International Journal of Cybersecurity Intelligence & Cybercrime

Volume 2 | Issue 1 Article 4

2-2019

The profile of the international cyber offender in the U.S.

Hadzhidimova, L., & Payne, B. (2019). *International Journal of Cybersecurity Intelligence and Cybercrime, 2* (1), 40-55.

The profile of the international cyber offender in the U.S.

Lora Hadzhidimova*, Old Dominion University, U.S.A

Brian Payne, Old Dominion University, U.S.A

Abstract:
This study explores the characteristics of international cyber offenders prosecuted in the U.S. Our findings to a large extent correspond with general studies about cyber offenders with a few important exceptions. First, the average age of the offenders in our study is slightly higher than others that do not focus exclusively on international offenders. Second, while this research confirms that China is among the leading country in committing cybercrimes when it comes to committing particular types of cybercrimes, the offenders come from other countries as well such as Romania, Estonia, Ukraine, South Africa, and Nigeria. Third, our results show that in each of the cases from the sample, the international offenders received prison sentences alone, or complemented with a fine or restitution. In addition, the sentence length of citizens of African countries is significantly higher than the ones of citizens of other geographic regions. Prison sentences for cyber frauds and identity thefts were also found to be much lengthier than sentences for other types of cybercrimes. Implications are provided.

Introduction

Cybercrime is a serious threat that faces the contemporary world. Reports show that the cost of cybercrime increased from $445 billion in 2014 to $600 billion in 2017 (Lau, 2018). The international scope of the acts, the anonymity of the perpetrators, and the obstacles that criminal justice agencies confront, exacerbate the cybercrime dilemma. In addition, many studies have found it difficult to compare the characteristics of cyber offenders and their sentences, a problem that could be attributed to the substantially different laws of countries prosecuting the offenders. The diverse legislative systems are also why international agreements about cybersecurity and extradition of criminals, in general, have been unsuccessful. Furthermore, some strategies that work in some countries may not work in others because of cultural, political and administrative reasons.

To understand appropriate criminological responses to cybercrime, it is essential to empirically assess internationally-focused data about cyber offenders. It is especially important to examine the environment from which cyber offenders are coming from, which is usually their country of origin, and

*Corresponding author
Lora Hadzhidimova, 7045 Batten Arts & Letters, Norfolk, VA 23529.
Email: lhadzhid@odu.edu

the environment in which they are inflicting the damages, which is usually where they are prosecuted. These environments should be assessed and compared in their complexity, based on the different conditions they create for facilitating or hindering cybercrime acts. Additionally, while some types of cybercrimes could be triggered by the nature of the political relationship between states, others could stem from economic reasons. To better understand international dynamics, we examine the characteristics of a non-U.S. sample of cyber offenders that were prosecuted in the U.S.

Review of Literature

Cybercrime typologies tend to focus on three different themes: (1) characteristics of offenders, (2) types of crimes committed by cyber offenders, and (3) sentences given to cyber offenders. While researchers have routinely identified the global nature of cybercrime as being one of the challenges to responding to these offenses and offenders, few studies have considered the international dynamics in relation to cybercriminal characteristics, cybercrime types, and sentencing patterns. In the following section, each of these areas are discussed with an aim towards providing an international framework for understanding and explaining cyber offending and the criminal justice system's response to these offenses.

Characteristics of Cybercriminals and International Issues

Research on the characteristics of cyber criminals has examined the demographic characteristics of cyber offenders (age and gender), their belonging to a political entity (citizenship), and their behavioral patterns (collaboration with other criminals). According to studies, the "stereotypical" perpetrator of a cybercrime is "male, 12-28 years old, single, and socially dysfunctional, possibly from a dysfunctional family" (Rogers, 2011, p. 223). However, Rogers (2011) adds that these particular factors are not the most essential in outlining a profile for cybercriminals; rather, he notes that it is more important to understand the context guiding the illicit activities. Others stress that it is also essential in more individualized profiling to collect information about the offenders' level of technical know-how, their personal traits, social characteristics, and their motivation (Saroha, 2014).

Cybercrimes are committed worldwide with such ease that sometimes events that appear to be happening from another continent are in fact much closer to the victim than it appears. Courts encounter obstacles in identifying the jurisdiction that has to handle the case. The first step toward resolving this issue is determining the citizenship of the perpetrator. According to international law, most countries respect the principle of extraterritoriality, which allows the authorities in the country of citizenship of the offender to take over the case regardless of the location of the crime (Grabosky, 2004). Two countries that have hostile relationships could compete over jurisdictional aspects, especially if an act is considered a crime in one legislative system but not a crime in the perpetrator's country of origin. All these dynamics lead Grabosky (2004) to conclude that "nations that lag behind the leaders risk becoming havens for cybercriminals of the future", (p.155).

Holt and Kilger (2012) call for more studies that include foreign citizens and their involvement in cyber and physical criminal acts. In addition, they suggest that researchers devote more time to exploring the elements that could result in cyberattacks against a foreign country's critical infrastructure. Rush et al. (2009) note that Russia, China, Brazil and India are leading nations in terms of the number of cybercrimes committed. In this regard, the cyber offender's country of origin, according to Brenner (2008), could have an underlying importance especially in places with authoritarian regimes in which the anonymity provides protection against repressive acts of violence for one's political actions. In addition, cultural factors may increase the likelihood of cyber offending (Yun et al., 2016).

Moreover, a cyber offender's country of origin and its law enforcement capabilities and legislative framework to fight cybercrime could also impact the perpetrator's determination to commit cybercrimes (Chang, 2013). Their legal awareness also plays a role in this process in which it is important to look at the average level of this component in different countries as this could contribute to addressing why some of their features appear to be conducive to cybercrime (Fedushko & Bardyn, 2013).

Additionally, cybercriminals employ different means for data encryption through which they ensure anonymity of their actions in cyberspace. They present a serious challenge to both law enforcement units and prosecutors, especially in countries with limited resources and training (Denning & Baugh, 1999; Grabosky, 2007). Moreover, the diplomatic and historical relationships between the two political entities could also affect to a large extent the level of cooperation between law enforcement officials (e.g., Japan with Burma, Cambodia, China, Laos, Taiwan, Thailand, and Vietnam, see Katzenstein & Okawara, 2002) or the lack of such, as is the case of China and Taiwan (Chang, 2012). Political tension between nations could also facilitate transnational cybercrime. On the other hand, a close relationship between the entities could limit the scope of cybercrime if agencies join efforts to combat the problem.

Another reason why more studies that examine characteristics of cyber offenders are necessary is the complexity of perpetrator networks that include foreign citizens that commit organized crimes using cyberspace (Leukfeldt, Lavorgna & Kleemans, 2017). An interview-based study conducted by Hutchings (2014) reveals the interconnectedness between cyber offenders and their readiness to collaborate in crimes. Typically, they execute the coordinated acts either in an attempt to profit from the crime financially, or in other cases, in pursuit of a political agenda set by their governments, other governmental or non-governmental entities, or themselves (Choo & Smith, 2008).

Cybercrime Types and International Issues

Two of the most common types of crimes are cyber fraud and identity theft. The 2017 Internet Crime Complaint Center (IC3) report shows that the number of victims of identity theft was 17,636 and the victims of confidence/romance fraud combined with those of credit card fraud were more than 15,500 (IC3, 2017). Research that focuses on cyber frauds finds that the perpetrators of these particular crimes are predominantly male, residents of densely populated urban areas, often with some international background, living in Eastern Europe, America, or Canada, and are usually not acting as representatives of their employers but in an individual capacity (Fried, 2001). However, some cyber fraud types are frequently committed by citizens of nations outside of these areas, but they also support the findings of the average cyber offender – males under the age of 30 (Warner, 2011). The same study also highlights that cyber frauds in Ghana are widespread, mainly identity fraud, frauds involving investments in gold mining, and estate fraud – the first two have targets that reside in Western countries, whereas the latter have targets that are mostly citizens of the offender's home country.

The central role of subcultures becomes apparent in other cybercrimes as well. Hacking, for instance, inspired the formation of a subculture among cybercriminals that emerged as a result of different levels of technological understanding (Holt, 2010). In this case, the conditions that the home country provides could also enable or restrict the access to knowledge that the hacker has. Another aspect of the hacking subculture is the element of entertainment that this activity brings to the hacker community. Turgeman-Goldschmidt (2005) argues that "seeking fun, knowledge, and computer virtuosity" (p.18) is what triggers the decision to engage in hacking.

The role of subcultures might apply differently in other forms of cybercrime. Consider, for example, theft of secrets rather than being connected to a "hacking subculture." The theft of secrets could also

take the shape of economic espionage if the criminal acts are conducted to feed into the political agenda of a state different than the one from which the secrets were stolen. What is problematic for law enforcement and prosecution in such cases is that there should be very strong evidence in support of the fact that the theft of secrets was in support and by request of foreign governments (Fidler, 2013). In cases of cyber espionage, it is even more important to identify the nationalities of the perpetrators and the authorities that they serve. Moreover, an established relationship of antagonism and lack of diplomatic relations between states and political entities could increase cyber espionage threats, as is the case with Chinese political behavior to Tibet (Deibert et al., 2009). According to some, China poses one of the biggest threats to cybersecurity. In terms of espionage practices, researchers confirm that it conducted a series of operations in order to obtain classified information from its political rivals (Hjortdal, 2011).

As for web defacement, the same conclusions are also valid, thus supporting the notion that political climate in the perpetrator's home country should be studied in detail. Holt et al. (2017) discovered that individuals "who supported the suppression of minority and outgroups in society" were more likely to engage in web defacement of government websites (p. 369).

When it comes to the cultural explanations of cybercrime, the cyber offender's country of origin can demonstrate some unique characteristics related to the target of the offense and the consequences that could follow from committing the crime. For instance, Holt and Copes (2010) conducted a study examining the subculture of digital piracy. Their findings show that digital pirates share a common understanding about the right to receive and disseminate information, while at the same time, they distinguish themselves from those who seek to gain profit from digital piracy. The sample that they used includes pirates from countries on three different continents (North America, Europe and Australia). The interviewees shared that they have little concern for the eventual legal consequences of their actions because of the perception that they will not get caught. The reality, however, could be quite different depending on the effectiveness not only of the law enforcement system but also of the judiciary in a country. Particularly in the case of digital piracy, different cultures could have different motives to perceive these crimes as "victimless". In other words, while subcultures in cybercrime networks exist independently from countries of origin "to share the meaning of specific ideas, material objects, and practices through interaction" (Williams & Copes, 2005, p.70), each member of the group could have followed a different path that led them to share these symbols of the cyberculture. The latter is a fact for which the country of origin and its culture may be responsible in the way it shapes the relationships in society both in terms of interpersonal interactions and the relationship between the state's administration and its citizens.

A critical assessment of the problem with music piracy, in particular, brings another perspective in regard to rationalizing the actions of individuals violating intellectual property laws. Some argue governments and industries establish control over the access to music and information that music pirates attempt to dismantle and rebel against (Hinduja, 2006; 2008). The power that these structures have in different countries could vary, thus, justifications for digital piracy by the pirates themselves could also differ depending on how they perceive them and their role in the process of distributing digital art products. A study by Hinduja and Higgins (2011) explored the typical characteristics of music pirates. The results showed that males were represented slightly more than females in the sample in terms of downloading frequency, similar to what is established in the literature: males typically outnumber females in pirating digital content in general (Higgins, 2006; Hollinger, 1993; Rahim et al., 1999; Sims et al., 1996; Solomon & O'Brien, 1990; Wood & Glass, 1996). The profile also revealed that mostly unemployed students, particularly those majoring in the social sciences, were illegally down-

loading content. In terms of age, 57.6% of offenders who engaged in digital piracy were 19 years of age or younger (Hinduja & Higgins, 2011).

Piracy and intellectual property violations receive a great deal of scholarly attention in the international literature. As Rutter and Bryce (2008) note, a study conducted across 68 nations by the International Intellectual Property Association showed that between 2000 and 2005, software piracy and counterfeiting increased by 100% (International Intellectual Property Association, 2006). Businesses selling counterfeit goods refer to a specific type of consumer culture that makes the user eager to own luxury goods. These illicit activities comprise of an entire business branch that was estimated by Organization for Economic Co-operation and Development to be worth approximately $200 billion in 2005 (Gistri et al., 2009). Contrary to stereotypes that describe the average users/customers of pirated software/counterfeit clothing as low-educated groups with blue-collar occupations, in a study from China, Cheung and Prendergast (2006) found that white-collar males are the biggest consumers of counterfeit/pirated goods. These findings reaffirm that international studies of cybercrimes should definitely account for culture in countries of residence/origin of the offenders.

Sentencing Cyber Offenders and International Issues

While the literature exploring sentences for traditional types of crime is voluminous and empirically diverse, there is a lack of studies focusing on the sentencing patterns of cybercrimes, especially those sentencing of international cyber offenders. One of the first studies that fills the gap in the literature in regard to the cybercrime sentencing is conducted by Marcum, Higgins and Tewksbury (2011). Among the most important findings from this study is the one that confirms a tendency that the authors highlight themselves – that the criminals who committed the most prosecuted cybercrimes (credit card fraud and identity theft) received lengthier sentences. In another study by Marcum, Higgins and Tewksbury (2012), the researchers cite U.S. Department of Justice data showing that between 2006 and 2010, 51.7% of the sentenced cybercriminals received prison time.

Smith, Grabosky and Urbas (2004) stress four major issues for prosecutors in international cases. First, establishing whose jurisdiction the case falls under is difficult. Second, the amount of evidence that is or could be collected to prosecute the case may present challenges. Third, establishing who the offender is and their physical location can be difficult. Fourth, resolving problems related to the possibility of extradition and bi-lateral agreements for legal assistance has the potential to create challenges.

It is clear that cybercrime is an international problem and cybercriminals come from all over the world. The international nature of these offenses and offenders has grown exponentially as the use of technology has spread across the world. What this means is that the potential for international cyber offending has grown dramatically. Many prior conclusions about the international aspects of cyber offending were from ancillary findings whose focus was on cybercrime in general as opposed to focusing specifically on the international issues associated with cyber offending.

There is a gap in the literature when it comes to comparative studies that explore sentencing patterns of cybercriminals across jurisdictions. Smith, Grabosky and Urbas argue that this could be attributed to a few problems, among which “imprecise and disparate definitions of computer crime that exist in many jurisdictions, the fact that many offences are prosecuted in lower level courts whose judge’s sentencing remarks are often not transcribed or reported, and the fact that computer crimes have only recently become prevalent enough to warrant special judicial attention to the collection of empirical data” (Smith, Grabosky, & Urbas, 2004, p. 125). While it is difficult to compare sentences across

jurisdictions, it is also important that research on cybercrime focus on the relationship between offending and citizenship/country of permanent residence. Therefore, in order to avoid comparing different jurisdictions but to still account for the international component in cyber offending, this study includes only on one jurisdiction (U.S.) but captures the different nationalities of cybercriminals and the variety of cybercrimes they commit. This study examines the profile of the international cyber offender in the U.S. based on personal characteristics of the offender, the types of cybercrimes they commit and responses to their actions by the U.S. criminal justice system. In this context, "international" indicates a non-U.S. citizen.

Focusing specifically on the international nature of cybercrimes and cybercriminals, the following questions are addressed: (1) What are the characteristics of international cyber offenders who are prosecuted in the U.S.; (2) What types of cybercrimes are committed by international cyber offenders prosecuted in the U.S.; (3) What are the normative patterns appearing to connect international cybercriminals with the types of crimes they commit; (4) What sentences are given to international cyber offenders; and (5) What are the patterns guiding the criminal sentences given to cyber offenders?

Methods

Data

This study uses data extracted from U.S. Department of Justice press releases between January 2009 and December 2017. The sample includes 225 offenders who are citizens of a foreign country and have been involved in an overall sample of 123 cases in which 414 crimes were committed. It should be noted that one cyber offender was involved in two separate cases.

Measure

Variables included age, gender, country of origin, number of group offenses, number of different types of offenses, and the sanction types that appear in press releases. Furthermore, we cross-tabulated the different cybercrime types with the countries of origin of the offenders. In addition, we outlined the leading countries in each offense category. Next, we conducted t-tests to examine if the average age of offenders were statistically significant when compared to offenders' gender. We repeated the same test for prison length by gender, prison length by geographic region, and prison length by offense type.

Analytic Plan

We created a coding sheet focused on three categories: personal characteristics about the perpetrator, crime-related characteristics, and sentence-related characteristics. The first section gathered data about the age, gender, and country of origin of the offender. The second section captured whether the offenders worked individually or with others, the average number of offenders in a particular case, the target of the offense, the types of the offenses, and the leading countries when it comes to a particular kind of cybercrime. The third category examined data that outline the criminal justice response to the cybercrime, the length of the sentence (if known), the amount of the fine, if any, and the restitution amount. Additional tests were conducted to identify the average age and prison lengths of the offenders by gender, country of origin, and offense type. Based on the results, we discuss the sentencing patterns and other specifics that our study revealed.

Results

Personal Characteristics

The minimum age of cyber offenders is 19 years and the maximum is 73. The average age of cyber offenders is 34.79 (N=181). As illustrated in Table 1, males are the predominant offenders, with

94% (212 out of 225) in the examined sample. Only 6% or 13 out of 225 offenders are female. The most frequently represented country of origin of cyber offenders (N=225) when all cybercrimes are considered is China (26.7%), followed by Romania (11.6%) and Russia (7.1%). Cyber offenders also came from Estonia (5.3%), Mexico (4%), Canada (4%), South Africa (3.6%), Nigeria (3.6%), Ukraine (3.1%), and Pakistan (3.1%). Other descriptive statistics are described in Table 1a-f.

Table 1a. Descriptive statistics: Offenders by age

	Minimum	Maximum	Mean
Age (N=182)	19	73	34.79

Table 1b. Descriptive statistics: Offenders by gender

	N	%
Gender (N=225)	19	73
Men	212	94.20
Women	13	5.80

Table 1c. Descriptive statistics: Offenders by country of origin

	N	%
Country of origin (N=225)		
China	60	26.7
Romania	26	11.6
Russia	16	7.1
Estonia	12	5.3
Canada	10	4.4
Mexico	9	4.0
South Africa	8	3.6
Nigeria	8	3.6
Pakistan	7	3.1
Ukraine	7	3.1
Germany	5	2.2
Iran	5	2.2
Venezuela	4	1.8
Hong Kong	3	1.3
India	3	1.3
Italy	3	1.3
Philippines	3	1.3
Sweden	3	1.3
Turkey	3	1.3
Vietnam	3	1.3
Latvia	2	0.9
Malaysia	2	0.9
Moldova	2	0.9
Cuba	2	0.9
Dominican Republic	2	0.9
U.K.	2	0.9
Other	15	6.7

Table 1d. Descriptive statistics: Group offenses

	N	%
Group Offense (N=225)		
No	71	31.6
Yes	154	68.4

Table 1e. Descriptive statistics: Offence targets

	N	%
Offense targets (N=225)		
Goods	80	35.6
Computer Systems	70	31
Personal and financial information	38	17
Trade secrets	37	16

Table 1f. Descriptive Statistics: Type of cyber offense

	N	%
Type of Cyber Offense (N=225)		
Fraud	101	44.9
Hacking	74	32.9
Counterfeit goods	57	25.3
Identity theft	53	23.6
Unauthorized access	49	21.8
Theft of secrets	38	16.9
Online sales fraud	13	5.8
Digital piracy	10	4.4
Phishing	6	2.7
Spamming	6	2.7
Securities fraud	5	2.2
Destruction of property	1	0.5
Web defacement	1	0.4

Note. The percentage calculated for this category is based on the number of offenders (N=225) and not on the total number of offenses (N=414) and thus the total sum in th is column exceeds 100%.

Crime-related Characteristics

The number of offenders involved in cybercrimes ranged from one to 29. The average number of offenders was 4.91. More than two-thirds of offenders (68.4%) were working in groups. As for the most frequently observed offense target, material and digital goods represented over 35% of overall targets of offense. Besides targeting goods, the end-goals of the cybercrimes also included computer systems (31%), personal and financial information (17%), and trade secrets (16%).

In terms of the types of cyber offenses that were committed, the results of our study show that cyber fraud is the predominant offense. The second most frequent cyber offense is hacking, followed by crimes involving counterfeit goods, identity theft, and unauthorized access. Data pointing to countries of citizenship of the offenders who commit the most commonly encountered cyber offenses are presented in Table 2. The leading countries, from which cyber offenders committing fraud mostly come from are Romania (17%), and Russia (12%). In terms of hacking, the offenders come from 27 different countries among which the leading one is Estonia (15%), followed by Romania (14%). China is where most offenders involved in counterfeit goods come from, with 47% of the overall 57 crimes, followed by

Mexico with 16%. China is also the leading country for theft of secrets. In fact, 84% of theft of secret offenses involved offenders from China. Citizens of Russia and Romania (each with 16%), followed by citizens of China (with 12%) are among the most frequent offenders who obtain unauthorized access to devices. South Africans (15%), followed by Nigerians and Ukrainians (both with 13%) commit the most identity theft.

Table 2. Citizenship of Offenders by the Most Frequently Committed Type of Cybercrimes

Citizenship of offenders by cybercrime type	Leading Country	N (%)	Second Leading Country	N (%)
Fraud (N=101)	Romania	17 (16.83%)	Russia	12 (11.88%)
Hacking (N=74)	Estonia	11 (14.86%)	Romania	10 (13.52%)
Counterfeit goods (N=57)	China	27 (47.37%)	Mexico	9 (15.79%)
Identity theft (N=53)	South Africa	8 (15.09%)	Nigeria/Ukraine	7 (13.21%)
Unauthorized access (N=49)	Russia/Romania	8 (16.33%)	China	6 (12.25%)
Theft of secrets (N=38)	China	32 (84.21%)	Canada	3 (7.89%)

The Criminal Justice Response to Non-U.S. Cybercriminals

The results of this part of our study, summarized in Table 3, reveal that for 71 of the 225 offenders, the sentence is known and involves incarceration as a sanction. The other imposed sanctions include restitution and fine. Probation was not imposed as a sanction in any of the cases from the research sample – a fact that will be explained later.

Table 3. Sanction Types in Sentences for Cybercrimes

Sanction types in sentences (N=71)	N	%	Minimum	Maximum	Mean
Incarceration	71	100	1 day	115 years	7 months
Restitution	21	9.3	$4,820	$55,080,226	$3,249,993
Fine	7	3.1	$4,000	$100,000	$30,142

Further analysis of the data showed that the average age of male offenders who were sentenced is 34.86 years, and 44.67 for female offenders. Since all of the known sentences involve incarceration, we also inquired about the length of incarceration by gender. On average, female criminals receive 12 months and males 94 months. We also compared the average prison length by country of origin of the offenders, grouped in regions that generally overlap with the different continents, except for Europe due to a clear distinction made in the literature between the offenders coming from Eastern Europe and Western Europe. As shown in Table 4, citizens of African countries received the lengthiest sentences – 409 months (with a median of 141 months). Prison sentences received by citizens of other areas were lower: Eastern Europe - 50 months, Asia - 48 months, North America (excluding U.S. citizens) - 45, Western Europe - 41 months, and South America - 38 months. Additionally, sentences for identity theft and fraud also reveal statistical significance when it comes to comparing them with other types of crime. While the average prison sentence for identity theft is 235 months, frauds it is 159 months,

whereas sentences for other types of crimes vary from 24 months for counterfeit goods to 76 months for theft of secrets. Small sample sizes warrant that these findings be interpreted with caution. Long sentences for a small group of offenders could skew the averages.

Table 4. Analyses of Prison Length by Gender, Age, Country of origin and Offense type

	Mean	*s.d.*	*t*	Range
Age by Gender (years)				
Male (N=56)	34.86	9.642		(22-73)
Female (N=3)	44.67	11.93		(31-53)
Prison length by Gender (months)				
Male (N=66)	93.55	214.745		(0.3-1380)
Female (N=5)	12.206	2.489		(9-16)
Prison Length by geographic region (months)				
Africa (N=8)	408.88	535.72	−5.53***	(51-1380)
Eastern Europe (N=18)	49.72	34.19	0.9	(8-135)
Asia (N=29)	48.22	41.48	1.34	(0.3-156)
North America (N=8)	44.75	39.68	0.62	(3-133)
Western Europe (N=4)	40.5	19.21	0.47	(12-54)
South America (N=4)	37.76	55.1	0.49	(3-120)
Prison Length by Offense Type (months)				
Hacking (N=21)	65.33	42.65	0.59	(12-156)
Fraud (N=29)	158.79	312.55	−2.48*	(12-1380)
Theft of Secrets (N=6)	76	32.55	0.14	(36-133)
Counterfeit goods (N=24)	24.43	22.84	1.87	(0.3 - 87)
Identity theft (N=16)	235.25	408.51	−3.47***	(16-1380)
Unauthorized access (N=12)	61.5	45.88	0.53	(16-180)
Phishing (N=2)	59	1.41	0.2	(58-60)
Spamming (N=3)	51	3	0.31	(48-54)
Online sales fraud (N=7)	38.86	25.54	0.65	(8-87)
Digital piracy (N=2)	36	33.94	0.36	(12-60)

*p≤.05, **p≤.01, ***p≤.001.

Note. Citizens of the U.S. are not included in the Northern American region because of the focus of this study, except for one case in which the offender acted as a spy on behalf of China. Also, crimes such as destruction of property, web defacement, and securities fraud are not included in the table because the sentencing in these cases either has not had occurred before the end of the data collection or the case in which it was known was only one.

Discussion

The findings from this study parallel many findings from past studies (Rogers, 2011; Rush et al., 2009; Hutchings, 2014; Fried, 2001; Warner, 2011; Marcum, Higgins & Tewksbury, 2011), while also providing new insight on the international patterns seemingly guiding cyber offending. For example, like other studies, this study showed that cyber offenders tend to be predominantly male, many of whom from countries that are political adversaries to the U.S. At the same time, differences regarding offender age, the inclusion of a high number of offenders from certain countries, group offending, and cybercrime types, shed some light on new ways to understand the international nature of cyber offending.

In terms of age, our findings show that the average age of cyber offenders is slightly higher than the average age established from previous studies. It is possible that our exclusion of U.S. citizens in this study increased the average age of the sample. When it comes to young international citizens, all of the obstacles standing in the way of prosecuting cybercrimes become even more complicated with

the presence of an individual who could be underage according to the jurisdiction of their country of origin. That could be a legitimate reason for why U.S. prosecutors are hesitant to pursue cases against young international cyber offenders. For instance, it is possible that an offender who is 18-years-old or under is from a country where the laws for juveniles are much lighter than the ones in the U.S. In this case, the jurisdictional issues and the resources allocated for resolving it could simply make the prosecutor unlikely to continue with the proceedings.

The results pertaining to the countries of origin of the cyber offenders also correspond to a large extent to the ones that previous studies suggested, except for one intriguing finding that this study underlines – that the number of Romanian cyber offenders exceeds the number of Russian ones. In a political context, China, Russia, and Iran are typically considered adversaries to the U.S., both in the physical and in the cyber domain. However, it appears that citizens of an Eastern-European country are represented much more than Russians who supposedly have political motivation to commit these criminal acts. While the numbers for Romania are surprising due to the fact that Washington does not have an antagonistic relationship with Bucharest, it is established in the literature that Eastern European countries are well known perpetrators of cybercrimes (Fried, 2001). Both Romania and Estonia are members of the European Union and NATO, so speculations about the nature of the cybercrimes as being politically triggered would be out of place. That said, since politically driven cyber-attacks could be excluded, a deeper analysis of the cultural and socio-economic conditions in these parts of Europe could probably explain why Eastern European citizens are among the most frequent perpetrators of cybercrimes, and particularly, specific types of cybercrimes for which they are prosecuted in the U.S.

The group dynamics of cyber offending uncovered in this study are consistent with prior research. According to our results, cybercriminals acting internationally are very often in collaboration with citizens of other countries. It is also common that different people in the organized cybercrime group execute different roles in the process of achieving the desired result. In cases of more elaborate schemes, it is possible that some of the participants do not even have specific interaction with devices but instead, facilitate the illicit actions of other members of the group. The former could involve offenders with knowledge in finance, economics, management, marketing and other fields. Academics and practitioners alike emphasize that cybercrimes increasingly include a broader scope, involving multiple countries and nationals of different states, and that they work increasingly in groups and not individually. Namely, the latter is an element that facilitates the execution of the cybercrime operation and creates various obstacles to the prosecution in terms of determining the physical location of the criminals, and the jurisdiction that should handle the case (Smith, Grabosky & Urbas, 2004).

Regarding crime types, the results show that fraud is the predominant cybercrime committed. This is interesting given that many cases of fraud are not reported by victims because of shame (Cross, 2015). The overrepresentation of fraud cases could be due to the fact that they are more likely to have identifiable victims, even if victims are often unlikely to report their experiences.

An additional finding that our study reveals pertains to the countries of origin of the offenders committing these crimes. While media attention focuses on frauds by individuals from African countries, it appears that they come predominantly from Eastern Europe, and more concretely from Russia, Romania, and Estonia. Similar conclusions can be drawn about hacking. Estonia and Romania are again the leading countries in this cybercrime category. All these results point to the question, what do these countries have in common and why are these cybercrimes so attractive to individuals coming from these countries – both questions that the literature should explore further considering cultural, political and socio-economic factors. When it comes to counterfeit goods and theft of secrets, however, we found that China is the leading country whose citizens commit the vast majority of these crimes –

a finding that also corresponds with previous studies. A large body of literature has been devoted to cyber schemes originating in some African countries. Our study confirms that mostly citizens of South Africa and Nigeria commit identity theft. In our sample, Ukraine is second in identity theft, sharing the same numbers with Nigeria. Previous studies frequently mention Eastern-European countries as places from where a large number of cybercrimes originate, especially fraud, and as our study showed, also hacking, unauthorized access and identity theft.

The results for the sentencing patterns of international citizens prosecuted in the U.S. also reveal some similarities with previous studies. The high number of prison sentences, for example, is consistent with prior research, though these findings show an even higher number than other studies do. In fact, all of the offenders in our sample with known sentences received a prison sentence. It is plausible that these sentences reflect a decision by prosecutors to focus on the most serious cases. In comparison to these results, statistics from the U.S. Department of Justice that include American citizens as well as internationals highlighted that 51.7% of sentenced cybercriminals received prison time (Marcum, Higgins and Tewksbury, 2012). The percentage of prison sentences in a non-U.S.-cybercriminals sample exceeded the one that included U.S. citizens by almost two-fold. This tendency could be attributed to various factors, among which, the fact that cybercrimes with international perpetrators are prosecuted only in certain cases with a high likelihood of resulting in a sentence. Another factor that could contribute to this explanation is that for U.S. citizens, the criminal justice system measures that could be imposed exceed the ones that could be successfully applied to international cybercriminals. For instance, probation in cases involving international cybercriminals could be inapplicable due to them being a high-level risk of flight beyond the U.S. border. Or, it simply could be that because our sample focused on press releases, less serious cases were excluded from our analysis. These tendencies in sentencing international cyber offenders should be further explored and analyzed by scholars.

The last set of findings in our study concerns the most commonly committed cyber offenses and from which countries these offenders are from. We found that the sentences of citizens from countries in Africa are significantly different than the ones given to criminals living in other geographic regions. These results should be revisited again considering some context: that identity theft is the fourth most frequently appearing offense in our sample, and that mostly individuals from South Africa and Nigeria are the perpetrators. That said, the sentences for identity theft are also statistically different than the sentences for other offenses, along with cyber fraud. Having in mind these circumstances, two questions logically follow: is identity theft and fraud judged more severely than other offenses, and are the perpetrators who happen to commit these crimes perceived as a higher-level threat than others and are thus sentenced to lengthier periods of incarceration? It is essential to identify whether the crime takes precedence in decisions about sentencing or the personality and some special characteristics of offenders. Future studies exclusively focusing on the factors that determine the sentences of cyber offenders are needed, especially in samples that include foreign citizens.

A few words about the limitations of this study also deserve attention. First, it includes a particular time-period (2009-2017) which was the only available information on the website of the U.S. Department of Justice. More than half of the cases that were included in our sample have not had yet concluded with a sentence. It is also possible that within this period, technological development, political tensions and cultural factors made some countries stand out more than others in regard to the number of cybercrime offenders. Furthermore, the average age and gender trends in cyber offending may have changed in comparison to previous years that are not included in the sample. Second, not only are there many cybercrimes that remained unreported, but even if reported, the prosecution may have decided not to continue with the legal proceedings due to the reasons highlighted by Smith,

Grabosky and Urbas (2004) that were enumerated previously in this essay. Third, because our sample included press releases, we are potentially excluding cases that prosecutors did not think were "newsworthy". What this suggests is that minor cases or less serious cases were excluded. Fourth, it is possible that some criminal acts look like they would constitute a particular crime but because the evidence on the case was not sufficient, the individual was indicted for another crime for which the evidence was sufficient.

An example of this final limitation would be a case involving theft of trade secrets for which the prosecution did not succeed in collecting evidence for espionage. Title 18, Section 1832 of the U.S. Code states that the only necessary element for a theft of trade secrets offense would be "that the thief be aware that the misappropriation will injure the secret's owner to the benefit of someone else" (Doyle, 2016, Summary section, para. 1). In order for an offense to qualify for an economic espionage, it is mandatory that "the thief intend to benefit a foreign government or one of its instrumentalities" (Doyle, 2016, Summary section, para. 1). In this case, intention may be the difficult aspect to prove. Moreover, there are some purely procedural issues that make prosecutors unlikely to pursue a case, such as the different institutions (the Department of Justice, for instance) that have to confirm that the case is most likely an economic espionage (Nasheri, 2012). Further evidence for this possibility is the very low number of indictments and sentences for economic espionage mainly conducted by Chinese nationals even though intelligence services suggest that other governments also frequently commit or attempt to commit economic espionage (Burstein, 2009).

Conclusion

This study explored the characteristics of international cyber offenders prosecuted in the U.S. To a large extent, the results from our study overlap with previous findings on the subject matter. The cyber offenders from our sample were predominantly male, as the literature suggests. Regardless, we would like to delineate some specifics that do not match previous results. First, the average age of international cyber offenders is somewhat higher than what the literature has established. Second, instead of observing major political adversaries of the U.S. as countries from which the most cyber offenders come from, Romania came in second place, after China, leaving Russia behind in the third place.

These findings create room for further discussion and empirical studies attempting to explain why Romanians are prosecuted, and allegedly commit cybercrimes, much more than Russians in the U.S. In terms of the most commonly observed type of cybercrime, cyber fraud has the highest number despite the pattern of underreporting and lack of attention by law enforcement that some studies suggest. Interestingly, sentences with the lengthiest prison time received were not citizens of Eastern Europe or Asia, but Africa. Lastly, the part of our study researching the U.S. criminal justice response to international cyber offenders showed that in all of the cases in which the sentence was known, it involved some prison time.

This conclusion is in full accordance with scholarship maintaining that in order for the prosecution to proceed with a case involving international citizens, there should not only be sufficient amount of evidence but also a reasonable expectation that the offender(s) will get a substantial sentence. Supplemental to this finding is also the fact that probation was not imposed as a sanction in any of the cases of the research sample. This could be attributed to the possibility that first, international citizens present a high international flight risk, and second, that the prison sentences imposed in all of the cases excluded the opportunity for probation. In terms of juxtaposing sentences of a larger sample of cyber offenders that include both domestic and international offenders, our study showed a much hig-

her likelihood of international citizens receiving prison time, as compared to the sample that includes U.S. citizens. Future empirical studies should focus on populations of international citizens prosecuted in other countries, so that results could be compared to the ones from our study.

References

Brenner, S. W. (2008). *Cyberthreats: The emerging fault lines of the nation state.* New York, NY: Oxford University Press.

Burstein, A. J. (2009). Trade secrecy as an instrument of national security rethinking the foundations of economic espionage. *Arizona State Law Journal,* 41(4), 933-990.

Chang, L. Y. (2013). Formal and informal modalities for policing cybercrime across the Taiwan Strait. *Policing and Society,* 23(4), 540-555.

Chang, Y. C. (2012). Combating cybercrime across the Taiwan Strait: investigation and prosecution issues. *Australian Journal of Forensic Sciences,* 44(1), 5-14.

Cheung, W. L., & Prendergast, G. (2006). Buyers' perceptions of pirated products in China. *Marketing Intelligence & Planning,* 24(5), 446-462.

Choo, K. K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. *Asian journal of criminology,* 3(1), 37-59.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology,* 21(2), 187-204.

Deibert, R. J., Rohozinski, R., Manchanda, A., Villeneuve, N., & Walton, G. M. F. (2009). *Tracking GhostNet: investigating a cyber espionage network.* Toronto, CA: Munk Centre for International Studies, University of Toronto.

Denning, D. E., & Baugh Jr, W. E. (1999). Hiding crimes in cyberspace. *Information, Communication & Society,* 2(3), 251-276.

Doyle, C. (2016). *Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act.* Congressional Research Service.

Fedushko, S., & Bardyn, N. (2013). Algorithm of the cyber criminals identification. *Global Journal of Engineering, Design & Technology (GJEDT),* 2(4), 56-62.

Fidler, D. P. (2013). Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies. *ASIL Insights,* 17(10).

Fried, R. (2001). Cyber scam artists: A new kind of con. *SANS Institute.* Retrieved from: https://www.sans.org/reading-room/whitepapers/threats/paper/482

Gistri, G., Romani, S., Pace, S., Gabrielli, V., & Grappi, S. (2009). Consumption practices of counterfeit luxury goods in the Italian context. *Journal of Brand Management,* 16(5-6), 364-374.

Grabosky, P. (2004). The global dimension of cybercrime. *Global Crime,* 6(1), 146-157.

Grabosky, P. (2007). Requirements of prosecution services to deal with cyber crime. *Crime, law and social change,* 47(4-5), 201-223.

Higgins, G. E. (2006). Gender differences in software piracy: The mediating roles of self-control theory and social learning theory. *Journal of Economic Crime Management,* 4(1), 1-30.

Hinduja, S. (2006). A critical examination of the digital music phenomenon. *Critical Criminology,* 14(4), 387-409.

Hinduja, S. (2008). Deindividuation and internet software piracy. *CyberPsychology & Behavior,* 11(4), 391-398.

Hinduja, S., & Higgins, G. E. (2011). Trends and patterns among music pirates. *Deviant Behavior,* 32(7), 563-588.

Hjortdal, M. (2011). China's use of cyber warfare: Espionage meets strategic deterrence. *Journal of Strategic Security,* 4(2), 1-23.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and unauthorized account access. *Security Journal,* 4(1), 2-12.

Holt, T. J. (2010). Examining the role of technology in the formation of deviant subcultures. *Social Science Computer Review,* 28(4), 466-481.

Holt, T. J., & Copes, H. (2010). Transferring subcultural knowledge on-line: Practices and beliefs of persistent digital pirates. *Deviant Behavior,* 31(7), 625-654.

Holt, T. J., & Kilger, M. (2012). Examining willingness to attack critical infrastructure online and offline. *Crime & Delinquency,* 58(5), 798-822.

Holt, T. J., Kilger, M., Chiang, L., & Yang, C. S. (2017). Exploring the correlates of individual willingness to engage in ideologically motivated cyberattacks. *Deviant Behavior,* 38(3), 356-373.

Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change,* 62(1), 1-20.

International Intellectual Property Association (2006). *International Intellectual Property Alliance 2006 Special 301 Report on Global Copyright Protection and Enforcement.* Retrieved January 3, 2019, from http://www.iipa.com/special301_TOCs/2006_SPEC301_TOC.html

Internet Crime Complaint Center (2017). *Internet Crime Report 2017.* Retrieved January 3, 2019, from https://www.ic3.gov/media/annualreport/2017_IC3Report.pdf

Katzenstein, P. J., & Okawara, N. (2002). Japan, Asian-Pacific security, and the case for analytical eclecticism. *International Security,* 26(3), 153-185.

Lau, L. (2018). *Cybercrime 'pandemic' may have cost the world $600 billion last year.* Retrieved January 2, 2019, from https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html.

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research,* 23(3), 287-300.

Marcum, C. D., Higgins, G. E., & Tewksbury, R. (2011). Doing Time for Cyber crime: An Examination of the Correlates of Sentence Length in the United States. *International Journal of Cyber Criminology,* 5(2), 825-835.

Marcum, C. D., Higgins, G. E., & Tewksbury, R. (2012). Incarceration or community placement: examining the sentences of cybercriminals. *Criminal Justice Studies,* 25(1), 33-40.

Nasheri, H. (2012). *The Challenge of Economic Espionage.* Retrieved January 3, 2019, from https://www.worldpoliticsreview.com/articles/12025/the-challenge-of-economic-espionage

Organization for Economic Co-operation and Development. (2007). *The Economic Impact of Counterfeiting and Piracy.* Paris: OECD Publications.

Rahim, M. M., Seyal, A. H., & Rahman, M. N. A. (1999). Software piracy among computing students: A Bruneian scenario. *Computers & Education,* 32(4), 301-321.

Rogers, M. K. (2011). The psyche of cybercriminals: A psycho-social perspective. In *Cybercrimes: A Multidisciplinary Analysis* (pp. 217-235). Springer Berlin Heidelberg.

Rush, H., Smith, C., Kraemer-Mbula, E., & Tang, P. (2009). *Crime online: Cybercrime and illegal innovation.* London: NESTA. Retrieved from: http://core.ac.uk/download/pdf/8223.pdf

Rutter, J., & Bryce, J. (2008). The Consumption of Counterfeit Goods: Here Be Pirates? *Sociology,* 42(6), 1146-1164.

Saroha, R. (2014). Profiling a cyber criminal. *International Journal of Information and Computation Technology,* 4(3), 253-258.

Sims, R. R., Cheng, H. K., & Teegen, H. (1996). Toward a profile of student software piraters. *Journal of Business Ethics,* 15(8), 839-849.

Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber Criminals on Trial.* Cambridge, UK: Cambridge University Press.

Solomon, S. L., & O'Brien, J. A. (1990). The effect of demographic factors on attitudes toward software piracy. *Journal of Computer Information Systems,* 30(3), 40-46.

Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review,* 23(1), 8-23.

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology,* 5(1), 736-749.

Williams, J. P., & Copes, H. (2005). "How edge are you?" Constructing authentic identities and subcultural boundaries in a straightedge internet forum. *Symbolic Interaction,* 28(1), 67-89.

Wood, W., & Glass, R. (1996). Sex as a determinant of software piracy. *Journal of Computer Information Systems,* 36(2), 37-43.

Yun, I., Kim, S., & Kwon, S. (2016). Low self-control among South Korean adolescents: A test of Gottfredon and Hirchi's generality hypothesis. *International Journal of Offender Therapy and Comparative Criminology,* 60(10), 1185-1208.