a vehicle and failing to return it – Dining at a restaurant and failing to pay the bill – Misrepresenting information on an application for a firearm
Credit Card/Automatic Teller Machine Fraud	The unlawful use of a credit (or debit) card or automated teller machine for fraudulent purposes
Impersonation	Falsely representing one’s identity or position and acting in the character or position thus unlawfully assumed to deceive others and thereby gain a profit or advantage, enjoy some right or privilege, or subject another person or entity to an expense, charge, or liability that would not have otherwise been incurred
Welfare Fraud	The use of deceitful statements, practices, or devices to unlawfully obtain welfare benefits
Wire Fraud	– The use of an electric or electronic communications facility to intentionally transmit a false and/or deceptive message in furtherance of a fraudulent activity – This classification applies to those cases where telephone, teletype, computers, e-mail, text messages, etc., are used in the commission or furtherance of a fraud. – For example, if someone uses a computer to order products through a fraudulent online auction site and pays for the products but never receives them, this incident should be classified as 26E = Wire Fraud.

Identity Theft	<ul style="list-style-type: none"> <li>- Wrongfully obtaining and using another person's personal data (e.g., name, date of birth, Social Security number, driver's license number).</li> <li>- Including opening a credit card, bank account, etc. using a person's information</li> </ul>
Hacking/Computer Invasion	Wrongfully gaining access to another person's or institution's computer software, hardware, or networks without authorized permissions or security clearances.
Money Laundering	The process of transforming the profits of a crime into a legitimate asset

## Section 5 | South Korea

The South Korean law enforcement categorizes cybercrime largely under three different fields for detailed classification: 'infringement of cyber-network,' 'criminal use of cyber-network,' and 'crime involving illegal contents.'

»» [Table 2-5-1] Cybercrime Classification in South Korean

Field	Category	Group
Infringement of Cyber-network	Hacking	Identity theft, Information leak, Information pollution
	Denial-of-service attack	
	Malware	
	Others	Business interruption through computer
Criminal Use of Cyber-network	Internet scam	Direct transaction scam, Cybermall scam, Video game scam
	Cyber Financial Crime	Phishing, Pharming, SMS phishing
	Infringement of personallocation data	
	Infringement of copyright	
Use of Illegal Contents	Others	Spam mail, Computer Scam
	Cyber porn	Porn, Child porn
	Cyber gambling	Sports ToTo, Racing
	Cyberstalking	
	Cyber defamation	
Others	Production of a false social security number	

Source: National Police Agency Internal Report, 2019

## Chapter 3

Comparative Study on the metric of cybercrime  
between the U.S. and South Korea

# MEASURING CYBERCRIME

Seokbeom Kim · Alice Elizabeth Perry · Yunsik Jang



## Chapter 3

# MEASURING CYBERCRIME

### Section 1 | Introduction

In the area of cybercrime, the criteria for collection of statistical data may differ from other crime areas, mainly given by:

- the transnational character of cybercrimes and the necessity of using international cooperation channels during the investigation;
- the offenders and the victims could be from different jurisdictions;
- the use of technical devices for conducting the criminal activity and the necessity of seizing and examination of such devices;
- the use of electronic means of payment in the criminal activity;
- the use of specific instruments for the collection of electronic evidence during the investigations;
- the intensive use of electronic evidence to prove the criminal activity;
- the specificity of various cybercrimes cases (computer fraud, computer attacks, child pornography through computer systems, etc.) (C-PROC, 2019, p.12).

The structure of statistical data may vary accordingly due to the organizational structure of the police units and tradition. Nevertheless, in the area of cybercrime, the following data is recommended to be collected and outlined as being relevant for drawing the clear picture of the phenomenon:

- cases initiated, under investigation, or solved;
- cases under the supervision of prosecutors or subject to the competence of prosecutors;
- reported/identified offenses;
- identified suspects (age, sex, nationality, etc);
- measures applied (custody/arrest);
- investigative powers (interceptions, surveillance, authorized computer access, etc.);
- locations searched;
- victims identified (age, sex, nationality, etc);
- prejudice (preferably, as value in money);
- assets seized (by type, category, and value) (C-PROC, 2019, p.13).

Generally, the following five methods have been used as the measuring the extent and scope of cybercrime: 1) Official crime statistics, 2) Victimization survey, 3) self-report, 4) crime cost, and 5) fear of crime.

## 1. Official Crime Statistics

The official crime statistics from law enforcement agencies is the most widely used in the field of criminal justice. There exist various statistics, including Uniform Crime Reports (UCR) and National Incident-Based Reporting System (NIBRS) in the United States. South Korea is also producing official crime statistics from their law enforcement.

Official crime statistics are generally utilized to measure the effectiveness of law enforcement through the arrest rate and to establish crime prevention policies and standards for resource deployment. Ultimately, official crime statistics play a crucial role in enhancing public safety and quality of life. Yet, regardless of their expectation as national statistics, official crime statistics has its own

limitation of failing to recognize hidden crimes, alteration of crime trend, change of policy or law, and statistics practice which puts their credibility in question. This limitation is critical for sex crimes, domestic violence, and cybercrime.

## 2. Victimization Survey

Victimization survey directly asks general populous if they were exposed to the type of crime. This type of survey allows the measurement of non-reported cases or officially rejected cases by the law enforcement due to whatever reasons and provides various data regarding offender, victim and the case itself (Maxfield and Babbie, 2009: 200). Victimization survey poses its inherent shortcoming as a survey; hence it must be treated carefully while comparing them with official crime statistics from institutions.

In South Korea, the Korean Institute of Criminology (KIC) administered the Korean Crime Victim Survey (KCVS), using the nationally representative sample of households. The KCVS was collected every two years since 2008. Therefore, the KCVS are repeated cross-sectional survey data in nature in that the same information was gathered through questionnaires or interviews from a different sample of individuals and households during each Wave. The population universe (the target population) of the KCVS is the population in private households and household members aged over 14 years old.

Regarding cybercrime victimization, the KCVS first tried to examine the prevalence and extent of cybercrime, specifically phishing, in 2008.

»» [Table 3-1-1] Phishing Victimization in 2008

N = 10,671		Frequency	Percentage
Received a phishing scheme	Actual victim of a phishing	89	0.83
	Non-victim	7,590	71.13
Not received		2,992	28.04

Source: KIC (2009)

The 2008 KCVS showed that 71.96% of out of 10,671 respondents reported that they received a phishing scheme via email, telephone, or text message more than once up to a total of one hundred (KIC, 2009). Among 7,679 respondents, 89 respondents (1.2%) said they were the victims of phishing by sending money or giving their personal information.

Aside from South Korea, England has considered including cybercrime in victimization surveys since 2014, and Crime Survey for England and Wales (CSEW) has been finally administered to capture the cybercrime cases in 2016. According to 2019 CSEW’s estimate of crime rate, approximately 23,000cases of crimes that pertain to computer misuse occurred.

»» [Table 3-1-2] Cybercrime Victimization Survey of 2019 CSEW

Computer Misuse Offences	2018	2019	differences
Computer viruses/malware	5,215	5,536	6
Denial of service attack	254	136	-46
Denial of service attack (extortion)	224	30	-87
Hacking – server	841	298	-65
Hacking – personal	3,973	2,996	-25
Hacking – social media and email	8,936	11,101	24
Hacking – PBX/dial through	230	102	-56
Hacking (extortion)	3,710	2,936	-21
Total	23,383	23,135	-1

Source: Office for National Statistics, CSEW (2019)

The victimization survey in the U.S. is very scarce. According to the Bureau of Justice Statistics (BJS), there are a few victimization surveys regarding cybercrime (BJS, 2019)

»» [Table 3-1-3] Cybercrime Victimization Survey in the U.S.

Survey	Survey Year	Major Findings
Cybercrime against Businesses	2005	<ul style="list-style-type: none"> <li>• 67 percent of responding businesses (7,818) detected cybercrime</li> <li>• The first report to provide data on monetary loss and system downtime resulting from cyber incidents</li> </ul>
National Computer Security Survey	2001	<ul style="list-style-type: none"> <li>• Almost three-fourths of businesses were victimized by cybercrime</li> </ul>

Source: BJS (Cybercrime, <https://www.bjs.gov/index.cfm?ty=tp&tid=41>)

### 3. Self-Reporting

A self-reporting survey includes a survey for both offender and victim. This provides useful information about hidden crimes (not reported to agencies), crimes against social legal interest that might not have any victim. Unlike the victimization surveys that generally conducted nationwide, self-reporting collects data for specific criminal acts.

In order to capture the extent of cybercrime victimization, Australian Cyber Security Centre (ACSC) established the self-report system for cybercrime victimization, known as “Report Cyber” (Australian Cyber Security Centre, 2020) on 1 July 2019, which replaced the prior Australian Cybercrime Online Reporting Network (ACORN). Since the goal of Report Cyber is to understand the extent of cybercrime, not all reported cybercrimes to the Report Cyber are investigated by Australian law enforcement agencies. The victim of cybercrime in Australia can file a self-report the following incidents (Australian Cyber Security Centre, 2020).

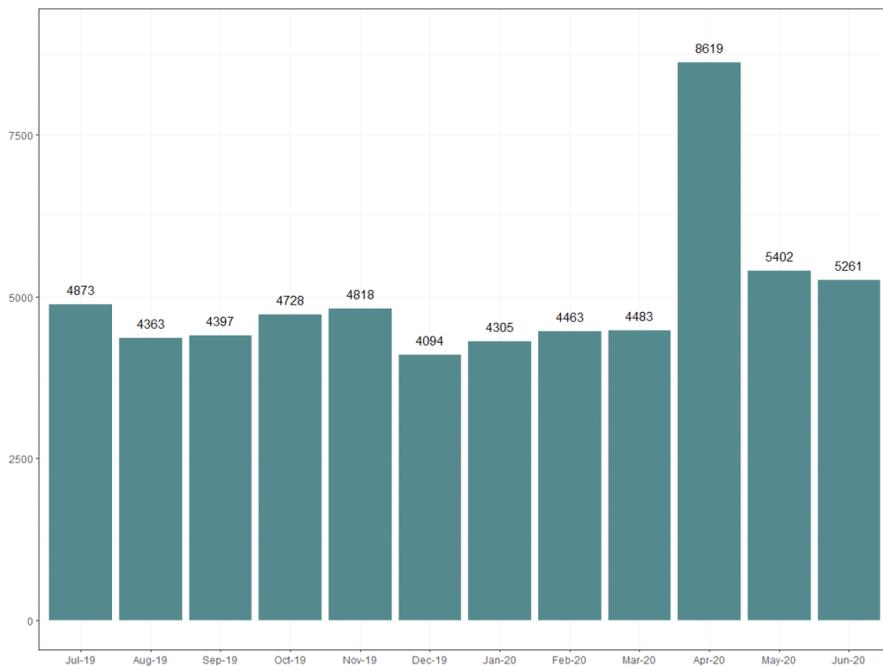
»» [Table 3-1-4] Self-reporting Categories of Cybercrime in Australia

Cyber abuse	<ul style="list-style-type: none"> <li>• When someone is bullying, harassing or stalking victim online</li> </ul>
Online Image Abuse	<ul style="list-style-type: none"> <li>• When someone has shared online, or is threatening to share online, intimate images or videos of victim</li> </ul>
Online shopping fraud or romance fraud	<ul style="list-style-type: none"> <li>• Victim have been deceived into sending money or goods to someone online</li> </ul>

Identity theft	<ul style="list-style-type: none"> <li>When someone has used victim’s personal or business identity information and accessed victim’s online accounts</li> </ul>
Email Compromise	<ul style="list-style-type: none"> <li>When victim received an email containing fraudulent information that deceived victim and led victim to send money</li> </ul>
Internet fraud	<ul style="list-style-type: none"> <li>When victim clicked on a phishing link or gave someone remote access to a computer or device, and money may have been taken from victim’s account(s)</li> </ul>
Ransomware or malware	<ul style="list-style-type: none"> <li>When victim’s system or devices have been compromised and someone may be demanding money</li> </ul>

In 2019, one in three Australian adults were impacted by cybercrime (Department of Home Affairs, 2020). From July 2019 to June 2020, ReportCyber received total 59,806 self-reported cybercrimes (Australian Cyber Security Centre, 2020).

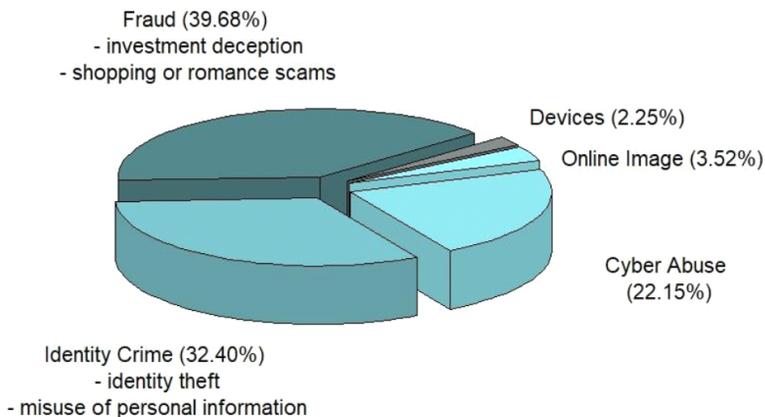
»» [Figure 3-1-1] Trend in Self-reporting of Cybercrime Victimization in Australia



Note: The spike in April 2020 relates to an Australian cybercrime campaign.  
 Source: ACSC annual cyber threat report (2020).

Among 59,806 self-reported cybercrimes, 'fraud (39.86%)' is the largest category of reported cybercrime, followed by identity crime (32.4%), cyber abuse (22.15%), and online image (3.52%).

»» [Figure 3-1-2] Self-reported Cybercrime in Australia (2019.7.1~2020.6.30)



#### 4. Crime Cost

The cost of crime cannot be calculated by simply summing up a cost of transgression. The crime not only impacts the victim but also cause society-wide collateral economic, physical, and political damage. Therefore, the concept of crime cost must include multiple aspects along with financial loss, inflicted physical injury, hospitalization of individual, and work loss. Sometimes, from a financial perspective, a cost-benefit analysis (also known as a benefit-cost analysis) is conducted. Cost incorporates tangible financial losses as well as the external and social costs of crime control. The Korean Institute of Criminology conducted the cost-benefit analysis in 2010 and 2011. In 2008, total social crime cost for violent crime and property crime was estimated up to 158 trillion won, approximately 16.2% of the total GDP. This is a piece of alarming news since it is 16 trillion won greater than a British crime survey conducted in 1999 with

identical methodology. Also, South Korean analysis showed a higher result cost than that of Britain, while response cost paid by law enforcement was lower.

## 5. Fear of Crime

Unlike previous indicators, the fear of crime reflects the effectiveness of crime prevention efforts instead of numeric values of occurred crimes. This is conducted with a nationwide victimization survey or independently if it were to test out specific policies applied in a limited region.

Since the early 1970s, fear of crime has been one of the most controversial topics in the study of criminology, as well as crime policy responses (Vieno et al., 2016). Nowadays, it is commonplace to describe the so-called fear of crime paradox (Grohe, DeValve, & Quinn, 2012; Warr, 2000) – overestimating the probability of becoming a victim of crime compared to the actual crime statistics – as the starting point of literature.

From a psychological perspective, fear of crime exerts negative impacts on one's mental health regardless of a person's prior victimization experiences, such as inducing anxiety or stress, lowering confidence, experiencing sleeping disturbances, and panic attacks (Miethe, 1995) and thus may potentially lead to serious and long-term emotional consequences (Ferraro, 1996; Miethe, 1995). Furthermore, once individuals have mistaken beliefs that violent crimes have gone up, they will change their behaviors in response (Wilson & Kelling, 1982). At the individual level, these changes begin with their protective (e.g., carrying a weapon or fortifying homes) and/or avoidance behaviors (e.g., avoiding unsafe areas) (Kappes, Greve, & Hellmers, 2013; May, Rader, & Goodrum, 2010; Rader, Cossman, & Allison, 2009; Warr, 1985; Wilcox, Jordan, & Pritchard, 2007; Wilcox, May, & Roberts, 2006). These behavioral changes lead people to withdraw from their communities and ultimately to weaken the informal social control (Wilson & Kelling, 1982). At the community level, neighborhoods or entire cities might

go into urban decay (Miethe, 1995; Wilson & Kelling, 1982) because fear of crime motivates residents to move to perceived safer places (Drakulich, 2015). Taken together, understanding the dynamics of fear of crime can be the first step in addressing problems resulting from it, and thoroughly specifying the causes of fear of crime could also be an important prerequisite for establishing relevant criminal justice policy.

## Section 2 | Current Practices within South Korean Law Enforcement

### 1. Investigative Procedure

If an individual were a victim of cybercrime, he or she can file a complaint online through a cybercrime report system on the Korean National Police webpage as well as offline by visiting nearby police stations.

» [Figure 3–2–1] Cybercrime Reporting System 1



Source: <http://www.police.go.kr/www/security/cyber.jsp>

After personal identity verification, the presumptive victims can freely select their types of victimization among three major categories of cybercrime: Infringement of cyber-network, Criminal use of cyber-network, and Crime involving illegal contents

and its subcategories such as Hacking, malware, ransomware.

▶▶▶ [Figure 3-2-2] Cybercrime Reporting System 2

신고 접수 대상을 선택해 주세요.  
하단의 내용을 잘 읽어보신 후 신고 접수될 피망하시는 사형에 해당하는 범죄 유형을 선택해 주세요.  
신고를 피망하시는 유형을 직접 검색하실 수도 있으며 세부유형에서는 '설명보기' 버튼을 클릭하시면 상세 설명을 확인하실 수 있습니다.

**! 자주 접수되는 대표적인 범죄 유형**

 서버사기	 사이버 명예훼손·모욕	 디지털성범죄	 해킹	 소액결제	 초권만남 사기
 메신저피싱	 음결제피싱	 로맨스스캠	 인터넷 투자사기	 사이버도박	 사이버 스토킹

**1 범죄유형** 검색어를 입력해 주세요. 🔍

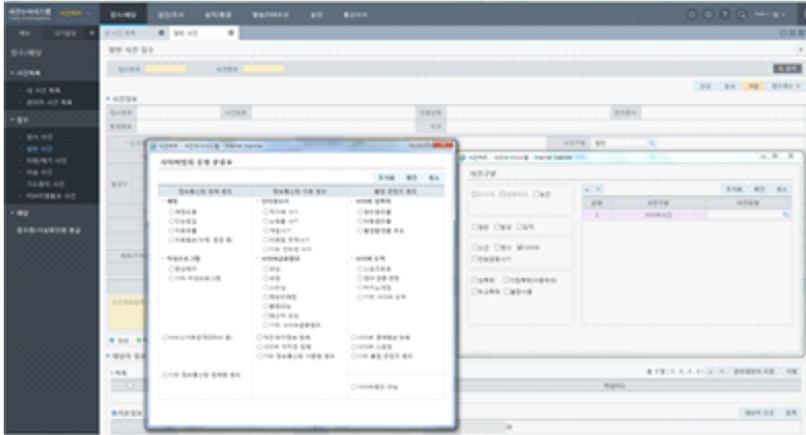
전체
해킹
소액결제
서비스기부공격
악성프로그램
기타정보통신망침해형 범죄
사이버도박

**2 세부유형** 검색어를 입력해 주세요. 🔍

단순침입	설명보기
자료유출	설명보기
자료훼손	설명보기
계정도용	설명보기

The majority of cybercrimes reported through cybercrime report systems are usually minor non-criminal cases. Hence, before the actual investigation starts, the investigator counsels the possible victim to determine whether the case belongs to a criminal offense; If the complaint is not a criminal case, then the complaint is rejected or provided with an online response. If the complaint is a criminal case, then the case is registered to KICS as a temporary case.

»» [Figure 3-2-3] Official Cybercrime Registering System (KICS)



Cybercrime Investigation and prosecution follow the procedure of ‘internal investigation’ ‘Investigation’ ‘Prosecution.’ Probable cause is required to initiate an investigation. A case under investigation is classified as a formal cybercrime case, and it is officially recorded and tracked.

## 2. Official Cybercrime Statistics

In 2011, South Korean police received 166,880 complaints, and approximately 55.7% of those complaints cases was determined as criminal cases. In contrast, the U.S. IC3 investigated only 37.3% of a total of 915,748 claims reported to the IC3, which is 18% less than what South Korean police investigated. Besides, there exists no official cybercrime statistics published at the police level in the U.S.

»» [Table 3-2-1] Types of Reported Cybercrime (South Korea)

Year	Cases	Fraud		Cyber violence	Illegal websites	Identity scam	Hacking	
		Electric transaction	Games				System	Private
2012	139,234	52,921	12,308	19,581	5,704	13,788	4,940	28,886
2011	166,880	60,619	17,990	17,749	5,968	21,299	3,415	38,221
Difference (%)	-16.6%	-12.7%	-31.6%	+10.3%	-4.4%	-35.3%	+44.7%	-24.4%

Source: Korean National Police Internal Data (2013)

Reported internet scams are 112,000 cases, which account for 74.9% of total cybercrime. Frauds are mainly minority scams such as direct transaction scams, online shopping scams, and internet game related scams. Within the use of illegal contents category, the majority of reported cases of 15,926 (10.6%) are related to internet defamations, followed by cyber porn (3,833 cases, 2.6%). In infringement of cyber-network category, hacking recorded the highest number of cases of 2,178 (1.5%). In 2018, a total of 149,604 cases was reported, and approximately 75% of the cases were solved by arrested. In terms of the arrested case rate, Internet scams (78.3%), cyber porn (85.6%), and cyber gambling (97.8%) showed relatively high arrest rate. This is expected since evidence of those offenses were identified relatively easily during the investigation. On the other hand, Hacking (26.8%) and Malware (42%) were less arrested since these offenses were more complicated to investigate. It is a significant reduction in arrest rate compared to the Internet scam. Among the cases reported through the online cybercrime report system, 92,665 cases went through law enforcement investigation. Assuming that this rate is identically applied to official national crime statistics, 78.2% of total cases rely on the Internet to be recognized.

»» [Table 3-2-2] Reported/Arrested Cases by the Types of Cybercrime

Field	Category	Case Reported	Case Arrested	Reported/Arrested Rate (%)
		149,604	112,133	75.0%
Infringement of Cyber-network	Hacking	2,178	584	26.8%
	Denial-of-service attack	20	14	70.0%
	Malware	119	50	42.0%
	Others	571	254	44.5%
Criminal Use of Cyber-network	Internet scam	112,000	87,714	78.3%
	Cyber Financial Crime	5,621	2,353	41.9%
	Infringement of personallocation data	246	142	57.7%
	Infringement of copyright	3,856	2,467	64.0%

Field	Category	Case Reported	Case Arrested	Reported/Arrested Rate (%)
	Others	1,951	1,250	64.1%
Use of Illegal Contents	Cyber porn	3,833	3,282	85.6%
	Cyber gambling	3,012	2,947	97.8%
	Cyber stalking	20	50	250.0%
	Cyber defamation	15,926	10,889	68.4%
	Others	208	137	65.9%

Source: National Police Agency Internal Report, 2019

In 2018, Korean law enforcement recognized 1,580,751 cases, and 9.4% of them were cybercrime.

▶▶▶ [Table 3-2-3] Reported/Arrested cases by the Types of Traditional Crime

Category	Case Reported	Case Arrested	Reported/Arrested Rate (%)
Total crime	1,580,751	1,328,609	84.0%
Aggravated Assault	287,611	112,133	39.0%
Theft	176,809	106,669	60.3%
Murder (attempted murder)	797	782	98.1%
Sexual assault	23,478	22,644	96.4%
Robbery	821	821	100.0%

Source: National Police Agency Internal Report, 2019

### 3. Other Cybercrime Statistics

Other than law enforcement, there are various institutions equipped online cybercrime reporting system. There exists an issue: many reported cases were neglected during their transfer to investigation or statistics count leading to a miscommunication between institutions. Each institute receives case reports for their own objectives.

»» [Table 3-2-4] Institutions with Online Cybercrime Reporting System

Institutions	Department/Subgroup	Report Types
National Police Agency	Cyberterrorism Response Center	Cybercrime
Supreme Prosecutors' Office	Homepage	General crime
Ministry of Culture, Sports and Tourism	Game Rating and Administration Committee Video Game Rating System	Illegal game contents, illegal currency exchange
	Copyright Protection Center	Copyright violation
National Gambling Control Commission		Illegal gambling
Korean Communications Commission	Korean Communication Standards Commission	Illegal website
Korean Communications Commission Ministry of Science, ICT and Future Planning	Korea Internet & Security Agency	Spamming, identity theft, phishing, hacking, worm/virus distribution
Korean Intellectual Property Office	Counterfeiting and Acts of Unfair Competition Center	Counterfeit goods
Fair Trade Commission	Korea Consumer Agency	Damage relief
Financial Supervisory Service		Illegal private loan, illegal cyber finance
National Intelligence Service		Cyberthreat
Consumers Union of Korea	Seoul Cybermarket Center	Phishing/scam website

Unfortunately, even though the majority of them can be considered as criminal cases, they are not transferred to law enforcement forces, making it harder to comprehend the criminal situation. Specifically, the information communications network act dictates that if the internet user experiences, for example, identity leak, then they must report to the Korean Communication Commission while service provider and system manager must report directly to the Minister of Science, ICT, and Future planning or Korean Communication Standards Commission. If the service provider illegally collects other personal identity through cyber-network scamming, they must be reported to the Korean Communication Commission or Korean Communication Standards Commission. Some of them charge fine if not reported accordingly.

»» [Table 3-2-5] Trends in Malware Damage and Hacking Incidents in South Korea

Year	2008	2009	2010	2011	2012
Malware damage	8,469	10,395	17,930	21,751	21,399
Hacking incidents	15,940	21,230	16,295	11,680	19,570

Source: 2013 National Information Protection Policy

Also, when a national institute recognizes or identifies cyberterrorism attempts, 'National cybersecurity management guideline' dictates to report to National Intelligence Service and National Security Department, preventing appropriate investigation of these cases and records for statistics. Until 2009, cyber-attack on national institutions were published through National Information Protection Policy, yet past 2010 it is no longer public.

Therefore, it is hard to collectively view how institutions' interaction and actions impact cybercrime and the determine policy to prevent cybercrime. Let alone crime control effect from crime investigation. This adds complexity to evaluate how effective and efficient policies and efforts to protect information. It also makes it hard to investigate and profile how criminals, criminal acts, and victims are related via various sources of information.

From the law enforcement perspective, the Criminal Procedure Act 234-2 states that if a government official recognizes criminal acts during their duty, it must be reported. Crime investigation is a key to criminal justice system and is one of the most important responsibility of a nation. Hence government officials hold the responsibility to pursue greater good and report any criminal acts they recognize. Specifically, Cyber-security management guidelines report criminal acts to law enforcement as a voluntary, leaving a possibility of violating constitutional right of free speech.

»» [Table 3-2-6] Deletion and Cancellation of Contents Harmful to Juveniles

	Total in 2013							Contents harmful to juveniles decision and decision cancellation*
	Cases	Correction request					Others	
		Total	Deletion	Cancellation	Access denial	Others		
Gambling	37,580	35,899	766	6,232	28,894	7		
Illegal food/drugs	22,382	22,204	8,538	907	12,759	0		
Pornography	34,634	32,330	4,767	8,126	17,608	1,829		
Infringement	4,768	3,135	1,388	2	1,745	0	7	
Other violation**	11,350	10,832	7,527	1,647	1,652	6		
Total	110,714	104,400	22,986	16,914	62,658	1,842	397	
							1	

Source: Korean Communication Commission 2013 Statistics for Communication review, [www.kocsc.or.kr](http://www.kocsc.or.kr)

Note: \* Contents harmful to juveniles' decision and decision cancellation

\*\* Other violations: copyright infringement, illegal identity transaction, Violation of National Security Act

Copyright Protection Center is designated as a regulation enforcement for illegal contents and copyright violations by the Ministry of Culture, Sports and Tourism; in 2012, Copyright Protection Center monitored more than 910 thousand cases for copyright violations.

»» [Table 3-2-7] Copyright Violation Incidents

Year	2010	2011	2012	2013	2014	2015	2016
Cases	278,408	376,475	919,812	1,660,097	1,934,647	2,394,879	2,230,018
Contents	34,395,367	86,338,298	76,368,247	130,310,047	141,739,494	117,455,201	29,133,588

Source: Copyright Protection Center, Annual Copyright Protection Report 2010-2017

#### 4. Self-Reporting

Self-report may be used as a supplement, though with limited applications, to identify hidden crimes not recognized by law enforcement and victimization surveys. Until recently, there had been no attempt in Korean law enforcement to conduct self-report on cybercrime. The Korea Internet & Security Agency recently

conducted a self-report on cybercrime during their own cybercrime survey.

According to this survey in 2013, 29.2% of 1500 K12 students and 14.4% of 1,000 general subjects have inflicted violence over a cyber network between 2012 and 2013. A victimization survey conducted alongside indicated that 30.3% of K12 students and 33.0% of people experienced cyber violence.

»» [Table 3-2-8] Self-Reporting Victimization Survey of 2013

Cyberviolence Type	K12 Students	General Populous
Cyber verbal abuse	25.2	14.4
Internet defamation	4.8	8.2
Cyber stalking	2.2	2.2
Cyber sexual violence	1.9	0.8
Identity leak	3.6	0.8
Cyberbullying	5.6	7.0
Total	29.2	14.4

Source: Korea Internet & Security Agency, Cyberviolence Survey, 2013

In this survey, cyberviolence was classified into ‘cyber verbal abuse,’ ‘Internet defamation,’ ‘Cyberstalking,’ ‘Identity leak,’ and ‘Cyberbullying,’ and asked detailed questions within a survey. For example, under cyber verbal abuse category, questions asked if the subject has personally attacked, or insulted via Internet, SMS messages or other network devices. It is unknown how many of them can be reported and recognized as a criminal case by the law enforcements. 85.1% of K12 students were already aware of cybercrime penalties and punishment, yet more than 50% showed distrust against committees regarding school bully or the Cyber Bureau of police agencies. Such views can lead to general distrust of criminal justice structures and protection for victims, hence further education regarding the difference between criminal cases and non-criminal cases and how the criminal justice system acts.

The KIC conducted a survey on criminal act using SNS environment in 2014, and 2.9% of 1,000 respondents answered that they have committed a sex crime,

fraud, stalking, impersonation, and moral violations. The survey argued that considering its openness, connectivity, and the tendency of information distribution, an attempt to reduce privacy intrusion, defamation, and pornography must be considered with caution.

»» [Table 3-2-9] Self-Reporting Victimization Survey of 2014(N=1,000)

Total case rate	Sex crimes	Fraud	Staking	Impersonation	Moral violation
2.9%	1.2%	0.4%	0.6%	0.8%	0.8%

Source: KIC, Survey of criminal act on SNS environment and criminal justice response, 2014

## 5. Victimization Survey

One example of assessing damage due to cybercrime is an annual Information Protection Survey conducted by the Korea Internet & Security Agency. In 2012, 6.3% of individuals suffered hacking, 9.2% suffered adware or spyware, and 18.8% experienced worm or virus attack. Among the people who suffered damage from the adverse effect of the Internet, only 18.4% reported and filed their cases to agencies or law enforcement, increasing reporting case rate by 4.7%. Korea Internet & Security Agency (KISA) spectates populations accessible to the Internet to be 38.12 million. Hence victims of Hacking, spyware, and worm or viruses are approximately 2.4 million, 3.5 million, and 7.16 million each. The combined number of victims is already 13.06 million, and 24 million cases were actively reported to institutions. During the same time period, law enforcement recorded 33,826 cases of cyberterrorism, and only 9,607 cases were reported for statistics. According to KISA, there were only 40,000 reported cases. This low number of cases signifies that the majority is recorded as civil cases rather than possible criminal cases. Therefore, most cases are left out from the record. This small number also shows that the validity and credibility of the data is questionable.

»» [Table 3-2-10] Information Protection Survey of 2013

Type	Hacking	Adware & Spyware	Worm & Virus
Total	6.3	9.2	18.8
12-19	5.2	8.7	16.1
20s	6.8	10.5	28.4
30s	6.1	10.2	17.1
40s	9.0	9.7	18.0
50s	2.6	4.9	11.8

Source: 2013 Information Protection Survey

For surveying companies, the subject group was designated as any company with computers that have more than five people. Compared to 2011, the identity leak experience rate has increased from 0.5% to 0.6%. It is predictable that the estimated victimized companies will outnumber previously approximated case of 2851. 1.4% of companies experienced cases related to information protection in 2012, with an estimated case of 6654. 81% of the reported attacks came externally, like Hacking, and 2.9% were deliberate information leaks due to internal personnel, while 16.7% were accidental. Only 29.7% of companies were reported to related agencies after the attack. It is interesting to note that all information service companies reported, while only 2.1% and 1.6% of private service or other service companies reported to law enforcement, respectively. This is expected since Personal Information Protection Act and Information Communication Act obligated any information service companies to report if any cyber attacks occur; there is no proof of evidence that 100% of occurred cases were reported.

»» [Table 3-2-11] Information Statistics Collection 1

Type	Victim/Subject	Case report rate and crime cost occurrence rate
Total security breach cases	76,761/2,440,146(3.1%)	N/A
Computer worm Trojan virus	69,425/2,440,146(2.8%)	Case Reported 10.8% Cost occurred 40%
Attempt of illegal external access on data	3,109/2,440,146(0.1%)	Case Reported 8.2% Cost occurred 39.9%

Type	Victim/Subject	Case report rate and crime cost occurrence rate
DoS attack	5,798/2,440,146(0.2%)	Case Reported 62.3% Cost occurred 41.1%
Information leak	4,724/2,440,146(0.2%)	Case Reported 21.5% Cost occurred 12.2%

Source: National Information Society Agency, 2013 Information Statistics Collection, 2013

UNODC administered surveys for 21 countries to examine the intrusion rate. The survey results found that the cybercrime victimization rates were ranged from one to 17% of the internet users. Such victimization rate was far exceeding traditional crime victimization rate of five percent. Besides, European companies reported two to 16% of victimization rate against cyber-attack including intrusion or phishing.

»» [Table 3-2-12] Information Statistics Collection 2

Type	Experience/Inexperience	Victimization rate
Private Business	45,300/1,820,148	2.4
Corporation	17,545/361,487	4.6
Non-business corporation	5,976/48,829	10.9
Unincorporated association	5,075/97,677	4.9
Local authorities	2,866/35,244	7.5

Source: UNODC (2013) Phishing attempts and illegal access on email

Victimization surveys may only provide limited information on whether or not the case can be recognized as a crime, yet it also includes information with regard to hidden crime. Korea Internet & Security Agency (2013) reported that 18.4% of responders and 29.7% of companies reported to law enforcement when they were victimized by cybercrime.

For subjects of cybercrime in SNS survey, only 2.7% of responders reported to law enforcement, yet none of them were able to capture the offender. Among the other responders who did not report to law enforcement, 15.6% said they were too lazy, 7.8% answered that they did not have sufficient evidence, and

1.7% did not know if they could file a case to the police.

However, the analysis of victimization surveys or self-report must be conducted with caution. One primary reason is that victimization surveys cannot identify if one offender has committed multiple crimes at once. For instance, leakage of personal identity of millions of people often occurs in Korea, and the size and awareness of leaked information may generate multiple victims of an identical case. Such cases may be misinterpreted and be less useful to assess crime and develop response systems.

## 6. Summary

A few observations can be made reviewing official national statistics from law enforcement. Due to hidden crimes, it is estimated that only 24%, 67.9%, and 73% of a sex crime, theft, and violent crimes are reported to law enforcement. On the other hand, 13.06 million people experience victimization in identity theft according to the victimization survey by Korea Internet & Security Agency. However, only 30,000 cases were reported to police, and 9,600 cases were investigated, which are 0.0025% and 0.0007% of the total expected victims. Even with the Korea Internet & Security Agency's internal report system, it only adds 40,000 additional cases. Furthermore, investigated cases are mostly comprised of illegal access or stealing accounts. This tendency of low report rate also occurs in general cybercrime.

### Section 3 | Current Practices in the U.S. Law Enforcement

#### 1. Federal and State Criminal Jurisdiction in the U.S.

Federal and state jurisdiction of crime in the United States is best understood with a useful summary of its historical context. The United States, though often

referred to as a 'democracy,' meaning one citizen and one vote and elected leaders who make decisions for its populous, is a form of government without a constitution. More concisely, the United States is a republic. "A republic ... is a form of government in which elected leaders operate under a constitution that protects the best interests of the nation and its people by limiting the power of its elected officials" (Carlan, P.E., Nored, L.S. & Downey, R.A., 2016).

The United States system of government is a compromise between the founders of the republic. It evolved after much negotiation, dispute and concession between the strong national government advocates, and strong state's rights advocates. The Constitutional Convention met in 1787 with fifty-five illustrious political leaders in attendance having been elected by their state governments to represent the interests of the state. James Madison was an ardent proponent of a strong national government. He believed that the states' power and their own individual interests were a threat to the new country. The representative from New York, Alexander Hamilton, a champion of a strong national government, maintained that the states must yield all their power to the national government (Robertson, D.B., 2012).

The state's rights advocates, feared a strong national government would subjugate the interests of the individual states; they favored a stronger national government, "but wanted specific, narrow new powers rather than the broad authority Madison wanted. "The larger states were at odds with the smaller states because they feared that their power would be diminished under a national government. The compromise proposed a new form of federalism that had at its foundation a 'shared sovereignty' (Robertson, 2012, p. 9).

This shared sovereignty provided for a dual court system - a federal system and court system in each state. The U.S. District Courts, are the federal trial courts and are 94 in number. There are U.S. District Courts in all fifty states, the District of Columbia, Puerto Rico, Guam, the Virgin Islands and the Northern

Mariana Islands. The U.S. Circuit Court of Appeals are appellate courts and hear appeals from courts within their region; there are eleven regional circuit courts whose territory includes any number of states. For example, the First Circuit oversees cases from Massachusetts, Maine, New Hampshire, Rhode Island and Puerto Rico. The highest court in the United States is the U.S. Supreme Court.

Each state has its own unique court system and is free to create multiple courts per its own state constitution. There is no uniformity among the states' court systems. Each state constitution can provide its citizens enhanced rights, for example, in Massachusetts, the highest appellate court, the Supreme Judicial Court, concluded that for purposes of probable cause under Article 14 of its state constitution, the Declaration of Rights, criminal defendants would receive more substantive rights than those provided under the Fourth Amendment (Grasso & McEvoy, 2018).

Relative to criminal cases, the states handle far more criminal cases per year than the federal system. In the twelve-month period ending March 30, 2020, the federal district courts processed 88,582 criminal defendants. In contrast, in 2018, the state courts, which included courts of general, limited and single jurisdiction, handled a total of 83.8 million cases. Massachusetts has both courts of limited and general jurisdiction. According to the Court Statistics Project, the 2018 State Court Caseload Digest, which comprises the latest data, and is a joint project of the Conference of State Court Administrators and the National Center for State Courts, the total for criminal cases in the United States was 17,171,953. This includes 2.2 million single jurisdiction cases, 3.5 million general jurisdiction cases, and 11.5 million limited jurisdiction cases (State Court Digest, 2018).

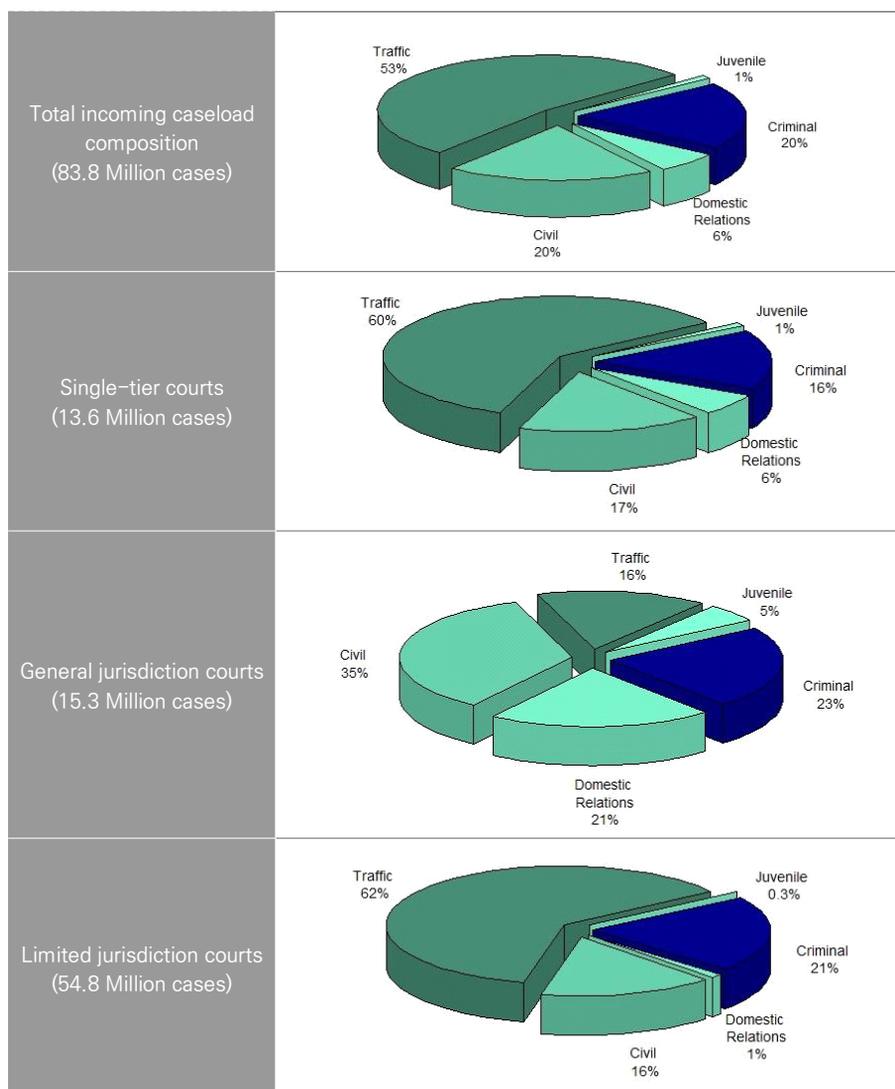
»» [Table 3-3-1] Massachusetts Statewide Criminal Caseloads by Year

2016	2017	2018
198,796	187,765	181,277

Source: Massachusetts State Court Internal Data (2020)

Thus, the bulk of the criminal cases are overwhelmingly the province of the state courts, not the federal system. This demonstrates the diversity of federal and state jurisdiction and the complexity of examining laws for each given state. Please note that the data does not include any reference to cybercrimes.

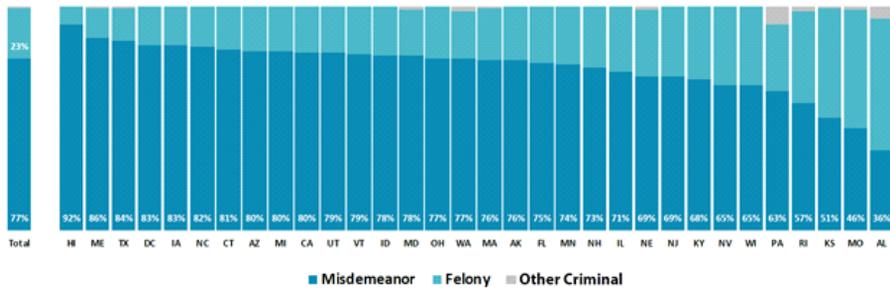
»» [Figure 3-3-1] Total Caseload for State Courts in United States



Source: Court Statistics Project (2020). State Court Caseload Digest: 2018 Data. National Center for State Courts.

States broadly classify their Criminal caseloads into three subcategories of cases: felonies, misdemeanors, and a residual “other” category that includes appeals from limited jurisdiction courts. This chart shows the composition of Criminal caseloads in the 32 states able to report this level of detail. In the aggregate, misdemeanor cases comprise about 77 percent of incoming Criminal cases in state trial courts and comprise more than half of all Criminal cases in 30 of the 32 states shown (Court Statistics Project, 2020).

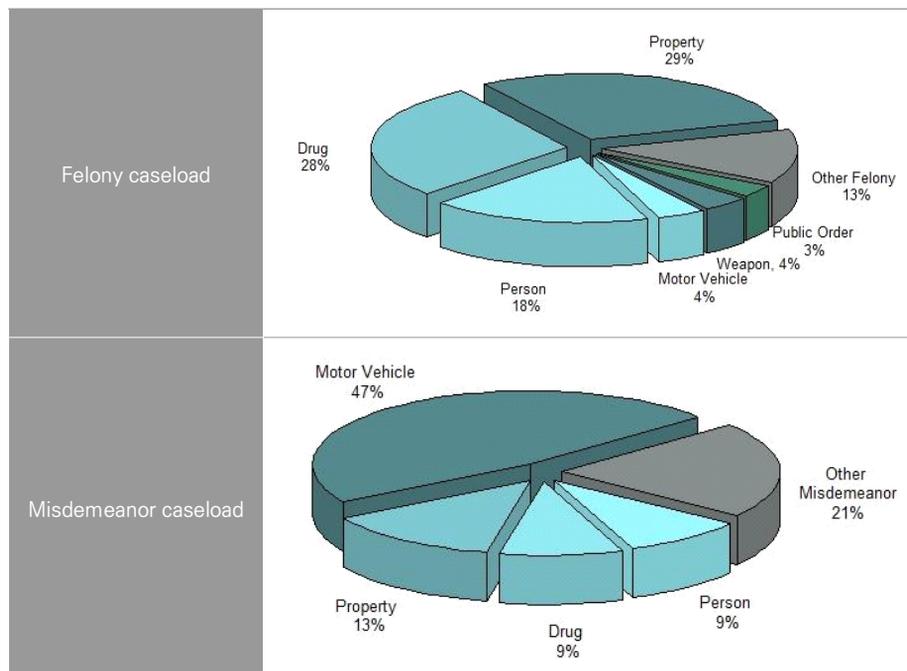
»» [Figure 3-3-2] Criminal Caseload Composition in 32 States



Source: Court Statistics Project (2020). State Court Caseload Digest: 2018 Data. National Center for State Courts.

The State Court Guide to Statistical Reporting defines 10 different types of felony cases and 11 different types of misdemeanor cases. Felony caseloads are comprised largely of property, drug, and person cases (a combined 75 percent) with smaller portions of the caseload made up of motor vehicle (including DWI/DUI), weapon, public order, and other cases (including domestic violence and elder abuse). Misdemeanor caseloads, in contrast to felony, are composed largely of motor vehicle cases (47%) while property, drug, and person cases make up a noticeable but smaller proportion (a combined 31%) of the caseload. Other misdemeanor cases, including domestic violence, elder abuse, weapon, public order, and protection order violations comprise the remaining 21 percent of the caseload.

» [Figure 3-3-3] Felony and Misdemeanor Criminal Caseload Composition in 21 States (including Massachusetts)



Source: Court Statistics Project (2020). State Court Caseload Digest: 2018 Data. National Center for State Courts.

## 2. Cybercrime in the U.S.

Generally, cybercrime has been described as "the destruction, theft, or unauthorized or illegal use, modification, or copying of information, programs, services, equipment, or communication networks" (Marcum, 2019, p. 3). The ubiquity of the internet has allowed the world's population to engage instantaneously. Some utilize the internet's resources for work and entertainment, yet others have put it to nefarious uses including criminality. Anyone who accesses the internet is literally communicating globally; it is a global issue. Even a consistent global definition eludes policymakers, researchers and law enforcement.

The 2001 Council of Europe's Convention on Cybercrime defines it as thus: "action directed against the confidentiality, integrity and availability of computer

systems, networks, and computer data as well as the misuse of such systems, networks and data. "Four categories of criminal offenses are delineated: (1.) offenses against the confidentiality, integrity, and availability of computer data and systems, (2.) computer-related offenses, (3.) content-related offenses, and (4.) offenses related to infringements of copyright and related rights (Peters, A. & Jordan, A., 2020, p. 488, fn. 4).

As state prosecutors are engaged with more street-level crimes that need immediate resolution owing to a defendant's speedy trial guarantee embodied in the Sixth Amendment to the U.S. Constitution and state constitutional guarantees, how much time is devoted to the issue of cybercrime?

Research indicates that cyberattacks are the fastest growing crime in the United States; the individual, corporations and governments are all at risk. The cost is enormous - a few examples will suffice - there has been an uptick in online crimes against children, a 40.9% increase in phishing attacks, and the 2018 ransomware attack on the city of Atlanta sabotaged city services and cost millions to resolve (Decker, 2020).

The breadth of the problem is staggering and the inability to track all of the cybercrime leaves law enforcement at a distinct disadvantage. How can you meaningfully address this multi-faceted problem if you are unaware of the magnitude of the problem? Herewith are a few categories of cybercrime criminality: child pornography, sexual solicitation, digital piracy, scams and cons, cyberbullying and cyberstalking, hacking, malware and cyberterrorism.

### A. Federal Cybercrime Statutes

The federal government has moved aggressively into the criminal arena with the passage of most of the federal criminal statutes occurring since 1970. There are approximately 4,500 federal crimes. Approximately 400 of these federal crimes were passed between 2008 and 2013 (Gardner, 2018, p. 41-42). Some

examples of federal statutes to combat internet crime include: the Computer Fraud and Abuse Act, the Federal Wire Fraud statute, the Copyright Act, the Child Pornography Prevention Act of 1996, and the Electronics Communications Privacy Act.

### 1) Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA) was passed in 1984; it is the federal anti-hacking statute. The federal act, which provides for fines and a prison sentence, outlaws, among other things, transmitting programs or codes that damage computer networks, and outlaws acquiring access to a computer for fraudulent purposes (Find Law, 2020). The act has come under criticism for being too vague, overbroad and too broad in the conduct it seeks to criminalize. States have the choice to adopt the CFAA or creating their own legal paradigm. The advantage to its adoption for a state is that there is a large body of case law and legal precedent that can aid their interpretation. Thus, the vast majority of states have "aligned their cybercrime codes with federal statutes, including the CFAA" (Brunner, 2020, p. 565).

In a significant development, the United States Supreme Court has agreed to hear a case involving an interpretation of CFAA in its October 2020 session. There has been disagreement amongst the circuits as to the breadth of the CFAA. The United States Supreme Court receives approximately 10,000 appeals each year and hears approximately 75 cases; this points to the need for clarification that they chose to opine on this case involving interpretation of CFAA. The case, *Van Buren v. United States*, 940 F. 3d 1192, arises from the conviction of a Georgia police sergeant Nathan Van Buren. He received \$6,000 from an acquaintance so that he would access the Georgia Crime Information center's database in order to discover whether a woman was an undercover officer. The defendant Van Buren was convicted of violating the CFAA, specifically 18 U.S.C. 1030 alleging computer fraud.

The issue before the court is whether a person who is authorized to access information on a computer for certain purposes violates Section 1030 (a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose. The defendant Van Buren has argued that accessing information for an improper or impermissible purpose does not exceed authorized access under Section 1030 (a)(2) or more concisely: whether “misusing databases that a defendant can lawfully access constitutes computer fraud.” There is a substantial split in the circuit courts. The Eleventh Circuit, together with the First (Massachusetts is in the First Circuit), Fifth, Seventh Circuits consider activity such as the defendant Van Buren’s as conduct exceeding one’s authorized access to a protected computer and would be a violation of the CFAA.

The Ninth Circuit takes a more limited view of section 1030 (a)(2) and the defendant in all likelihood would be entitled to an acquittal under that circuit’s interpretation. Van Buren’s petition for certiorari argued that ‘reading the statute more broadly would criminalize ordinary computer use throughout the country.’ Given the varied interpretations within the circuits, Van Buren’s argument has apparently hit a nerve with the United States Supreme Court justices ‘concerned with the criminal justice implications of the CFAA’s language.’ This resolution of the case by the Supreme Court is a chance to resolve the interpretative difficulties inherent in the CFAA statute.

Brunner reveals in *Challenges and Opportunities in State and Local Cybercrime Enforcement*, that “while researchers have conducted comprehensive studies analyzing prosecutions under CFAA, there is little research examining how crime prosecutions have played out at the state level. This may be perhaps due to a lack of data, the “enforcement gap” for cybercrime, and the hesitancy amongst state and local law enforcement to wade into this arena of law in the face of a multitude of competing cases for other criminal offenses” (Brunner, 2020, p. 566). Again, the technical complexity of these crimes may be outside the time

requirements of most prosecutors who must respond to the immediacy of street crime and its victims.

As the momentum of cybercrimes continues unabated, it has become imperative that state and local law enforcement agencies and prosecutors develop a working knowledge of the basic technical components of cybercrime. The U.S. Secret Service's National Computer Forensics Institute (NCFI) has taken up the task of providing training and education on cyber issues like digital evidence to prosecutors and judges free of charge, however the training opportunities are limited (Brunner, p. 576).

With the evidentiary importance and the breadth of digital evidence, amendments to the Federal Rules of Evidence were necessary and were passed in December 2018 (Federal Rules of Evidence 902 (13), (14)). Though some states have passed procedural authentication rules, many states are slow to author evidentiary rules governing the admission of digital evidence.

There is an upside to the gaps in the states' learning curve -increased partnerships with federal agencies have emerged in an effort to accelerate the acquisition of relevant and topical information necessary for the investigation and prosecution of these cases. The most common state/federal partnerships include the FBI Cyber Task Forces, the USSS Electronic Crimes Task Forces, the Internet Crimes Against Children (ICAC), and a conglomeration of federal agencies investigating criminality on the dark web (Brunner, p. 577).

Given cybercrimes interstate fluidity and global reach, there are myriad issues of a multi-jurisdictional nature. This is a challenge for state and local enforcement. A variety of resources allow for the international procurement of evidence and suspects. Transnational crimes call for cooperation between countries. A letter rogatory is one tool used by prosecutors. It is a request from a court in one country to a court in another country to perform a judicial act. The Department of Justice's Office of International Affairs in the United States provides information

on what information is required for each international court to pursue the process (Marcum, p. 7).

The second way to effect transnational cooperation is through the Mutual Legal Assistance Treaty (MLAT). Per Marcum, in *Cybercrime*, “The treaty does not simply request a response; it imposes a legal obligation on the responding country to act. In 2009, the United States had MLAT’s with fifty-three other countries” (Marcum, p. 7).

Federal courts have declined to extend the CFAA to cover cyberbullying and cyber-harassment so states have enacted legislation to address those issues. Though cyberbullying has been proposed at the federal level, at present, there is no federal legislation relative to this crime (Engle, 2020, p. 485).

## 2) The Federal Wire Fraud Statute

The Federal Wire Fraud Statute focuses on crimes committed over the telephone lines so is “better suited to some Internet crimes than other laws. The wire fraud act applies to schemes to secure property or money through fraud perpetrated over interstate wire communications. Some courts have held that this law, may be used to punish violations of copyright laws, such as unauthorized copying of computer programs. The law provides for fines and prison sentences. Where the subject of the fraud is a financial institution, the fines can reach seven figures” (Find Law, 2020).

## 3) The Copyright Act

The Copyright Act specifically addresses Internet thefts of copyrighted works which include computer programs and a range of other work products. One of the most expensive crimes perpetrated over the Internet is software piracy. This act provides for fines and other penalties. U.S. District courts have taken divergent positions as to whether the wire fraud statute reaches copyright infringement.

Partly as a response to these decisions, Congress amended the Copyright Act to criminalize the willful infringement of a copyright, by electronic means, "if the infringement was committed by the reproduction or distribution...during any 180-day period of 1 or more copies...of 1 or more copyrighted works, which have a total retail value of more than \$1,000...."(Find Law, 2020).

#### 4) The Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) allows for prosecution of the interception of wire and electronic communications. "It ...punishes unauthorized access to or alteration of electronically stored information, as well as efforts to prevent authorized access to such information... It has seen further use as a way to punish unauthorized reception of encrypted satellite television broadcasts." Like the CFAA, this act is used to prosecute computer hackers. The ECPA updates the Wiretap Act to extend to electronic communications, in addition to oral and wire communications (Find Law, 2020).

#### 5) The Child Pornography Prevention Act

According to Krause, the federal government in the 1980's and 1990's made the prosecution of obscenity cases a priority and they were largely successful. With the proliferation of hardcore websites on the Internet, both commercial and amateur, the number of prosecutions for obscenity declined dramatically as priorities changed. Today, the federal government directs its resources to the prosecution of child pornography and human trafficking. According to data supplied in *ACLU v. Gonzales*, there have been less than ten prosecutions for adult obscenity since 2005 (Krause, 2008).

## B. Massachusetts State Statutes and Cybercrime

The Massachusetts legislature convened a 'Special Senate Committee on Cyber

Security Readiness.’ The committee was chaired by Senator Michael Moore and Senator Ryan Fattman from Worcester county and Senator Eric Lesser from Hampden county. The report was issued on August 15, 2018. A large portion of the committee’s task was to address private sector concerns; this paper focuses on the criminal public sector concerns addressed by the committee members and the experts they interviewed. The committee admitted that Massachusetts was in a vulnerable position when it came to protection of its cyber systems and identified recent breaches in the towns of Holyoke, Leominster, and Brookline. The committee referenced a 2007 general strategic plan and, further, in 2014, specific anti-cyberterrorism measures that were promulgated by the state Homeland Security Division, but as the legislative committee noted, “...with no way to ensure that these measures are occurring, and no way to enforce their implementation, these measures are not being used in the Commonwealth” (Massachusetts Senate Legislative Cyber Readiness Committee, 2018, p. 8).

The committee members heard from Chief Information Security Officer and Chief Technology Officer (EOTSS), Dennis McDermitt. He explained that the ‘bad guy’ targets include: data, for use in identity theft and cybercrime or multidimensional use of data for nefarious means (Senate Legislative Committee Report, p. 27).

Brandon C. Brin, IT Director, for Legislative Information Services and an invited speaker to the National Conference of State Legislatures (NCSL) 2017 Legislative Summit offered a number of proposals regarding the public sector and advancement of knowledge in this area. He suggested transparency surrounding data breaches and recommended notifying the public about breaches, thus ensuring the public trust. These breaches must also be reported to law enforcement and regulatory agencies. He expressed his belief that cybersecurity education should begin in elementary and secondary school and should be an integral part of a STEM curriculum. He advocated for training and guidelines for state and municipal employees who handle financial transactions and sensitive personal information.

Other suggestions include defining the scope of 'cybercrime' so that reporting incidents are accomplished at a federal level. This reporting accuracy ensures that adequate and appropriate funding and resources are directed to state and local jurisdictions; this would include an updating for clarity of M.G.L. c. 266, section 120, Unauthorized Access of a Computer System (Senate Legislative Committee Report, p. 27).

The committee and its experts recognized that law enforcement 'may need unique training and additional resources to combat cybercrime.' It was acknowledged that "When it comes to the court system, the decentralized nature of internet-based crimes makes prosecution difficult, a hurdle that must be addressed via legislation that is responsive to these modern times." A further recommendation was that the government should partner with academics focused on cybersecurity research in Massachusetts.

Lastly, the legislative committee recommended the creation of a 'Cybersecurity Control and Review Board (CCRB). This would be a five-person oversight committee made up of private sector and cybersecurity representatives. It was recommended that the board would be tasked with improving cybersecurity across businesses in Massachusetts. Two house bills were proposed: 1. *An Act Addressing Cybercrime Through Enhanced Criminal Penalties, Civil Remedies, and Transparency* (HB2814): Amends various laws regulating electronic security breaches, cybersecurity, and cybercrime, and establishes a special commission on cybersecurity charged with assessing cybersecurity threats and recommending legislation, risk management strategies, and response plans to prevent and mediate attacks, and 2. *An Act Ensuring Cyber Security in the Commonwealth* (HB3655): Establishes a nine-member task force to study the need for increased cybersecurity within government agencies. According to Senator Michael Moore, neither bill passed (M. Moore, personal conversation, June 29, 2020).

### 1) Massachusetts State Cybercrime Statutes: overview

All states have enacted computer crime statutes. Most state statutes address the following issues: 1.) online harassment; 2.) spam; 3.) spyware; 4.) the protection of personal information; and 5.) cyberbullying. Some Massachusetts statutes include: Obtaining computer services by fraud, unauthorized access to computer, cyberbullying, criminal harassment, cyber stalking, identity fraud, possession of child pornography, dissemination/distribution of child pornography, creating child pornography, illegal downloads, copyright, file sharing and piracy.

### 2) Obtaining Computer Services by Fraud (M.G.L. c. 266, s. 33A)

Whoever, with intent to defraud, obtains, or attempts to obtain, or aids or abets another in obtaining, any commercial computer service by false representation, false statement, unauthorized charging to the account of another, by installing or tampering with any facilities or equipment or by any other means, shall be punished... As used in this section, the words “commercial computer service” shall mean the use of computers, computer systems, computer programs or computer networks, or the access to or copying of the data, where such use, access or copying is offered by the proprietor or operator of the computer, system, program, network or data to others on a subscription or other basis for monetary consideration.

### 3) Unauthorized Access to Computer (M.G.L. c. 266, s. 120F)

“Whoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access, shall be punished...”

“The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.”

4) Cyberbullying (M.G.L. c. 71, s. 370)

“Bullying”, the repeated use by one or more students or by a member of a school staff including, but not limited to, an educator, administrator, school nurse, cafeteria worker, custodian, bus driver, athletic coach, advisor to an extracurricular activity or paraprofessional of a written, verbal or electronic expression or a physical act or gesture or any combination thereof, directed at a victim that: (i) causes physical or emotional harm to the victim or damage to the victim's property; (ii) places the victim in reasonable fear of harm to himself or of damage to his property; (iii) creates a hostile environment at school for the victim; (iv) infringes on the rights of the victim at school; or (v) materially and substantially disrupts the education process or the orderly operation of a school. For the purposes of this section, bullying shall include cyber-bullying.

5) Criminal Harassment (M.G.L. c. 265, s. 43A(a))

Whoever willfully and maliciously engages in a knowing pattern of conduct or series of acts over a period of time directed at a specific person, which seriously alarms that person and would cause a reasonable person to suffer substantial emotional distress, shall be guilty of the crime of criminal harassment. The conduct or acts described in this paragraph shall include, but not be limited to, conduct or acts conducted by mail or by use of a telephonic or telecommunication device or electronic communication device including, but not limited to, any device that transfers signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system, including, but not limited to, electronic mail, internet communications, instant messages or facsimile communications.

6) Stalking (M.G.L. c. 265, s. 43)

(a) Whoever (1) willfully and maliciously engages in a knowing pattern of

conduct or series of acts over a period of time directed at a specific person which seriously alarms or annoys that person and would cause a reasonable person to suffer substantial emotional distress, and (2) makes a threat with the intent to place the person in imminent fear of death or bodily injury, shall be guilty of the crime of stalking... The conduct, acts or threats described in this subsection shall include, but not be limited to, conduct, acts or threats conducted by mail or by use of a telephonic or telecommunication device or electronic communication device including, but not limited to, any device that transfers signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system, including, but not limited to, electronic mail, internet communications, instant messages or facsimile communications.

#### 7) Identity Fraud (M.G.L. c. 266, s. 37E)

- (a) For purposes of this section, the following words shall have the following meanings:
- i) "Harass", willfully and maliciously engage in an act directed at a specific person or persons, which act seriously alarms or annoys such person or persons and would cause a reasonable person to suffer substantial emotional distress.
  - ii) "Personal identifying information", any name or number that may be used, alone or in conjunction with any other information, to assume the identity of an individual, including any name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, credit card number or computer password identification.

- iii) "Pose", to falsely represent oneself, directly or indirectly, as another person or persons.
  - iv) "Victim", any person who has suffered financial loss or any entity that provided money, credit, goods, services or anything of value and has suffered financial loss as a direct result of the commission or attempted commission of a violation of this section.
- (b) Whoever, with intent to defraud, poses as another person without the express authorization of that person and uses such person's personal identifying information to obtain or to attempt to obtain money, credit, goods, services, anything of value, any identification card or other evidence of such person's identity, or to harass another shall be guilty of identity fraud.
- (c) Whoever, with intent to defraud, obtains personal identifying information about another person without the express authorization of such person, with the intent to pose as such person or who obtains personal identifying information about a person without the express authorization of such person in order to assist another to pose as such person in order to obtain money, credit, goods, services, anything of value, any identification card or other evidence of such person's identity, or to harass another shall be guilty of the crime of identity fraud.

(c1/2) Whoever possesses a tool, instrument or other article adapted, designed or commonly used for accessing a person's financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, personal identification number, mother's maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person under circumstances evincing an intent to use

or knowledge that some person intends to use the same in the commission of larceny shall be guilty of identity fraud.

**8) Possession of Child Pornography (M.G.L. c. 272, s. 29C)**

Whoever knowingly purchases or possesses a negative, slide, book, magazine, film, videotape, photograph or other similar visual reproduction, or depiction by computer, of any child whom the person knows or reasonably should know to be under the age of 18 years of age and such child is:

- i) actually or by simulation engaged in any act of sexual intercourse with any person or animal;
- ii) actually or by simulation engaged in any act of sexual contact involving the sex organs of the child and the mouth, anus or sex organs of the child and the sex organs of another person or animal;
- iii) actually or by simulation engaged in any act of masturbation;
- iv) actually or by simulation portrayed as being the object of, or otherwise engaged in, any act of lewd fondling, touching, or caressing involving another person or animal;
- v) actually or by simulation engaged in any act of excretion or urination within a sexual context;
- vi) actually or by simulation portrayed or depicted as bound, fettered, or subject to sadistic, masochistic, or sadomasochistic abuse in any sexual context; or
- vii) depicted or portrayed in any pose, posture or setting involving a lewd exhibition of the unclothed genitals, pubic area, buttocks or, if such person is female, a fully or partially developed breast of the child; with knowledge of the nature or content thereof shall be punished.

9) Dissemination/Distribution of Child Pornography (M.G.L. c. 272, 29B)

- (a) Whoever, with lascivious intent, disseminates any visual material that contains a representation or reproduction of any posture or exhibition in a state of nudity involving the use of a child who is under eighteen years of age, knowing the contents of such visual material or having sufficient facts in his possession to have knowledge of the contents thereof, or has in his possession any such visual material knowing the contents or having sufficient facts in his possession to have knowledge of the contents thereof, with the intent to disseminate the same, shall be punished...
- (b) Whoever with lascivious intent disseminates any visual material that contains a representation or reproduction of any act that depicts, describes, or represents sexual conduct participated or engaged in by a child who is under eighteen years of age, knowing the contents of such visual material or having sufficient facts in his possession to have knowledge of the contents thereof, or whoever has in his possession any such visual material knowing the contents or having sufficient facts in his possession to have knowledge of the contents thereof, with the intent to disseminate the same, shall be punished...
- (c) For the purposes of this section, the determination whether the child in any visual material prohibited hereunder is under eighteen years of age may be made by the personal testimony of such child, by the testimony of a person who produced, processed, published, printed or manufactured such visual material that the child therein was known to him to be under eighteen years of age, by testimony of a person who observed the visual material, or by expert medical testimony as to the age of the child based upon the child's physical appearance, by inspection of the visual material, or by any other method authorized by any general or special law or by any applicable rule of evidence.

- (d) In a prosecution under this section, a minor shall be deemed incapable of consenting to any conduct of the defendant for which said defendant is being prosecuted.
- (e) Pursuant to this section, proof that dissemination of any visual material that contains a representation or reproduction of sexual conduct or of any posture or exhibition in a state of nudity involving the use of a child who is under eighteen years of age was for a bona fide scientific, medical, or educational purpose for a bona fide school, museum, or library may be considered as evidence of a lack of lascivious intent.

10) Creating Child Pornography (M.G.L. c. 272, s. 29A)

- (a) Whoever, either with knowledge that a person is a child under eighteen years of age or while in possession of such facts that he should have reason to know that such person is a child under eighteen years of age, and with lascivious intent, hires, coerces, solicits or entices, employs, procures, uses, causes, encourages, or knowingly permits such child to pose or be exhibited in a state of nudity, for the purpose of representation or reproduction in any visual material, shall be punished...
- (b) Whoever, either with knowledge that a person is a child under eighteen years of age or while in possession of such facts that he should have reason to know that such person is a child under eighteen years of age, hires, coerces, solicits or entices, employs, procures, uses, causes, encourages, or knowingly permits such child to participate or engage in any act that depicts, describes, or represents sexual conduct for the purpose of representation or reproduction in any visual material, or to engage in any live performance involving sexual conduct, shall be punished...
- (c) In a prosecution under this section, a minor shall be deemed incapable of consenting to any conduct of the defendant for which said defendant

is being prosecuted.

11) Illegal Downloads, Copyright, File Sharing and Piracy (M.G.L. c. 266, s. 143A)

Whoever directly or indirectly by any means, knowingly transfers or causes to be transferred any sound recorded on a phonograph record, disc, wire, tape, film, videocassette or other article on which such sound is recorded, with intent to sell, rent or transport, or cause to be sold, rented or transported, or to use or cause to be used for profit through public performance such article on which such sound is so transferred, without the consent of the owner, or whoever sells any such article with the knowledge that the sound thereon has been so transferred without the consent of the owner, shall be punished as provided in section 143E.

Although a number of states have passed Sexting laws, Massachusetts has not. Sexting is defined as sending sexually explicit videos or photographs via text message to another's cell phone. If the videos or photographs are of a child under the age of eighteen years old, the state of Massachusetts may prosecute under the child pornography laws.

### 3. Cybercrime Statistics

#### A. FBI's Internet Crime Report

Since 2000, the FBI's IC3 has been a center to receive complaints of Internet-facilitated criminal activity (FBI, 2019). According to the "2019 Internet Crime Report," more than 467 thousand cybercrime cases were reported in 2019, an increase of nearly 33% compared to the previous year (FBI, 2019). Over the last five years, on average, the number of complaints received per year reached over 340,000. The complaints to the IC3 consistently showed an upward trend. In 2019, the financial losses due to the Internet-facilitated fraud scheme reached 3.5 billion USD, an increase of nearly 30% compared to the previous year (FBI, 2019)

»» [Table 3–3–2] Reported Internet-facilitated Fraud and Financial Losses (2015–2019)

	2014	2015	2016	2017	2018	2019
# of complaints	269,422	288,012	298,728	301,580	351,937	467,361
% Increase		6.9%	3.7%	1.0%	16.7%	35.8%
Financial loss(billion USD)	0.8	1.1	1.5	1.4	2.7	3.5
% Increase		37.5%	36.4%	-6.7%	92.9%	29.6%

Source: FBI, Internet Crime Report 2018 & 2019

The Recovery Asset Team (RAT) within IC3 was established in February 2018 for the recovery of fraudulently transferred victim's funds between U.S. domestic accounts (FBI, 2018). If a suspicious Internet-facilitated fraud scheme was detected, the RAT notifies such fraudulent activity to the recipient bank, along with requesting freezing of account (FBI, 2018). The recovery rate of losses to recovery were 75% in 2018 and 79% in 2019, respectively.

»» [Table 3–3–3] Recovery Rate of Financial Losses by the RAT (2018–2019)

	2018	2019
Incidents	1,061	1,307
Losses (USD)	257,096,991	384,237,651
Recovery (USD)	192,699,195	304,930,696
Recovery rate (%)	75	79

Source: FBI, Internet Crime Report 2018 & 2019

Based on the total number of complaints and the total amount of financial loss, the most vulnerable were above 60 years of age, while under 25 years old's victimization rate skyrocketed between 2018 and 2019.

»» [Table 3–3–4] Victim by Age Group (2018–2019)

		Under 25	20–29	30–39	40–49	50–59	Over 60
Total incidents	2019	10,724	44,496	52,820	51,864	50,608	68,013
	2018	9,129	40,924	46,342	50,545	48,642	62,085
		17.5%	8.7%	14.0%	2.6%	4.0%	9.5%

		Under 25	20-29	30-39	40-49	50-59	Over 60
Total loss (USD)	2019	421,169,232	174,673,470	332,208,189	529,231,267	589,624,844	835,164,766
	2018	12,553,082	134,485,965	305,699,977	405,612,455	494,926,300	649,227,724
		3255%	29.9%	8.7%	60.5%	19.1%	28.6%

Source: FBI, Internet Crime Report 2018 & 2019

IC3 report showed that ‘Phishing/Vishing/Smishing/Pharming’ was, by far, the most reported offense, comprising 23% of total cybercrime victimization in 2019. It is a 334% increase compared to the previous year. In addition, Non-payment/non-delivery, extortion, personal data breach, and spoofing round out the top five categories of complaints referred to IC3 during 2019.

»» [Table 3-3-5] Cybercrime Types by Victim Count (2018-2019)

	2018	2019	
Total	454,895	501,119	10.2%
Phishing/Vishing/Smishing/Pharming	26,379	114,702	334.8%
Non-Payment/Non-Delivery	65,116	61,832	-5.0%
Extortion	51,146	43,101	-15.7%
Personal Data Breach	50,642	38,218	-24.5%
Spoofing	15,569	25,789	65.6%
BEC/EAC	20,373	23,775	16.7%
Confidence Fraud/Romance	18,493	19,473	5.3%
Identity Theft	16,128	16,053	-0.5%
Harassment/Threats of Violence	18,415	15,502	-15.8%
Overpayment	15,512	15,395	-0.8%
Advanced Fee	16,362	14,607	-10.7%
Employment	14,979	14,493	-3.2%
Credit Card Fraud	15,210	14,378	-5.5%
Government Impersonation	10,978	13,873	26.4%
Tech Support	14,408	13,633	-5.4%
Real Estate/Rental	11,300	11,677	3.3%
Lottery/Sweepstakes/Inheritance	7,146	7,767	8.7%
Misrepresentation	5,959	5,975	0.3%
Investment	3,693	3,999	8.3%
IPR/Copyright and Counterfeit	2,249	3,892	73.1%

	2018	2019	
Malware/Scareware/Virus	-	2,373	
Ransomware	1,493	2,047	37.1%
Corporate Data Breach	-	1,795	
Denial of Service/TDoS	1,799	1,353	-24.8%
Crimes Against Children	1,394	1,312	-5.9%
Re-shipping	907	929	2.4%
Civil Matter	768	908	18.2%
Health Care Related	337	657	95.0%
Charity	-	407	
Gambling	181	262	44.8%
Terrorism	120	61	-49.2%
Hacktivist	77	39	-49.4%
No Lead Value	36,936	-	
Other	10,826	10,842	0.1%

Source: FBI, Internet Crime Report 2018 & 2019.

However, the cybercrime statistics of IC3 has critical limitations. As shown in IC3 Report, 1) one complaint may have multiple crime types, 2) some complainants may have filed more than once, creating a possible duplicate complaint, 3) victim outside of U.S. territory can file a complaint. Therefore, losses reported in foreign currencies are converted to U.S. dollars when possible (FBI, 2019, p.28). When limited to victims within the American territory, there were a total 349,226 of victims in 2019, 8.9% increase compared to the previous year.

»» [Table 3-3-6] Number of Complaints within the American Territory (2018-2019)

		2018	2019	
	Total	320,623	349,226	8.9%
1	California	49,031	50,132	2.2%
2	Florida	23,984	27,178	13.3%
3	Texas	25,589	27,178	6.2%
4	New York	18,124	21,371	17.9%
5	Washington	10,775	13,095	21.5%
6	Maryland	8,777	11,709	33.4%

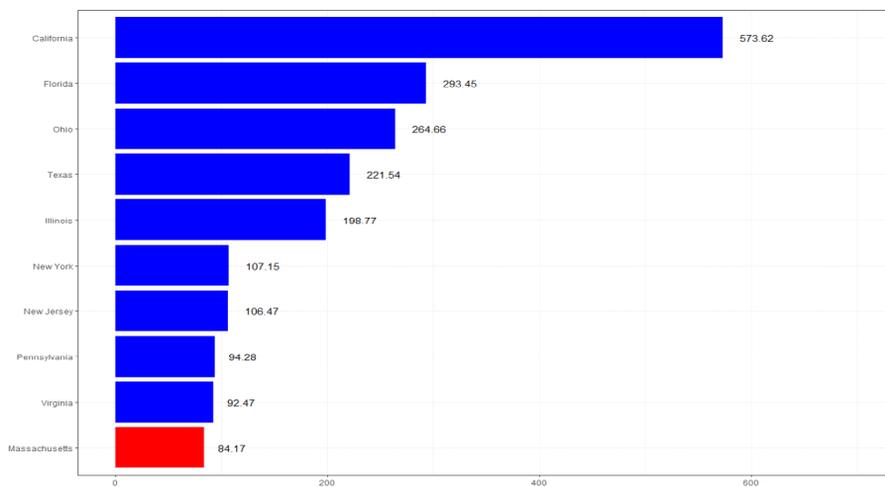
82 Comparative Study on the metric of cybercrime between the U.S. and South Korea

		2018	2019	
7	Virginia	14,800	11,674	-21.1%
8	Pennsylvania	10,554	10,914	3.4%
9	Illinois	10,087	10,337	2.5%
10	Indiana	4,676	9,746	108.4%
11	Colorado	9,328	9,689	3.9%
12	Ohio	7,812	9,321	19.3%
13	Georgia	9,095	9,074	-0.2%
14	New Jersey	8,440	9,067	7.4%
15	Michigan	7,533	8,249	9.5%
16	North Carolina	7,523	8,223	9.3%
17	Arizona	8,027	7,795	-2.9%
18	Massachusetts	6,173	6,492	5.2%
19	Nevada	5,228	6,381	22.1%
20	Wisconsin	6,621	6,378	-3.7%
21	Tennessee	5,584	5,586	0.0%
22	Iowa	1,983	5,094	156.9%
23	Missouri	5,508	5,083	-7.7%
24	Oregon	4,511	4,813	6.7%
25	South Carolina	3,575	4,541	27.0%
26	Connecticut	3,134	4,412	40.8%
27	Minnesota	4,304	4,388	2.0%
28	Alabama	4,585	4,108	-10.4%
29	Louisiana	3,469	3,804	9.7%
30	Utah	3,041	3,304	8.6%
31	Kentucky	2,813	3,083	9.6%
32	Oklahoma	2,644	2,887	9.2%
33	New Mexico	2,127	2,037	-4.2%
34	Arkansas	1,849	1,991	7.7%
35	Kansas	2,098	1,970	-6.1%
36	Mississippi	1,882	1,654	-12.1%
37	Idaho	1,513	1,485	-1.9%
38	Alaska	1,603	1,451	-9.5%
39	District of Columbia	1,364	1,407	3.2%
40	Hawaii	1,100	1,396	26.9%
41	Nebraska	1,205	1,350	12.0%

		2018	2019	
42	West Virginia	1,109	1,227	10.6%
43	New Hampshire	1,056	1,155	9.4%
44	Delaware	897	1,062	18.4%
45	Rhode Island	1,028	1,011	-1.7%
46	Montana	787	967	22.9%
47	Maine	832	880	5.8%
48	Puerto Rico	704	839	19.2%
49	Wyoming	497	550	10.7%
50	Vermont	525	500	-4.8%
51	North Dakota	459	489	6.5%
52	South Dakota	465	473	1.7%
53	U.S. Virgin Islands	65	75	15.4%
54	Guam	52	71	36.5%
55	U.S. Minor Outlying Islands	47	46	-2.1%
56	American Samoa	16	23	43.8%
57	Northern Marina Islands	15	11	-26.7%

Source: FBI, Internet Crime Report 2018 & 2019.

»» [Figure 3-3-4] Monetary Loss to Victims from Cybercrime in United States by Top States 2019 (in millions)



Source: Statista (2020)

## B. National Incident-Based Reporting System (NIBRS) data in Massachusetts

The following statistics are from the Federal Bureau of Investigations CJIS division. In 2016, Identity Theft and Hacking/Computer Invasion were added as fraud offenses to the National Incident-Based Reporting System (NIBRS) data collection (Decker, 2020, p. 591). The data represents reported offenses by individual cities and towns in Massachusetts. This author included other offenses aside from Hacking/Computer Invasion surmising that the included categories *may* have some aspect of cyber criminality though the statistics do not reflect this. It is hopeful that as more focus is generated on cybercrimes that the more detailed NIBRS data will expound on the crime categories as it relates to cybercrime.

The National Incident Based Reporting System (NIBRS), from which the aforementioned statistics about Massachusetts crime were gleaned, is the broader collection system. The data in the Uniform Crime Reporting (UCR) program and the Summary Reporting System (SRS) are being transitioned to the NIBRS. These programs are essential tools for policy makers, politicians, law enforcement, advocates and the public in evaluating crime (Decker, p. 585).

The NIBRS, the latest United States crime reporting data collection is designed to not only tally the numbers in specific offenses, but it provides details about bodily injuries, whether a weapon was used, and the location of each crime. The NIBRS compiles data on fifty-two offenses; a more expansive list than the prior data collection tools. In 2017, it was reported by the FBI that 42% of law enforcement were reporting data to NIBRS. The full conversion to the NIBRS is expected in 2021 (Decker, p. 590).

It is anticipated that the NIBRS system will modernize data collection methods. Where does cybercrime factor into NIBRS? Unfortunately, not very well. Of the fifty-two most serious offenses, designated as Group A Offenses, only one category, listed under fraud offenses, called 'hacking/computer invasion,' is designated for

cybercrime. Though the system has made some changes in the cybercrime area, “...it remains deficient in that it fails to focus on cybercrime, fails to account for the full range of computer-generated crimes, and continues to focus on traditional street and property crimes...” (Decker, p. 591).

### 1) Federal NIBRS data (Massachusetts)

The following statistics are from the Federal Bureau of Investigations CJIS division. In 2016, Identity Theft and Hacking/Computer Invasion were added as fraud offenses to the National Incident-Based Reporting System (NIBRS) data collection (Decker, 2020, p. 591). The data represents reported offenses by individual cities and towns in Massachusetts. This author included other offenses aside from Hacking/Computer Invasion surmising that the included categories *may* have some aspect of cyber criminality though the statistics do not reflect this. It is hopeful that as more focus is generated on cybercrimes that the more detailed NIBRS data will expound on the crime categories as it relates to cybercrime.

In 2018, 3,049 cases of hacking/computer invasion, 706 cases of identity theft, 664 cases of wire fraud were reported through NIBRS. Each cybercrime comprised 18.01%, 4.13%, and 3.88% of total Fraud offenses, respectively.

»» [Table 3-3-7] Crimes Reported to NIBRS 2018 for All Cities and Towns in Massachusetts

City/Town	Population	Fraud Offenses					Obscene Pornography
		Total	Credit Card/ATM Fraud	Wire Fraud	Identity Theft	Hacking/Computer Invasion	
Total		17,096	3,476 (20.33%)	664 (3.88%)	706 (4.13%)	3,079 (18.01%)	534
Abington	16,443	50	16	2	0	111	0
Acton	24,038	129	0	35	0	127	2
Acushnet	10,576	17	7	0	0	47	0
Adams	8,036	18	1	0	0	63	0
Agawam	28,955	128	55	1	0	286	0
Amesbury	17,623	38	12	0	0	124	3
Amherst	40,242	32	7	0	0	126	0

86 Comparative Study on the metric of cybercrime between the U.S. and South Korea

City/Town	Population	Fraud Offenses					Obscene Pornography
		Total	Credit Card/ATM Fraud	Wire Fraud	Identity Theft	Hacking/Computer Invasion	
Andover	36,324	119	0	49	5	139	0
Aquinnah	329	0	0	0	0	3	0
Arlington	45,876	93	51	0	0	148	4
Ashburnham	6,335	13	0	0	0	17	0
Ashland	17,860	51	22	0	0	77	1
Athol	11,721	27	6	1	0	129	0
Attleboro	44,719	191	44	11	1	444	8
Auburn	16,771	76	21	0	0	297	1
Ayer	8,246	31	12	2	1	56	0
Barnstable	44,015	132	17	14	0	370	1
Bedford	14,319	16	0	0	0	48	0
Belchertown	15,165	31	10	1	0	68	0
Bellingham	17,184	53	16	0	0	239	0
Belmont	26,700	74	44	0	0	117	0
Berkley	6,748	12	4	0	0	0	0
Berlin	3,222	9	1	0	3	0	1
Bernardston	2,108	14	1	0	0	0	0
Beverly	42,114	81	25	15	0	0	2
Billerica	44,482	123	29	29	38	6	5
Blackstone	9,345	5	0	1	0	0	1
Bolton	5,335	21	2	0	0	0	4
Bourne	19,894	77	7	0	1	0	3
Boxborough	6,634	14	1	0	0	0	0
Boxford	8,355	18	10	1	0	2	0
Boylston	4,674	5	5	0	0	0	0
Braintree	37,345	151	53	94	0	0	1
Brewster	9,831	21	3	0	0	0	1
Bridgewater	27,584	49	7	0	0	0	1
Brockton	95,922	282	24	0	0	0	17
Brookline	59,199	85	22	20	0	0	0
Burlington	27,562	136	19	0	0	0	4
Cambridge	114,881	491	42	0	0	0	9
Canton	23,709	65	20	0	2	0	1
Carlisle	5,289	15	3	0	0	0	1
Carver	11,743	33	3	0	2	0	2
Charlton	13,652	50	1	0	1	0	3
Chatham	6,174	19	2	0	0	0	0

City/Town	Population	Fraud Offenses					Obscene Pornography
		Total	Credit Card/ATM Fraud	Wire Fraud	Identity Theft	Hacking/Computer Invasion	
Chelmsford	35,264	120	59	42	0	0	3
Chelsea	40,974	128	18	0	0	0	6
Chilmark	923	5	0	0	0	0	0
Clinton	14,009	3	1	0	0	0	0
Cohasset	8,665	32	2	1	1	0	0
Concord	19,459	50	8	0	1	0	0
Dalton	6,556	4	1	0	0	0	1
Danvers	27,703	114	46	3	0	0	3
Dartmouth	34,322	126	11	0	2	0	2
Dedham	25,437	50	38	1	0	0	0
Deerfield	5,012	13	1	0	0	0	1
Dennis	13,872	58	9	1	2	1	1
Douglas	8,925	14	0	0	1	0	0
Dover	6,104	30	10	1	1	0	0
Dracut	31,917	88	23	0	10	0	1
Dudley	11,807	11	0	0	0	0	3
Dunstable	3,407	4	0	0	0	0	0
Duxbury	16,049	46	3	0	1	0	0
East Bridgewater	14,558	43	1	0	1	0	3
Eastham	4,871	23	3	0	1	1	2
Easthampton	16,050	33	5	0	0	0	3
East Longmeadow	16,398	45	7	0	0	0	4
Easton	25,225	63	0	0	3	0	4
Edgartown	4,357	8	0	0	0	0	0
Erving	1,762	11	2	0	0	0	2
Everett	47,005	143	85	8	22	0	1
Fairhaven	16,076	52	6	0	0	0	2
Fall River	89,475	253	10	1	0	0	15
Falmouth	31,033	126	4	0	0	0	10
Fitchburg	40,836	118	17	0	0	0	7
Foxborough	17,667	58	7	0	0	2	4
Framingham	72,510	100	37	0	0	0	2
Franklin	33,156	8	8	0	0	0	0
Freetown	9,404	22	3	0	0	0	3
Gardner	20,704	80	4	0	0	0	5
Georgetown	8,757	26	7	0	1	0	2
Gill	1,498	2	0	0	0	0	0

88 Comparative Study on the metric of cybercrime between the U.S. and South Korea

City/Town	Population	Fraud Offenses					Obscene Pornography
		Total	Credit Card/ATM Fraud	Wire Fraud	Identity Theft	Hacking/Computer Invasion	
Gloucester	30,356	66	19	0	0	0	1
Goshen	1,067	0	0	0	0	0	0
Grafton	18,900	31	4	0	3	0	1
Granby	6,347	11	2	0	0	0	0
Great Barrington	6,821	2	0	0	0	0	1
Greenfield	17,443	53	8	0	0	0	1
Groton	11,462	22	6	0	0	0	1
Groveland	6,833	7	3	0	0	0	0
Hadley	5,347	48	9	0	0	0	0
Halifax	7,901	25	0	0	0	0	0
Hamilton	8,088	25	1	0	0	0	1
Hampden	5,213	7	1	0	0	0	0
Hanover	14,521	75	36	1	0	0	0
Hanson	10,858	20	6	0	1	0	3
Hardwick	3,029	8	0	0	1	0	0
Harvard	6,572	79	7	0	0	0	1
Harwich	12,130	42	3	1	0	0	0
Hatfield	3,302	6	0	0	0	0	0
Haverhill	64,012	143	39	0	0	0	8
Hingham	23,588	71	20	0	0	0	1
Holbrook	11,052	38	5	0	0	0	3
Holland	2,502	3	0	0	0	0	1
Holliston	14,924	10	1	0	0	0	1
Holyoke	40,470	75	41	0	1	0	7
Hopedale	5,984	5	2	0	0	0	1
Hopkinton	18,516	11	2	0	1	0	0
Hudson	20,060	29	6	0	0	0	1
Ipswich	14,107	24	4	0	1	0	1
Kingston	13,700	39	10	0	0	0	3
Lakeville	11,525	0	0	0	0	0	1
Lancaster	8,074	22	5	0	1	0	2
Lee	5,694	8	2	0	0	0	1
Leicester	11,435	35	2	0	1	0	3
Lenox	4,941	6	0	1	0	0	1
Leominster	41,727	187	21	0	0	0	7
Lexington	34,050	37	8	0	8	0	0
Lincoln	6,839	9	4	0	0	0	0

City/Town	Population	Fraud Offenses					Obscene Pornography
		Total	Credit Card/ATM Fraud	Wire Fraud	Identity Theft	Hacking/Computer Invasion	
Littleton	10,292	28	3	1	0	0	1
Longmeadow	15,898	44	2	0	0	0	0
Lowell	111,989	334	126	32	0	0	7
Ludlow	21,590	77	9	0	0	0	1
Lunenburg	11,498	40	6	0	3	0	2
Lynn	94,558	208	53	0	0	0	7
Lynnfield	13,141	45	9	0	0	0	0
Malden	61,469	80	21	0	0	0	4
Manchester-by-the-Sea	5,428	8	4	3	0	0	0
Mansfield	24,050	97	15	0	2	0	2
Marblehead	20,652	42	8	2	1	0	1
Marion	5,134	25	0	0	0	0	1
Marlborough	40,052	199	16	0	0	0	3
Marshfield	25,922	13	0	0	0	0	3
Mashpee	14,215	45	7	0	0	0	1
Mattapoissett	6,369	8	3	0	1	0	0
Maynard	10,744	21	3	0	0	0	4
Medford	57,997	75	3	0	0	0	0
Medway	13,406	3	0	0	0	0	2
Melrose	28,552	30	1	1	0	0	0
Mendon	6,130	16	1	0	1	0	2
Merrimac	6,993	10	2	0	0	0	1
Methuen	50,676	192	102	1	1	0	1
Middleboro	25,125	70	10	1	2	1	5
Middleton	9,991	1	0	0	0	0	0
Milford	29,056	85	11	1	0	0	3
Millbury	13,802	65	9	0	1	0	1
Millville	3,260	9	2	0	1	0	1
Milton	27,642	8	1	0	7	0	1
Monson	8,890	23	3	0	0	0	1
Montague	8,235	12	0	0	0	0	1
Nahant	3,513	3	1	0	0	0	0
Nantucket	11,388	26	10	4	0	0	1
Natick	36,717	97	20	0	0	0	8
Needham	31,264	109	4	0	0	0	3
New Bedford	95,106	481	21	0	4	1	21
New Braintree	1,028	0	0	0	0	0	0

90 Comparative Study on the metric of cybercrime between the U.S. and South Korea

City/Town	Population	Fraud Offenses					Obscene Pornography
		Total	Credit Card/ATM Fraud	Wire Fraud	Identity Theft	Hacking/Computer Invasion	
Newbury	7,135	23	2	0	0	1	4
Newburyport	18,146	74	13	0	1	0	4
Newton	89,505	194	44	21	34	5	1
Norfolk	11,872	30	3	4	21	0	0
North Adams	12,858	51	12	0	0	0	9
Northampton	28,587	92	8	0	0	0	6
North Andover	31,394	43	3	0	1	0	1
North Attleboro	29,208	62	30	27	5	0	0
Northborough	15,124	0	0	0	0	0	0
Northbridge	16,759	46	4	0	0	0	0
Northfield	2,982	2	0	0	0	0	0
North Reading	15,849	17	4	0	0	0	1
Norton	19,983	15	0	0	0	0	0
Norwell	11,144	16	1	0	1	0	1
Norwood	29,267	121	19	3	0	0	3
Oak Bluffs	4,699	7	0	0	0	0	1
Oakham	1,952	2	0	0	1	0	0
Orleans	5,809	17	0	0	0	0	1
Oxford	14,015	47	3	0	1	0	2
Palmer	12,320	24	1	0	0	0	3
Paxton	4,888	3	0	0	1	0	0
Peabody	53,209	152	39	0	0	0	1
Pelham	1,326	1	0	0	0	0	0
Pembroke	18,446	51	3	0	0	0	2
Pepperell	12,234	37	3	0	0	0	1
Pittsfield	42,298	149	6	0	0	0	15
Plainville	9,281	37	16	2	13	0	0
Plymouth	60,349	125	16	0	0	0	6
Plympton	2,988	10	1	0	0	0	0
Princeton	3,458	3	1	0	0	0	0
Provincetown	2,960	23	3	0	0	0	1
Quincy	94,388	302	75	2	0	0	2
Randolph	34,535	62	23	12	0	0	2
Raynham	14,320	55	7	1	0	0	1
Reading	26,293	32	32	0	0	0	0
Rehoboth	12,268	56	6	0	5	0	0
Revere	54,296	169	14	0	0	0	11

City/Town	Population	Fraud Offenses					Obscene Pornography
		Total	Credit Card/ATM Fraud	Wire Fraud	Identity Theft	Hacking/Computer Invasion	
Rochester	5,623	13	3	0	0	0	5
Rockport	7,284	5	1	0	0	0	0
Rowley	6,392	6	1	0	1	0	3
Rutland	8,803	24	3	0	1	1	2
Salem	43,634	225	55	10	47	1	1
Salisbury	9,567	40	4	0	0	0	1
Sandwich	20,248	44	1	0	0	0	0
Saugus	28,471	127	23	0	3	0	0
Scituate	18,761	28	7	0	0	0	1
Seekonk	15,820	54	18	0	1	0	2
Sharon	18,373	21	2	0	0	0	1
Shelburne	1,842	7	1	0	0	0	0
Sherborn	4,351	30	1	0	0	0	0
Shirley	7,724	11	2	2	0	0	2
Shrewsbury	37,631	54	11	0	41	1	0
Somerset	18,166	48	4	0	0	0	3
Somerville	82,161	174	48	0	0	0	1
Southampton	6,254	9	3	0	2	0	1
Southborough	10,187	24	3	0	1	0	1
Southbridge	16,933	73	9	0	4	0	6
South Hadley	17,799	72	7	0	0	0	5
Southwick	9,810	27	5	0	0	0	0
Spencer	11,989	35	6	17	0	0	0
Springfield	155,179	803	286	37	59	1	26
Sterling	8,181	19	3	0	0	0	0
Stockbridge	1,900	10	1	0	0	0	0
Stoneham	22,135	87	2	0	0	0	1
Stoughton	28,729	73	11	0	0	0	2
Stow	7,171	21	7	0	1	0	0
Sturbridge	9,626	37	5	0	0	0	1
Sudbury	19,037	61	5	0	0	0	5
Sunderland	3,638	2	1	0	0	0	1
Sutton	9,527	49	6	0	0	0	0
Swampscott	15,380	37	9	0	0	0	0
Swansea	16,619	53	11	0	0	0	2
Taunton	57,304	40	4	0	0	0	4
Templeton	8,156	11	2	0	0	0	2

92 Comparative Study on the metric of cybercrime between the U.S. and South Korea

City/Town	Population	Fraud Offenses					Obscene Pornography
		Total	Credit Card/ATM Fraud	Wire Fraud	Identity Theft	Hacking/Computer Invasion	
Tewksbury	31,561	136	12	0	0	0	1
Tisbury	4,131	7	0	0	0	0	0
Topsfield	6,628	12	0	0	0	0	0
Townsend	9,600	17	4	0	1	0	4
Truro	2,004	9	0	0	1	0	0
Tyngsboro	12,499	17	3	0	0	0	1
Upton	7,979	28	4	0	1	0	1
Wakefield	27,447	118	8	0	1	0	2
Wales	1,902	3	0	0	0	0	0
Walpole	25,204	80	13	0	0	0	3
Waltham	62,655	100	3	0	0	0	1
Ware	9,850	17	2	0	0	0	2
Wareham	22,747	65	6	1	1	0	1
Watertown	36,320	126	20	16	1	0	0
Wayland	14,088	0	0	0	0	0	0
Webster	17,051	49	4	1	0	1	3
Wellesley	29,681	75	13	0	1	0	0
Wellfleet	2,733	3	1	0	0	0	0
Wenham	5,299	7	3	1	0	0	0
Westborough	19,226	78	15	1	9	1	1
West Boylston	8,103	31	3	2	4	0	0
West Bridgewater	7,272	47	3	0	1	0	0
Westfield	41,854	119	21	0	0	0	5
Westford	24,649	26	3	0	0	0	3
Westminster	7,835	19	6	0	0	0	2
West Newbury	4,694	15	2	0	1	0	1
Weston	12,264	11	2	0	0	0	1
Westport	15,959	42	3	0	4	0	1
West Springfield	28,802	163	9	0	2	0	7
West Tisbury	2,920	3	0	0	0	0	1
Westwood	16,267	77	9	0	2	0	0
Weymouth	57,069	125	18	0	0	0	5
Whately	1,559	4	0	0	0	0	0
Whitman	15,093	23	2	0	0	0	2
Wilbraham	14,760	43	5	1	2	1	0
Williamsburg	2,493	3	0	0	0	0	0
Williamstown	7,845	10	1	0	0	1	2

City/Town	Population	Fraud Offenses					Obscene Pornography
		Total	Credit Card/ATM Fraud	Wire Fraud	Identity Theft	Hacking/Computer Invasion	
Wilmington	24,005	60	8	0	0	0	0
Winchendon	10,933	30	1	0	0	0	7
Winchester	23,036	0	0	0	0	0	0
Winthrop	18,783	39	5	0	0	0	0
Woburn	39,895	158	27	2	0	0	0
Worcester	186,188	1,118	405	98	269	14	9
Wrentham	11,952	39	4	2	17	0	0
Yarmouth	23,269	55	13	0	0	0	3
Assumption College	2,913	3	0	0	0	0	0
Bentley University	5,771	3	1	0	0	0	0
Boston University	40,807	76	15	17	0	0	1
Bridgewater State University	13,289	8	0	0	0	0	0
Dean College	1,568	0	0	0	0	0	0
Hampshire College	1,382	3	1	0	0	0	0
Massachusetts College of Liberal Arts	2,249	1	0	0	0	0	0
Massachusetts Institute of Technology	12,144	17	1	0	0	0	0
Massasoit Community College	10,613	2	0	0	0	0	0
Mount Holyoke College	2,599	8	2	1	0	0	0
Quinsigamond Community College	10,602		0	0	0	0	0
Salem State University	11,057	3	0	0	0	0	0
Smith College	3,221	1	0	0	0	0	0
Springfield Technical Community College	7,713	0	0	0	0	0	0
Tufts University:							
Medford	12,802	6	1	0	0	0	0
Suffolk		1	0	0	0	0	0
Worcester		1	1	0	0	0	0
University of Massachusetts:							
Amherst	34,778	22	4	0	0	0	3
Harbor Campus, Boston	20,882	3	0	0	0	0	0
Medical Center, Worcester	1,171	4	0	0	0	0	0

City/Town	Population	Fraud Offenses					Obscene Pornography
		Total	Credit Card/ATM Fraud	Wire Fraud	Identity Theft	Hacking/Computer Invasion	
Westfield State University	8,017	3	0	0	0	1	0
Worcester Polytechnic Institute	7,288	7	2	0	0	0	0

Source: FBI, CJIS division internal data, 2020.

Based on 2018 FBI data, we interviewed three of the largest police departments in Massachusetts: The Boston police department, Worcester police department, and Springfield police department. Although all three departments use NIBRS reporting system, only one - the Worcester police department - kept the specific category of ‘cybercrime.’ The Boston and Springfield police department do not have a separate crime category for cybercrimes as in Worcester.

2) Massachusetts’ Executive Office of Public Safety and Security (EOPSS)

Being made a request for cybercrime statistics, the Cybercrime Unit for the Massachusetts State police provided the below statistics based on the NIBRS data from the Massachusetts’ Executive Office of Public Safety and Security (EOPSS). The Massachusetts’ EOPSS collects NIBRS and UCR data from law enforcement agencies in accordance with the FBI’s Uniform Crime Reporting Program (Executive Office of Public Safety and Security, 2020).

The number of crimes in Massachusetts has been in the downward trend since 2010, although the year of 2019 saw a slight bump in number of crimes.

»» [Table 3-3-8] Total Arrests in Massachusetts by Year

Year	Population	Number of crimes	Crime rate Per 100,000	Clearance rate
2010	6,547,629	294,564	4,499	26%
2011	6,607,003	284,761 (-3.33%)	4,310	27%
2012	6,646,144	281,091 (-1.29%)	4,229	27%
2013	6,651,112	269,317 (-4.19%)	4,049	28%

Year	Population	Number of crimes	Crime rate Per 100,000	Clearance rate
2014	6,698,697	250,570 (-6.96%)	3,741	29%
2015	6,739,216	238,331 (-4.88%)	3,536	29%
2016	6,811,779	229,343 (-3.77%)	3,367	30%
2017	6,859,819	216,824 (-5.46%)	3,161	31%
2018	6,902,149	199,516 (-7.98%)	2,891	31%
2019	6,892,503	200,707 (0.60%)	2,912	30%

Source: Executive Office of Public Safety and Security, 2020

As stated above, the cybercrime in the U.S is dealt under the name of offense – identity theft, wire fraud, hacking/computer invasion. In 2019, the total of 865 Identity Theft, 899 wire fraud, and 59 hacking were reported, respectively. However, their clearance rates are very low from 0.67 to 2.66.

»» [Table 3–3–9] The Number of Offenses regarding Crimes Against Property Offenses in 2019

Offense Type	Total	Cleared		Not Cleared	
		Number of offenses	%	Number of offenses	%
Shoplifting	12,313	5,059	41.09	7,254	58.91
Destruction/Damage/Vandalism of Property	25,215	4,566	18.11	20,649	81.89
All Other Larceny	23,732	2,086	8.79	21,646	91.21
Burglary/Breaking & Entering	10,645	1,685	15.83	8,960	84.17
False Pretenses/Swindle/Confidence Game	9,443	1,134	12.01	8,309	87.99
Stolen Property Offenses	1,620	917	56.6	703	43.4
Theft from Building	7,495	672	8.97	6,823	91.03
Counterfeiting/Forgery	3,075	664	21.59	2,411	78.41
Robbery	2,637	618	23.44	2,019	76.56
Motor Vehicle Theft	4,775	595	12.46	4,180	87.54
Theft from Motor Vehicle	8,770	499	5.69	8,271	94.31
Impersonation	4,929	239	4.85	4,690	95.15
Credit Card/Automatic Teller Fraud	3,007	220	7.32	2,787	92.68
Pocket-picking	737	109	14.79	628	85.21
Arson	308	89	28.9	219	71.1

Offense Type	Total	Cleared		Not Cleared	
		Number of offenses	%	Number of offenses	%
Embezzlement	419	88	21	331	79
Purse-snatching	280	37	13.21	243	86.79
Theft of Motor Vehicle Parts/Accessories	1,343	29	2.16	1,314	97.84
Identity Theft	865	23	2.66	842	97.34
Extortion/Blackmail	273	20	7.33	253	92.67
Wire Fraud	899	6	0.67	893	99.33
Bribery	6	5	83.33	1	16.67
Welfare Fraud	8	1	12.5	7	87.5
Hacking/Computer Invasion	58	1	1.72	57	98.28
Theft from Coin Operated Machine or Device	19	1	5.26	18	94.74

Arrest counts provide a measure of law enforcement's response to crime. The arrest practices for certain conduct like drunkenness, disorderly conduct, vagrancy, and related violations may differ amongst agencies. However, the practices for more serious conduct like robbery, burglary, and other serious crime are more likely to be uniform across all jurisdictions. Reporting procedures require that an arrest be counted on each separate occasion a person is taken into custody or cited. NIBRS arrests include the following three categories:

- a) On-View Arrest (apprehension without a warrant or previous incident report)
- b) Summoned/Cited (not taken into custody)
- c) Taken into Custody

Annual arrest figures do not measure the number of individuals arrested, since one person may be arrested several times during the year for the same crime or different crimes. One person can also be arrested for multiple crimes at the same time; this is indicated in NIBRS through the use of the multiple arrest indicator. It should be noted that the arrestee data in this theme is NIBRS and only reflects data from agencies who have successfully submitted NIBRS data for

the selected year (Executive Office of Public Safety and Security, 2020). Since the clearance rate of cybercrime is so low, the number of areestees regarding cybercrime also significantly small- total 22 in 2019.

»» [Table 3-3-10] 2019 Crime Against Property Arrests by Offense in Massachusetts

Arrest Offense for A and B Arrests	Number of Arrestees
Shoplifting	4,959
Destruction/Damage/Vandalism of Property	1,979
All Other Larceny	1,569
Burglary/Breaking & Entering	1,402
False Pretenses/Swindle/Confidence Game	740
Stolen Property Offenses	629
Robbery	580
Theft From Building	538
Motor Vehicle Theft	457
Theft From Motor Vehicle	409
Counterfeiting/Forgery	408
Credit Card/Automatic Teller Fraud	110
Embezzlement	84
Impersonation	76
Pocket-picking	74
Arson	62
Purse-snatching	28
Theft of Motor Vehicle Parts/Accessories	15
Identity Theft	14
Wire Fraud	7
Extortion/Blackmail	6
Theft From Coin Operated Machine or Device	4
Hacking/Computer Invasion	1

Source: Executive Office of Public Safety and Security, 2020

Note: Numbers represent all countable arrests

### 3) Police Department

#### (1) Massachusetts State Police

This author made a request for cybercrime statistics to the Massachusetts State police legal division. The following was provided by the legal counsel from the Cybercrime Unit for the Massachusetts State police.

»» [Table 3-3-11] Massachusetts State Police Cybercrime cases (2017-2019)

Year	Cases
2017	653
2018	542
2019	430

Source: Massachusetts State Police Cybercrime Unit and Legal department (2020)

In a follow-up interview (*D. Brunelli*, August 13, 2020), it was explained that the statistics were a result of a request to the state police cybercrime unit for assistance regarding criminal cases. The cybercrime unit does not delineate what type of crime, for example, cyberstalking, that it is responding to, only that there was a response by the cybercrime unit when there was a request for assistance; they keep track of the number of requests for assistance only.

#### (2) Boston Police Department

Although Boston Police uses the NIBRS system for crime reporting and tracking, crimes committed over the internet or using other cybercrime methods would not change how the crime is reported. Though police may be considered factors in the commission of these crimes, the Boston Police Department do not have a separate crime category for cybercrimes (Interviewed with *F. DeLuca*, 2020).

#### (3) Worcester Police Department

Among three police departments, the Worcester Police department only kept track of specifically ‘cybercrime.’ However, as shown below provided cybercrime

statistics from the Worcester Police Department Crime Analysis Unit, cybercrimes were not delineated further, for example, identity theft, child pornography (Interviewed with T. Antul, 2020).

»» [Table 3–3–12] Worcester Police Department Total Cybercrime Cases (2017–2020)

Year	Count of P_INCID_NO	INCID_TYPE_DESC
2017	14	CYC–Cyber Crimes
2018	31	CYC–Cyber Crimes
2019	28	CYC–Cyber Crimes
2020 YTD 10/7/20	20	CYC–Cyber Crimes

Source: Worcester Police Department Crime Analysis Unit, NIBRS data, 2020

#### (4) Springfield Police Department

The Springfield Police Department adopts and uses NIBRS system. Upon inquiry, and citing ‘cybercrimes,’ the Springfield police department maintained following NIBRS codes and data.

»» [Table 3–3–13] The NIBRS Systems of the Springfield Police Department

Offense Type	NIBRS code
Child Pornography – Possession of Child Pornography – Pornography/obscene material	370
Identity Theft	26C
Impersonation – When money is taken through identity theft	26F
Hacking/Computer Invasion	26G

Source: Springfield Police Department Crime Analysis Unit, NIBRS data, 2020

Since January 1, 2017 to 2020, there have been *eleven* incident reports related to 26G with potential charges listed as identify fraud, threat to commit a crime, larceny under \$1,200, unlawful wiretap, credit card fraud, criminal harassment, unauthorized access to computer system (Interviewed with R. Walsh, 2020).

#### 4) Massachusetts Attorney General's Office

The criminal jurisdiction of the Massachusetts Attorney's General's office, supported by a team from the Massachusetts State police, investigate and prosecute the following types of crimes: public corruption, financial fraud, public trust violations, illegal narcotics offenses, insurance and employment fraud, human trafficking, and electronic crimes.

Relative to cybercrime, the Attorney General's Cybercrime Division investigates and prosecutes complex criminal cases involving digital evidence. The division is available for consultation on criminal matters involving technology and is available to conduct a forensic examination of digital evidence. In 2009, the Attorney General's office developed and manages a Digital Evidence laboratory. This laboratory not only assists other law enforcement agencies, but a houses state-of-the-art training facility.

A public records request was made to the Massachusetts Attorney General's office for the total of cybercrimes handled by the office during the last three years (2017, 2018, 2019) and, if possible, a delineation of the specific cybercrimes, for example, cyberbullying, etc. The total cybercrimes handled by the Massachusetts Attorney General's office for the three- year period is 17 cases. This number seems surprisingly low as the office is lauded by a number of law enforcement that I spoke to during the course of this research. In fact, members of law enforcement had attended the yearly cybercrime seminar presented by the office. It could be an issue in reporting procedures.

The Massachusetts Attorney General's Office is on the forefront of cybercrime investigation. For the last eight years, the office has held a National Cyber Crime Conference. The conference will be held next on April 26, 2021 to April 28, 2021. It is geared to prosecutors, law enforcement and forensic examiners.

»» [Table 3-3-14] Cybercrimes Handled by Massachusetts Attorney General's Office (2017-2019)

Cybercrime Case Type	No. of Cases
Possession/Dissemination of Child Pornography	12
Electronic/Telephonic Criminal Harassment	2
Credit Card Fraud	1
Posing/Exhibiting Child in State of Nudity	1
Dissemination of Matter Harmful to a Minor	1

Source: Massachusetts Attorney General's Office Internal Data 2017-2019

#### 4. Summary

Without a concise definition of what 'cybercrime' is, there will be no progress made on calculating the number of 'cybercrimes.' Is cybercrime something perpetrated by anonymous figures on the Dark Web hacking into personal accounts? Is it a cybercrime where a domestic violence crime is perpetrated, in part, by cyberstalking? In many conversations with law enforcement in Massachusetts and New York at all levels - federal, state, and local - the issue is first, how do we categorize cybercrime? The NIBRS reporting system is used by state and local law enforcement and contains few references to specific crimes in the particular state. Further, states differ in their description of what cybercrime is, if they categorize it at all.

For example, if a patrol officer is logging in crimes to NIBRS and the case is a domestic violence case, the case will be filed under the appropriate assault code, but if cyberstalking was involved, that will not be reported because there is no NIBRS designation for cyberstalking and the crime, in the patrol officer's estimation, is a domestic violence case.

The aforementioned state court criminal caseloads are representative of the problem as all states have different criminal statutes relative to 'cybercrime.' The tally of cybercrime, the real numbers, is like an iceberg. We see the tip of the iceberg, but we have no idea the depth and breadth of this behemoth, because

it is underwater. Without a national and very specific delineation of what cybercrime entails, the number of 'cybercrimes' committed on the state level will remain hidden and underwater.

There are jurisdictional issues as well. Most state criminal statutes require prosecutors to prove in what locale the crime occurred. Many cybercrimes are committed out of state. Some states have broadened their jurisdictional rules and others have changed statutory language to reflect that prosecution can occur where the cybercrime begins outside the state but is consummated in the state (Engle, 2020, p. 506.)

As cybercrime grows exponentially, departments struggle to fund cybercrime units. The lack of specialized cybercrime unit's thwarts detection, investigation and prosecution of this type of criminality. Another issue is the "rapid advancement of technology and the international nature of computer crime, including: (A) the use of encryption; (B) extraterritoriality; (C) international criminal activity; and (D) the authentication of hearsay rules of evidence in trial" (Engle, p. 507).

Encryption allows a person to prevent others from accessing or reading their cell phones or computers. This stymies law enforcement because they cannot access, for example, a computer to search for child pornography. The U.S. Supreme Court has not ruled on the constitutionality of forced decryption. One district court ruled that a fingerprint seizure does not violate a person's Fifth Amendment privilege against self-incrimination because it is not testimonial as revelation of a password would be (See *In re Search Warrant Application for* (redacted text in the original), 279 F. Supp. 3d 800, 806 (N.E. Ill. 2017)). These issues are challenging but must be addressed sooner than later.

There is good news on the Massachusetts front as Governor Charles Baker's Five Year Capital Investment Plan for fiscal years 2019 through 2023 includes a million and a half dollars for the study, design, and renovations to the Massachusetts State Police Headquarters in Framingham, Massachusetts to create

a new division that will address domestic and international terrorism and cybercrime/human trafficking. This portends well for small or medium-sized departments who are without the capital to start a specialized cybercrime unit of their own. The use of this new cybercrime unit will be a boon to cybercrime investigations. In the same vein, the Fusion Center, operated by the Massachusetts State Police, located in Braintree, Massachusetts provides invaluable assistance to law enforcement and prosecutors in computer and electronic cases.

Lastly, one of the most imperative tasks is to discover the true extent and breadth of the cybercrime problem in Massachusetts through specific delineations of what constitutes cybercrime and how we tally the numbers. Without that specificity, the true extent of the problem will continue to elude us.

»» [Table 3–3–15] Summary of Massachusetts Cybercrime Statistics

	NIBRS	Specific Cybercrime statistics	Note
State police department	○	×	Only responding to a request for assistance
Boston police department	○	×	
Worcester police department	○	×	
Springfield police department	○	×	
Massachusetts Attorney General's Office	×	<ul style="list-style-type: none"> <li>- Possession/Dissemination of Child Pornography</li> <li>- Electronic/Telephonic Criminal Harassment</li> <li>- Credit Card Fraud</li> <li>- Posing/Exhibiting Child in State of Nudity</li> <li>- Dissemination of Matter Harmful to a Minor</li> </ul>	- Only 17 cases were prosecuted (2017–2019)
Massachusetts' Executive Office of Public Safety and Security	○	×	<2018 # of Offenses > - Wire fraud 616 (5) - Identity Theft 825 (27) - Hacking 50 (0) * (cleared case)
FBI (Massachusetts)	○	×	<2018 statistics> - Wire fraud 664 - Identity Theft 706 - Hacking 3,079



## Chapter 4

Comparative Study on the metric of cybercrime  
between the U.S. and South Korea

# CONCLUSION

Seokbeom Kim · Youngoh Jo



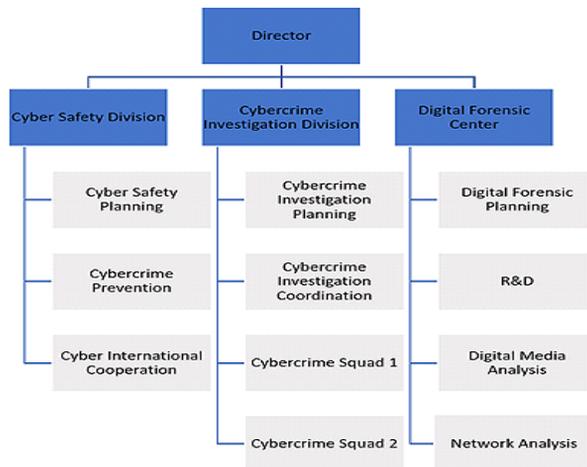
Section 1 | Comparison of the Metrics of Cybercrime

Some similarities and differences can be found concerning measuring cybercrime between South Korea and the U.S.

1. The Cyber-policing Organization

Cyber law enforcement in South Korea maintained a centralized national police system of 1,895 persons (1.51% of the total Korean police force) as of 2019.

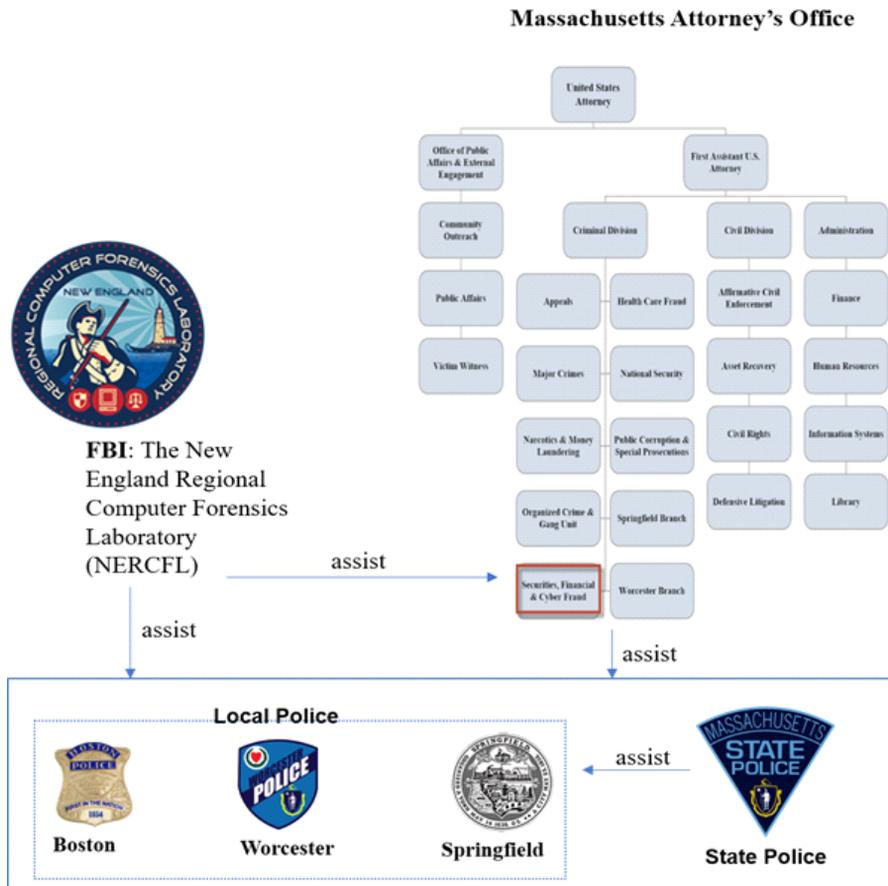
»» [Figure 4-1-1] Organization Chart of the Cybersecurity Bureau in the Korean National Police Agency



The cybersecurity bureau in the Korean National Police Agency (KNPA) takes responsibility for investigating cybercrime and making and executing cybercrime prevention strategies and policies.

In Massachusetts, The Cyber Crime Division under Securities, Financial and Cyber Fraud division investigates and prosecutes cybercrime cases involving digital evidence. FBI established The New England Regional Computer Forensics Laboratory (NERCFL), which is devoted entirely to examining digital evidence, such as computers and cell phones (RCFL, 2019). In addition, The Massachusetts legislature convened a ‘Special Senate Committee on Cyber Security Readiness.’

»» [Figure 4-1-2] Workflow Chart of the Cybercrime Investigation in Massachusetts



The committee suggests defining the scope of ‘cybercrime’ so that reporting incidents are accomplished at a federal level. This reporting accuracy ensures that adequate and appropriate funding and resources are directed to state and local jurisdictions; this would include an updating for clarity of M.G.L. c. 266, section 120, Unauthorized Access of a Computer System (Senate Legislative Committee Report, p. 27).

## 2. Definition and Classification of Cybercrime

The definition of cybercrime is dynamic in nature because cybercrime evolves according to the developments in information and communications technology (ICT). Moreover, “classification” is a means for grouping things alike. The perception of “what is alike” vary by society. Therefore, it is challenging to establish a universally established definition and criterion of cybercrime classification across countries.

In South Korea, police define cybercrime as the crime related to the illegal use of cyber-network or the infringement of computer-accessible or electronic records (Korean National Police Agency, 2020). Based on such cybercrime definition, South Korean police have categorized cybercrime into primarily three categories since 2014: the infringement of cyber-network, the unlawful use of cyber-network, and the use of illegal content.

In the U.S., any specific definition of cybercrime cannot be found. Furthermore, the term ‘computer crime’ was used in NIBRS instead of cybercrime. Among the 52 NIBRS “Group A Offenses” (i.e., the most serious offenses), three categories, listed under fraud offenses, called “wire fraud,” “hacking/computer invasion,” and “identity theft” seem to be designated for cybercrime, when compared to South Korea. Sometimes, NIBRS requires the specification of location by the offender’s intent during the crime commission. If the crime location is related to a virtual or internet-based network of two or more computers in separate locations that

communicate either through wireless or wired connections,’ then the location of the crime is coded as ‘Cyberspace’ (FBI, 2020, p. 95), which was added in fall 2014 (FBI, 2020, p. 96).

Based on the current cybercrime classification, South Korean law enforcement maintained a more detailed categorization of cybercrime and seemed to be more responsive to the current cybercrime trend.

» [Table 4-1-1] Comparison of the Official Classification of Cybercrime

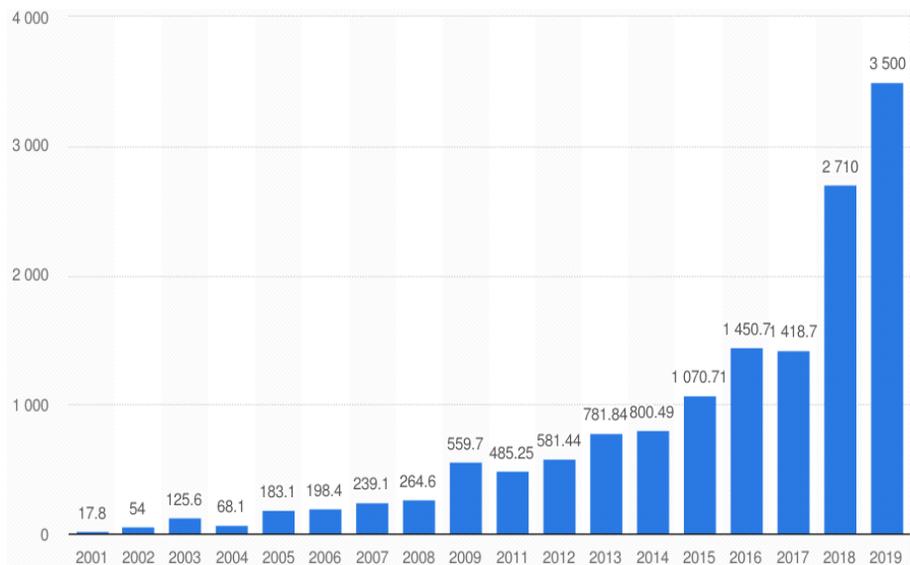
The U.S. (NIBRS)	South Korea		
	Field	Category	Group
- Identity theft - Hacking/computer invasion	Infringement of Cyber-network	Hacking	Identity theft Information leak
		DDoS	
		Malware	
		Others	
- Wire fraud	Criminal Use of Cyber-network	Internet scam	Transaction scam Cybermall scam Video game scam
		Cyber Financial Crime	Phishing Pharming Smishing Sextortion
		Infringement of personal location data	
		Infringement of copyright	
		Others	Spam mail
※ other crime (since 2014): the specification of crime location (cyberspace)	Use of Illegal Contents	Cyber porn	Porn Child porn
		Cyber gambling	Sports ToTo Racing
		Cyberstalking	
		Cyber defamation	

### 3. The Kind of Data Collected

The current cybercrime measurement in South Korea and the U.S. primarily largely relies on the incident, which the victim or third party voluntarily reports to law enforcement. The counting incidents are seemingly straightforward; however, incidents may involve one (or multiple) criminal behavior(s) against one (or multiple) victims. For example, cyberstalking might involve serial and multiple criminal behaviors, and Malware might affect multiple victims. Therefore, both South Korea and the U.S. require law enforcement to separately report the occurrence of crime, which constitutes such incidents.

Other than counting incidents or crime, there are other cybercrime measures, such as estimates of damage or financial loss or the fear of cybercrime victimizations. For example, the FBI's Internet Crime Complaint Center (IC3) has annually measured the reported monetary damage in the U.S., and then estimated the financial damage caused by cybercrime; 3.5 billion dollars in 2019.

»» [Figure 4-1-3] Reported Monetary Damage in the U.S. (in millions)



Source: IC3 annual report 2001-2019 (Clement, 2020b)

Furthermore, the FBI’s IC3 publicizes a relatively detailed victimization rate based on the victim’s self-reporting to the FBI, along with victims by age group and top 10 states by the number of victims (FBI, 2020).

»» [Table 4–1–2] Cybercrime Type by Victim Count

Crime Type	Victim Count
Phishing/Vishing/Smishing/Pharming	114,702
Non-Payment/Non-Delivery	61,832
Extortion	43,101
Personal Data Breach	38,218
Spoofing	25,789
BEC/EAC	23,775
Confidence Fraud/Romance	19,473
Identity Theft	16,053
Harassment/Threats of Violence	15,502
Overpayment	15,395
Advanced Fee	14,607
Employment	14,493
Credit Card Fraud	14,378
Government Impersonation	13,873
Tech Support	13,633
Real Estate/Rental	11,677
Lottery/Sweepstakes/Inheritance	7,767
Misrepresentation	5,975
Investment	3,999
IPR/Copyright and Counterfeit	3,892
Malware/Scareware/Virus	2,373
Ransomware	2,047
Corporate Data Breach	1,795
Denial of Service/TDoS	1,353
Crimes Against Children	1,312
Re-shipping	929
Civil Matter	908
Health Care Related	657
Charity	407
Gambling	262
Terrorism	61
Hackivist	39
Other	10,842

Source : FBI, 2019 Internet Crime Report

Regarding the victimization survey, the Korea Internet & Security Agency (KISA) and the Korean Institute of Criminology (KIC) conducted victimization surveys to supplement the official cybercrime statistics. However, there were a few victimization surveys regarding cybercrime in the U.S. (BJS, 2019), typically not

yet incorporated in the NCVS.

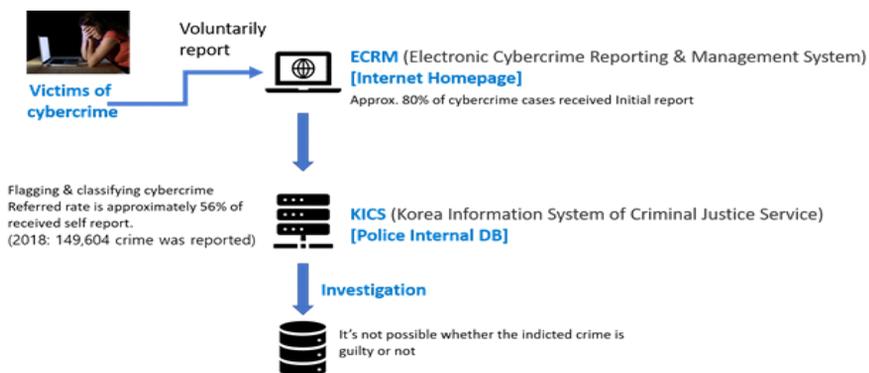
»» [Table 4-1-3] Comparison of the Kind of Cybercrime Data Collected

	South Korea	The U.S.
Incident	○	○
Crime	○	○
Characteristics of Victim (Count, age, etc.)	×	○
Financial Losses (estimates)	×	○
Victimization Survey	○	×

#### 4. The Levels of Data Collected

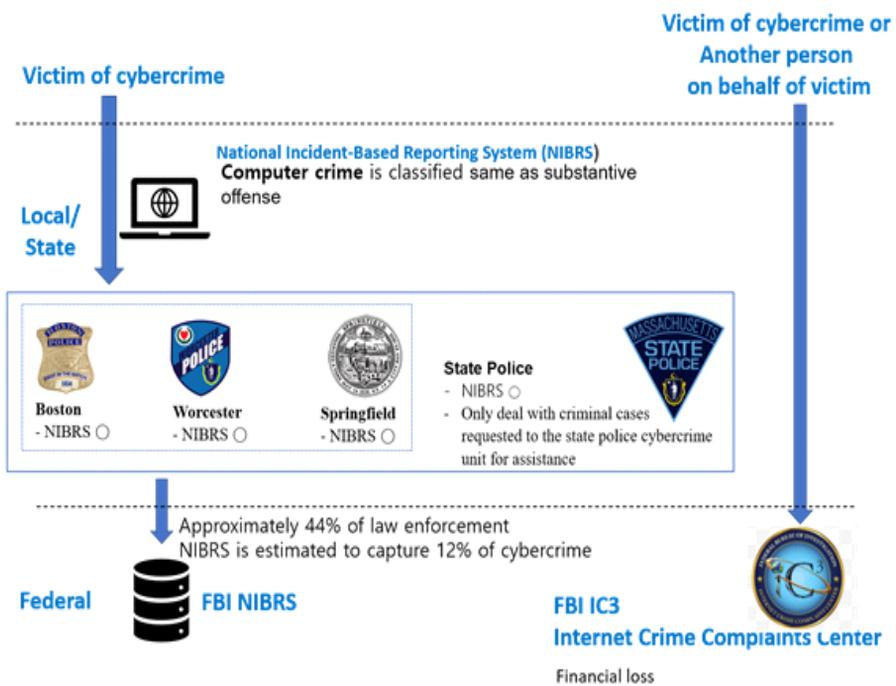
In South Korea, cybercrime victims or the third party (the legal representative) can voluntarily report their cybercrime victimization to the police. This initial reporting consists of approximately 80% of the cybercrime cases reported in South Korea in 2018. After the initial investigation, about 56% of the reported crime was registered as an official crime in 2018. Therefore, the local, regional, and national-level cybercrime statistics can be collected through the centralized police system. However, the current system does not track whether the registered crime was indicted or not in the court.

»» [Figure 4-1-4] The Flowchart of Reporting Cybercrime in South Korea



In the U.S., the local, state, and national-level cybercrime statistics can be collected through NIBRS, but very limited to specific crimes, like hacking, as mentioned earlier. Typically, there is no assigned police officer to tackle cybercrimes at the local level. The role of state police is limited to assist local police only when local police asked state police to intervene in the cybercrime case.

» [Figure 4-1-5] The Flowchart of Reporting Cybercrime in the U.S.



Jurisdictional issues are the most salient issue to the local and state police in the U.S. Many cybercrimes are committed out of state or internationally. Some states have broadened their jurisdictional rules, but it is challenging to prosecute cybercrime outside the state. For example, the total cybercrimes handled by the Massachusetts Attorney General’s office for the three- year period is only 17 cases. This number seems surprisingly low. These features hinder the understanding of the extent and prevalence of cybercrime. Another problem regarding NIBRS is

that only approximately 44% of law enforcement joined NIBRS at the national level. Therefore, the cybercrime statistics through NIBRS are estimated to only account for 12% of the U's total cybercrime in the U.S.

## Section 2 | Policy Implication

### 1. Developing Index Cybercrime

Crime can be defined as an act that the law makes punishable (Garner, 2014). However, what behavior can be punishable vary greatly across nations. For example, cyber defamation, an act of intentionally insulting or offending other individual(s) or group(s) in cyberspace, is rarely punished in the U.S. because American society puts more value on the freedom of speech. In contrast, cyber defamation accounts for almost 11% of the entire cybercrime in South Korea. Therefore, it would not be very meaningful to compare simple cybercrime occurrences reported across nations unless the meaning of cybercrime is the same or similar across countries.

Index crime has been widely used in traditional crime statistics to compare one nation's crime level to another. In the U.S., eight crimes (violent crime: murder, rape, robbery, and aggravated assault; property crime: burglary, larceny, motor vehicle theft, and arson) have served as a standard indicator of the nation's crime level because of their seriousness and frequent occurrence. Cybercrime also needs a kind of index cybercrime to compare cybercrime trends across countries. Future research should delve into developing index cybercrime.

## 2. Adopting Alternative Measures of Cybercrime

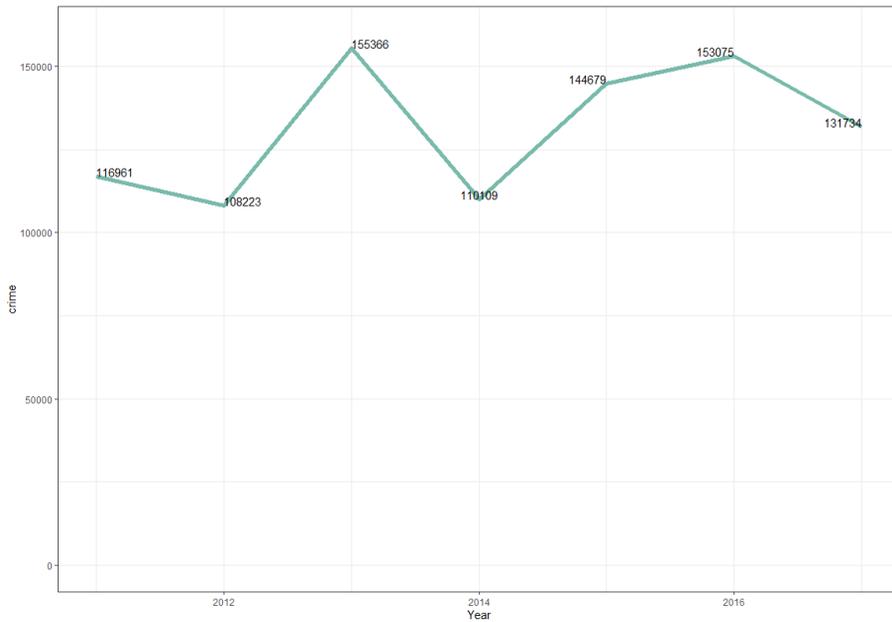
The U.S. has seen that changing the current cybercrime classification typically requires either enacted legislation or the long-years advisory process. Consequently, it would be challenging for the crime statistics to adapt to the broader range of new cybercrime offenses and offense types that characterize contemporary cybercrime. Although South Korea could relatively quickly and easily change cybercrime categorization, official data is said to be lagged behind the current cybercrime trend. Victimization survey plays an essential role in supplementing the official data since it is well known to be flexible to categorize cybercrime. Therefore, a victimization survey can mirror the current trend of cybercrime.

In addition, According to the Korean official data, internet scam accounts for slightly over 47% of reported cybercrime in 2019. But its portion has been getting grower over time. Therefore, South Korean police should gather information about financial losses caused by the cyber scam, etc., as publicized in the FBI's IC3 report. The recovered financial losses would be a good performance indicator of cyber law enforcement.

## 3. Enhancing the Reliability of Official Cybercrime Statistics

The reported cybercrime statistics fluctuate year by year. Nearly 50,000 cases were increased from 2012 to 2013, but approximately 45,000 cases were decreased in 2014. Such fluctuation might be related to the cybercrime reporting system. As we already earlier, the reported cybercrime was initially reviewed or consulted by the police. During this process, a substantial amount of reported cybercrimes was excluded for further criminal investigation. In the future, the Korean police's initial filtering process should be regulated by objective guidelines. NIBRS manual would be a good example of such approaches.

»» [Figure 4-2-1] Trend in Reported Cybercrime in South Korea



#### 4. Publicize Detailed Official Cybercrime Data

UCR and NIBRS have publicized detailed crime data. Such openness contributes to accumulating the knowledge of characteristics of offenders as well as victims through numerous research. South Korean law enforcement has boasted of collecting more detailed cybercrime data than any other country. Still, their hesitance to publicize cybercrime data hinders the further understanding of the characteristics of cybercrime. South Korean law enforcement should consider disclosing detailed information on cybercrime so that academia or related parties can conduct various independent research on cybercrime, which, in turn, contributes to measuring and preventing cybercrime in the future.



# References

- Aitken. R. (2019). Official Annual Cybercrime Report, Herjavec Group, Retrieved (2. May. 2020.). From <https://www.forbes.com/sites/rogeraitken/2018/08/19/global-information-security-spending-to-exceed-124b-in-2019-privacy-concerns-driving-demand/#b66e01971128>.
- Australian Federal Police. (2020). *cybercrime*. Retrieved from <https://www.afp.gov.au/what-we-do/crime-types/cyber-crimel>
- Baum, K., Catalano, S., Rand, M., & Rose, K. (2009). *Stalking Victimization in the United States*. Washington, D.C.: U.S. Department of Justice.
- Baylon, C. & Antwi-Boasiako. A.(2016). Increasing Internet Connectivity While Combatting Cybercrime: Ghana as a Case Study (Paper Series: No: 44). Global Commission on Internet Governance. [https://www.cigionline.org/sites/default/files/documents/GCIG%20no.44\\_0.pdf](https://www.cigionline.org/sites/default/files/documents/GCIG%20no.44_0.pdf)
- Bebinger, M. (2019, March 21). Fentanyl-Linked Deaths: The U.S. Opioid Epidemic's Third Wave Begins, *NPR News*. Retrieved from <https://www.npr.org/sections/health-shots/2019/03/21/704557684/fentanyl-linked-deaths-the-u-s-opioid-epidemics-third-wave-begins>
- Brenan, M. (2018). Cybercrimes Remain Most Worrisome to Americans, Gallup poll, <https://news.gallup.com/poll/244676/cybercrimes-remain-worrisome-americans.aspx> (Accessed 20. May. 2020.)
- Centers for Disease Control and Prevention, CDC National Center for Injury Prevention and Control, Issue brief. July 2017, Retrieved from <https://www.cdc.gov/drugoverdose/pdf/pbss/PBSS-Report-072017.pdf>
- Clement, J. (2020a). The annual number of data breaches and exposed records in the United States from 2005 to 2019 (in millions), Retrieved from <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

- Clement, J. (2020b). *Amount of monetary damage caused by reported cybercrime to the IC3 from 2001 to 2019 (in million U.S. dollars)*, Retrieved from <https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/>
- Clement, J. (2019). *U.S. perception towards police response to fight cybercrime 2018*, Retrieved from <https://www.statista.com/statistics/1022724/perception-of-law-enforcement-response-to-cybercrime-us/>
- CSO (2020, Apr 17). The 15 biggest data breaches of the 21st century, Retrieved from <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>
- Department of Home Affairs. (2020). Australia's cyber security strategy 2020, Retrieved from <https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf>
- Drakulich, K. M. (2015). Concerns for self or family? Sources of and responses to altruistic fear. *Journal of Interpersonal Violence, 30*(7), 1168-1207. doi:10.1177/0886260514539842
- Drug Enforcement Administration. (2018, September). *Tracking Fentanyl: The china connection*. Retrieved (June 9, 2020). From: [https://www.dea.gov/sites/default/files/2018-09/DEA%20Testimony%20-%20China%20and%20Fentanyl%20HFAC\\_0.pdf](https://www.dea.gov/sites/default/files/2018-09/DEA%20Testimony%20-%20China%20and%20Fentanyl%20HFAC_0.pdf).
- European Union, Cybercrime Programme Office of the Council of Europe (C-PROC), Cybercrime Division. (2019). Global action on cybercrime extended, Version 10.
- Executive Office of Public Safety and Security. (2020). Crime Statistics. Retrieved from <https://www.mass.gov/crime-statistics>
- Ferraro, K. F. (1996). Women's fear of victimization: Shadow of sexual assault? *Social Forces, 75*(2), 667-690. doi:10.1093/sf/75.2.667
- Grohe, B., DeValve, M., & Quinn, E. (2012). Is perception reality? The comparison of citizens' levels of fear of crime versus perception of crime problems in communities. *Crime Prevention & Community Safety, 14*(3), 196-211.

doi:10.1057/cpcs.2012.3

- Henry, N., & Powell, A. (2018). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma, Violence, & Abuse*, 19(2), 195-208. <https://doi.org/10.1177/1524838016650189>
- Holt, T.J., & Bossler, A.M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30, 1-25.
- Holt., T. J. & Bossler, A. M. (2017). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*, New York: Routledge.
- James, N. (2018, June). *Recent Violent Crime Trends in the United States*, Congressional Research Service (7-5700), Retrieved (June 9, 2020). From: <https://fas.org/sgp/crs/misc/R45236.pdf>.
- Kappes, C., Greve, W., & Hellmers, S. (2013). Fear of crime in old age: Precautious behaviour and its relation to situational fear. *European Journal of Ageing*, 10(2), 111-125. doi:10.1007/s10433-012-0255-3
- Korean Institute of Criminology. (2009). *Korean Crime Survey in 2008*.
- Kraft, E.M., & Wang, J. (2010). An exploratory study of the cyberbullying and cyberstalking experiences and factors related to victimization of students at a public liberal arts college. *International Journal of Technoethics*, 1, 74-91.
- May, D. C., Rader, N. E., & Goodrum, S. (2010). A gendered assessment of the "Threat of Victimization": Examining gender differences in fear of crime, perceived risk, avoidance, and defensive behaviors. *Criminal Justice Review (Sage Publications)*, 35(2), 159-182. doi:10.1177/0734016809349166
- McGuire, M., & Dowling, S. (2013). *Cyber Crime: A Review of the Evidence. Research Report 75, Summary of key findings and implications*. London: U.K. Home Office.
- Miethe, T. D. (1995). Fear and withdrawal from urban life. *The ANNALS of the American Academy of Political and Social Science*, 539(1), 14-27. doi:10.1177/0002716295539001002

- Morgan, R. E. & Oudekerk B. A. (2019, September). *Criminal Victimization*, 2018. Retrieved (May 27, 2020). From: <https://www.bjs.gov/content/pub/pdf/cv18.pdf>.
- Morgan, S. (2019). Global Information Security Spending To Exceed \$124B In 2019, Privacy Concerns Driving Demand, *Forbes*, Retrieved (2. May. 2020.) From <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>.
- Office for National Statistics, Crime Survey for England and Wales (CSEW), (2020), Crime in England and Wales: Appendix tables, Retrieved (June 9, 2020). From: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables>.
- Parliamnet of Australia. (2020). *Cybercrime Legislation Amendment Bill 2011*, Retrieved from [https://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/bd/bd1112a/12bd031#:~:text=The%20Cybercrime%20Legislation%20Amendment%20Bill,Act%201997%20\(the%20Telecommunications%20Act\)](https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1112a/12bd031#:~:text=The%20Cybercrime%20Legislation%20Amendment%20Bill,Act%201997%20(the%20Telecommunications%20Act))
- Rader, N. E., Cossman, J. S., & Allison, M. (2009). Considering the gendered nature of constrained behavior practices among male and female college students. *Journal of Contemporary Criminal Justice*, 25(3), 282-299. doi:10.1177/1043986209335015
- Rosenfeld, R. & Weisburd, D. (2016). Explaining Recent Crime Trends: Introduction to the Special Issue. *J Quant Criminol* 32, 329-334 <https://doi.org/10.1007/s10940-016-9317>
- Roser, M., Ritchie, H. & Ortiz-Ospina, E. (2015). *Internet*. Published online at OurWorldInData.org. Retrieved (June 9, 2020). From: <https://ourworldindata.org/internet>.
- Scammers steal "hundreds of millions" using fake unemployment claims (2020, May 27), *CBS News*. Retrieved from <https://www.cbsnews.com/news/unemployment-scams-fake-claims-hundreds-of-millions/>
- Sheridan, L.P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law*, 13, 627-640.

- Statistics Korea, e-Nara Indicators, ([www.index.go.kr](http://www.index.go.kr)), *Reported cybercrime cases in South Korea (2010~2018)*, Retrieved from [http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx\\_cd=1608](http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1608)
- Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2015). The dark Figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly*. DOI:10.1080/07418825.2014.994658.
- U.S. Census Bureau (2019). *2019 U.S. Population Estimates Continue to Show the Nation's Growth Is Slowing*. Retrieved from: <https://www.census.gov/newsroom/press-releases/2019/popest-nation.html>.
- U.S. Department of Justice, Bureau of Justice Statistics, Summary findings of stalking. Retrieved (23. May. 2020.). from <https://www.bjs.gov/index.cfm?ty=tp&tid=973>.
- United Nations Office on Drugs and Crime. (2019). E4J University Module Series: Cybercrime. Retrieved (12. May. 2020). From <https://www.unodc.org/e4j/en/cybercrime/module-2/introduction-and-learning-outcomes.html>
- United States Department of Justice, Federal Bureau of Investigation. (2019). National Incident-Based Reporting System User Manual, Retrieved (21. May. 2020.), from <https://www.fbi.gov/file-repository/ucr/ucr-2019-1-nibrs-user-manual.pdf/view>.
- United States Department of Justice, Federal Bureau of Investigation. (2018). 2018 Internet Crime Report. Retrieved (2. Jun. 2020.), from [https://pdf.ic3.gov/2018\\_IC3Report.pdf](https://pdf.ic3.gov/2018_IC3Report.pdf).
- United States Department of Justice, Federal Bureau of Investigation. (2019). 2019 Internet Crime Report. Retrieved (2. Jun. 2020.), from [https://pdf.ic3.gov/2019\\_IC3Report.pdf](https://pdf.ic3.gov/2019_IC3Report.pdf).
- United States Department of Justice, Federal Bureau of Investigation. (2019). FBI Releases 2018 Crime Statistics. FBI Press Releases. Retrieved (2. Jun. 2020.), from <https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-2018-crime-statistics>.
- United States Department of Justice, Federal Bureau of Investigation. (2017). Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the

- Cambridge Cyber Summit. *Justice news*, Retrieved (2. Jun. 2020), from <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rose-nstein-delivers-remarks-cambridge-cyber-summit>.
- United States White House, The Council of Economic Advisers. *The Cost of Malicious Cyber Activity to the U.S. Economy*. February 2018, pp. 1. <https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf> (Accessed 2. Jun. 2020.)
- Vieno, A., Lenzi, M., Roccatò, M., Russo, S., Monaci, M. G., & Scacchi, L. (2016). Social Capital and Fear of Crime in Adolescence: A Multilevel Study. *American Journal of Community Psychology*, 58(1-2), 100-110. doi:10.1002/ajcp.12071
- Wall, D. (2001). Cybercrimes and the Internet. In D. Wall (Ed.), *Crime and the Internet* (pp. 1-17). New York: Routledge.
- Wall, D. S. (2015, October 21). It's about time cybercrimes appeared in crime figures if we are to take the problem seriously, *Phys.org News*. Retrieved from <https://phys.org/news/2015-10-cybercrimes-crime-figures-problem.html>
- Warr, M. (1985). Fear of rape among urban women. *Social Problems*, 32(3), 238. doi:10.2307/800684
- Warr, M. (2000). Fear of crime in the United States: Avenues for research and policy. In D. Duffee (Ed.), *Measurement and analysis of crime: Criminal justice 2000* (pp. 451-489). Criminal Justice: Washington, DC: U.S. Department of Justice, Office of Justice Programs.
- Wilcox, P., Jordan, C. E., & Pritchard, A. J. (2007). A multidimensional examination of campus safety: victimization, perceptions of danger, worry about crime, and precautionary behavior among college women in the post-Clery Era. *Crime & Delinquency*, 53(2), 219-254. doi:10.1177/0097700405283664
- Wilcox, P., May, D. C., & Roberts, S. D. (2006). Student weapon possession and the "Fear and Victimization Hypothesis": Unraveling the temporal order. *Justice Quarterly*, 23(4), 502-529. doi:10.1080/07418820600985362
- Wilson, J. Q., & Kelling, G. L. (1982). Broken windows. *Atlantic Monthly*, February,

46-52.

World Bank. (2020). *Share of the population using the Internet, 1990 to 2017*. Retrieved (June 9, 2020). From: <https://ourworldindata.org/grapher/share-of-individuals-using-the-internet?tab=chart&time=1990..&country=KOR~USA>.

Zeizima, K. (2017, November 3). Why the fight against opioid abuse is happening at the post office, *the Washington Post*. Retrieved from <https://www.washingtonpost.com/national/2017/11/03/why-the-fight-against-opioid-abuse-is-happening-at-the-post-office/>





Research Report 20-B-06

**Comparative Study on the metric of cybercrime  
between the U.S. and South Korea**

First Published December 31, 2020

© In Sup Han

Printed in Seoul, Korea

by Korean Institute of Criminology

114 Taebong-no, Seocho-gu, Seoul, 06764, Republic of Korea

[www. eng.kic.re.kr](http://www.eng.kic.re.kr)

No part of this publication may be reproduced, translated, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, microfilming, recording, or otherwise, without written permission from the Publisher

I S B N | 979-11-89908-99-7 93330