Cybercrimes in the Former Soviet Union and Central and Eastern Europe: Current Status and Key Drivers

By: Nir Kshetri

Kshetri, Nir (2013). "Cybercrimes in the Former Soviet Union and Central and Eastern Europe: Current Status and Key Drivers," *Crime, Law and Social Change*, 60(1), pp 39-65.

The final publication is available at http://link.springer.com/article/10.1007%2Fs10611-013-9431-4.

Abstract:

Some economies in the Former Soviet Union and Central and Eastern Europe (FSU&CEE) are known as cybercrime hotspots. FSU&CEE economies have shown complex and varied responses to cybercrimes due partly to the differential incentives and pressures they face. This study builds upon literatures on white-collar crime, institutional theory and international relations (IR)/international political economy (IPE) perspectives to examine the low rates of prosecution and conviction of suspected cybercriminals in some economies in the FSU&CEE and variation in such rates across these economies. The findings indicate that cybercrime cases are more likely to be prosecuted and sanctions are imposed in economies that are characterized by a higher degree of cooperation and integration with the West. Cybercriminals are less likely to be jurisdictionally shielded in such economies. Our findings also suggest that a high degree of cooperation and integration with the West would lead to access to resources to enhance system capacity and law enforcement performance to fight cybercrimes.

Keywords: cybercrime | former soviet union | eastern Europe | central Europe | cybercriminals

Article:

Introduction

Some economies in the Former Soviet Union and Central and Eastern Europe (FSU&CEE) have become top cybercrime hotspots. According to Merchant Risk Council, six of the top ten economies from which most online frauds originated in the early 2000s were from FSU&CEE [99]. An estimate suggested that, in 2004, there were over 50 gangs of professional cybercriminals in these economies [42].

Cybercrime rings in some FSU&CEE economies have mastered complex tricks. Sophisticated frauds involving a complex fusion of strategy, technology, processes, and people such as cyber-extortion, distributed denial-of-service (DDoS) attacks and hijacking users' searches and clicks are associated with these economies. Corruption, the lack of sufficiently high penalties, ineffective, inefficient, inadequate, and weak legislation and lax law enforcement have fueled cybercrime in these economies [57].

Key private sector players have also allegedly encouraged cybercrimes. For instance, ISPs in the region arguably have no vested interest in fighting spam as doing so would decrease their revenue [80]. According to the anti-spam organization, Spamhaus, the Russian domain name registrar NAUNET allegedly harbored cybercriminals (http://www.spamhaus.org/news/article/680/).

In response to FSU&CEE- originated cybercrimes, institutional changes are taking place in the West. The U.S. State Department, for instance, provides instruction and training to employees on security, especially securing devices in Russia and China [84].

Criminologists have emphasized the need to understand the causes and motivations of frauds against consumers against the backdrop of rapid growth in such frauds transcending international boundaries [47]. Prior researchers have also suggested that an understanding of the structure of opportunity associated with white-collar crimes would help take countermeasures to prevent such crimes [13]. This argument is equally valid for cybercrimes.

The salient feature of FSU&CEE economies, from our perspective, the rates at which suspected cybercriminals are investigated, apprehended, prosecuted, and convicted are low in these economies, as in most economies. Since cybercrimes in many aspects are similar to white-collar crimes, it is logical to draw upon the literature on white-collar offenses. Prior researchers have suggested three explanations that may account for the low rates of prosecutions and convictions and differential treatment of white-collar offenders: organizational advantage argument, alternative sanctions argument and system capacity argument [46,86,94,105]. This article attempts to examine these explanations and associated mechanisms in more detail in the context of cybercrime by drawing upon institutional theory and international relations (IR)/international political economy (IPE) perspectives.

The paper is structured as follows. We proceed by first examining relevant theories and concepts. Next, we analyze the nature, extent and impact of cybercrimes associated with the region. Then, we investigate the push and pull factors related to cybercrimes. It is followed by a section on case studies of some firms from the region engaged in cybercrimes. Following this is a section institutional and IR/IPE explanations regarding FSU&CEE economies' approaches to cyberspace. The final section provides discussion and implications.

Relevant theories and concepts

Differential treatment of white-collar offenders

As is the case of most emerging economies, rates of prosecution and conviction are low for cyber-offenders in many FSU&CEE economies. For instance, prosecutions related to cybercrime are vanishingly low at 5–6 people a year in Russia [106]. Likewise, according to the Interior Ministry of Ukraine, 400 people were arrested in the country for Internet and banking fraud charges during 2002–2011 but only eight were convicted [80]. While hard data are difficult to obtain, more internationally integrated CEE economies are expected to have higher prosecution and conviction rates. What factors explain the fact that, only a small proportion of cyber-offenders are prosecuted and most go unpunished in some FSU&CEE economies? What are the sources of regional variation in the prosecution and conviction rates of cyber-offenders?

The literatures on the white-collar crime could be particularly helpful for identifying important micro-level causes and dynamics associated with individuals' engagement in cybercrime activities. Based upon the related literature of white-collar offenders [46,86,94,105], three explanations can be offered regarding the differential treatment of cyber-offenders. According to an organizational advantage argument, offenders that are in "organizationally shielded" positions receive more lenient treatment. Hagan and Parker [46] analysis of securities fraud in Canada indicated that employers were less likely to be prosecuted under criminal statutes than were offenders in lower-class positions. The authors concluded that organizational structure of corporations embedded class advantage in such a way that employers were often shielded from prosecution.

According to an alternative sanctions argument, civil sanctions may replace criminal sanctions in the response to white-collar crimes. Shapiro [94] study of violators of securities law in the U.S indicated a higher tendency to prosecute lower-status offenders than higher-status ones. Her analysis, however, indicated that the variation in prosecutions and sanctions across different levels of status was due to the availability of alternative sanctions in cases involving higher-status offenders and was not because of a class bias.

Finally the system capacity argument maintains that the legal response to suspected crime is a function of organizational resources and caseload pressures [86]. Resource limitations are of particular concern for white-collar crimes due to their complexity, which require substantial amounts of investigative and prosecutorial efforts [105].

It is recognized, however, that the three explanations above provide complementary rather than mutually exclusive interpretation regarding the differential treatment of white-collar offenders. For instance, prior research indicates that the limited capacity of criminal justice agencies due to the complexity and hidden nature of white-collar crime and the system overload caused by such crimes reduces state capacity to respond to such crimes [12]. Likewise, due to the difficulty involved in obtaining direct evidence against high level criminals that are “organizationally shielded”, system capacity limitations may lead to prosecution of lower-level employees, for whom it is easier to locate the evidence [105].

Institutional and IR/ IPE perspectives

The institutional and IR/ IPE perspectives would help us understand the macro picture of cybercrime associated with FSU&CEE economies by providing further insights into low rates of prosecution and conviction for cyber-offenders in some of these economies, and variation in such rates. Prior researchers have recognized that economic activities and actors are embedded in formal and informal institutions [44,83]. The nature of activities of cybercriminals fits squarely with what Baumol [8] calls destructive entrepreneurship. Baumol hypothesized that the distribution of productive, unproductive, and destructive entrepreneurs is a function of the “relative payoffs” offered to these activities by the society’s “rules of the game”. These rules are referred as institutions [77].

In light of the cross-border nature of most serious cybercrime activities, it is also important to understand the importance of cyber-security issue from the IR/IPE perspective. A large body of literature indicates that with the decline of violent geopolitical conflicts, traditional issues such as nuclear war are losing salience and the focus and organizing principle in international relations have been on nontraditional security issues [3,25,110]. Cyber-threat is increasingly recognized as a legitimate security issue because cyber-attacks present threats to national security for the simple fact that most of the critical infrastructures are connected to the Internet [60,61]. This issue is also tightly linked to economic security of countries.

Assessing the nature, extent and impact of cybercrimes associated with the FSU&CEE

Cybercrimes originated in the FSU&CEE economies share two important characteristics. First, a significant proportion of them are linked with organized crimes [38], which is clearly demonstrated many large-scale entrepreneurial initiatives (see Cases 1–3 and Table 1). Cybercrime groups in FSU&CEE are well-known for efficient global teams and supply chain management, best adaptive global strategies, effective incentive structures and meaningful global collaborations [43]. For instance, IT security analysts observed that a large number of people are required to run the Rustock botnet (Table 1; [9]). More broadly, most economic and financial crimes in Russia and other former Soviet Union economies are associated with organized crime groups [62].

Table 1

Some examples of notable international cybercrime networks associated with the FSU&CEE economies

Malware/Crime gang	**Active in**	**Operations**	**Remarks**
Conficker	Last reported: 2010	Controlled 7 m computer systems at 230 regional and ccTLDs.	Bandwidth capacity: 28 tb/sec
Pushdo/Cutwail	2009–2010	100,000 bots (40 % in India), 30 C&C servers in Europe, North America, Russia	> 1.7 trillion e-mails in 15 months
Rustock	2006–Q12011	2.5 million computers (2010, peak), Operated from Russia	Peak: > 50 % of global spam
ShadowCrew (Clearinghouse for cards, document)	2004–2005	4,000 members in Bulgaria, Canada, Poland, Sweden, the U. S. and others, 1.7 million stolen card no., $4.3 million losses	Masterminds arrested in six countries including the U.S.
Zeus	Since 2007	1.6 million attacks (2010Q1) (15 % of malware attacks)	2011Q1: 44 % of all financial malware infections.
		Stole 70*million*(*attempted*220 million) by Sept. 2010 in the U.S., over $9 million in 3 months in the U.K.	Sept. 2010: arrests of 92 members in the U.S., 19 in the U.K., 5 in Ukraine.
		> 500 C&C servers in Russia, the U.S., Romania, and Ukraine.	
		Early 2010: botnet of 100,000 PCs.	
GhostMarket Forum	2009	8,000 members selling Zeus, manufacturing crystal meth and bomb-making.	Used a bank account in Costa Rica to process funds.
		Losses from credit details: £16.2 million.	
Mpack	2007	May 2007: compromised > 160,000 computers.	Mpack kit: sold for 700–1,000.
Coreflood	2002–2011	Controlled > 2.3 m PCs.	April, 2011: U.S. DoJ and FBI seized C&C servers.

Malware/Crime gang	**Active in**	**Operations**	**Remarks**
		Theft: > $100 million.	evolved with > 100 updates
		3/2009–1/2010: a C&C server held 190 GB of data from > 400,000 victim computers.	
Bredolab	May 2009– Oct. 2010	Infected 3 million PCs/month (controlled up to 29 million PCs).	An Armenian arrested.
		3.6 billion spam e-mails daily containing the malware	Dutch authorities seized 143 servers.
Innovative Marketing Ukraine (IMU)	2003–2009	> 600 employees in Kiev/ subsidiaries in India, Poland, Canada, U.S. and Argentina.	Incorporated in Belize, main offices in Kiev
		Sold programs in > two dozen countries, generated US$ 180 million (2008).	Credit card payments handler: Bank of Bahrain & Kuwait, Singapore’s DBS Bank.
			Call centers in Ukraine, India and the U.S.
Blackhole	Since 2011	Arguably the most commonly detected malware family in 2012H1	Believed to be developed by Russian hackers
Flashback	2012	Estimated to infect 550,000–600,000 Macs at its peak.	Believed to be created by the Russian gang which created the MacDefender malware in 2011 [32,78].
Rove Digital (Domain Name Server (DNS) changer)	2006–2011	Hijacked > 4 million computers in over 100 countries, generated > $14 million in profits. The group had 100 C&C servers worldwide including one each in New York and Chicago.	The gang included six Estonians and one Russian. Nov. 2011: dismantled by U.S. federal agencies. The two-year FBI investigation was codenamed “Operation Ghost Click”.

Second, unlike their counterparts in other parts of the world, cybercriminals in some FSU&CEE economies pursue business models that offer quick monetization. For instance, stolen financial information is more easily converted into cash than trade secrets [111]. Likewise, cyber-offenses involving the creation of fake profiles on social networking (SN) sites in some FSU economies have monetization aspects. In Armenia, for instance, criminals reportedly open SN accounts with the names of different people and use them to distribute pornography. They then extort money to eliminate such pages [76]. This is in contrast to the approaches followed by cyber-offenders in India and the Middle East, where fake SN profiles are often created to defame and malign the victim.

We consider two internationally known cybercrime hot spots: Russia and Ukraine.

Cybercrimes in Russia

According to some estimates 10,000–20,000 people in Russia work in "dark side" activities such as engaging in bank frauds, selling scareware and sending fake pharmacy spam [65]. Various aspects of cybercrime in Russia and their enforcement are fascinating, puzzling, controversial and complex. Russian hacking rings and organized crime networks have reportedly collaborated with criminals groups with other countries. For instance, Russian hacking rings allegedly helped Japanese gangs to attack law-enforcement agencies' databases [103] and worked with Australian scammers to transfer stolen money from overseas banks [40]. Malaysia's HeiTech Padu Berhad's director noted that Russian organized crime groups financially sponsored the country's cybercriminals [49]. An employee of an anti-virus company allegedly engaged in virus creation.

A number of recent high-profile cybercrimes are allegedly traced to Russia. For instance, in the widely publicized coreflood case, the U.S. Federal Bureau of Investigation (FBI) and Department of Justice (DoJ) filed a civil complaint against 13 "John Doe defendants", believed to be in Russia. The Koobface malware, which started in 2008 by sending fake messages on Facebook and other SN sites reportedly originated in Russia. The infected machines were flooded with ads for gray products such as fake antivirus software. Victims' searches were also "hijacked" to deliver traffic to rouge websites [111].

Cybercrimes in Ukraine

Some analysts maintain that Ukraine is ahead of Russia in cybercrime ([80], quoting Trend Micro's Paul Ferguson). Some Ukrainian elites have publicly admitted that the country's cybercriminals have been threats to the world. Valentyn Petrov, an official at the Security Service of Ukraine (Sluzhba Bezpeky Ukrayiny, or SBU) noted: "Ukrainian hackers are well-known in the world. Our country is a potential source of cyber threats to other countries" [80].

A notable example is the Zeus malware, which likely originated from the country (Table 1). In 2010, the FBI’s cybercrime operations, code-named Trident Breach, broke up an international ring using Zeus, which stole US$ 70 million from the payroll accounts of small businesses and local government in the U.S. More than half of the sum reportedly went to Ukraine [80]. There were arrests in four countries, including 39 in the U.S. Most individuals detained were international students who acted as mules.

Western targets

Cyber gangs traced to FSU&CEE have allegedly stolen substantial amount of money from Western businesses and consumers. According to the Romanian police, over 80 % of online frauds originating from Romania targets U.S. consumers and businesses. One estimate suggests that U.S. consumers and businesses lose about US$ 1 billion to Romania-based cybercriminals.

Criminal syndicates in FSU&CEE have mastered several ways of defrauding banks. U.S. banks are estimated to lose US$ 1 billion a year [33]. A study of the Federal Deposit Insurance Corporation indicated that cybercrimes associated with FSU&CEE cost U.S. companies and their banks over US$ 15 billion during 2002–11 [72]. As an example, in 2009, the Michigan-based Experi-Metal lost US$ 1.9 million from bank accounts. Cybercriminals transferred funds to Russia, Estonia and other countries in 93 payments [72]. In December 2011, a Ukrainian general, a Moldavian and an Israeli were arrested in Romania for allegedly stealing banking credentials of at least two organizations and laundering funds to fake companies. They stole US$ 1 million from Minneapolis-based Society of Corporate Compliance and Ethics [56].

Predatory groups in foreign markets

International cybercriminals’ greatest vulnerabilities arguably lie in obtaining the crime proceeds such as extortion ransom money or stolen funds [5]. One way to increase portability of crime proceeds would be to establish what McDougal [69] refers as “a predatory group” in foreign markets.

Beginning the late 2008, the creators of Zeus reportedly employed an estimated 3,000 money mules in the U.S., the U.K. and other economies. They stole banking credentials and moved money from the compromised accounts into hundreds of accounts opened under false identities. Many of the mules were U.S. residents recruited through social networking sites, newspapers and other channels, who were lured into work-at-home jobs [90]. The stolen funds were often transferred using money transfer agencies such as Western Union.

The New York-based gang was operated by a Russian citizen who supplied the mules with fake identity documents, and managed their activities. The gang allegedly cleared over US$ 3 million from victim corporations [55]. In September 2010, the U.S. attorney’s office in New York charged 37 defendants. Four of the defendants were “managers” of the operation, “a few others” were recruiters, and the rest were money mules [45]. Some of them had come to the U.S. solely to engage in frauds.

British police also arrested 20 people for using Zeus and 13 of them were jailed in October 2011. Two Ukrainians were major players, who allegedly stole US$ 4.5 million in 6 months. The main kingpin operated from Ukraine, who acquired stolen credentials and coordinated the theft. The “man on the ground” was in the U.K. [28].

Similarly, most of Romanian cybercriminals’ auction fraud victims are in the Western countries. In 2006, U.S. law-enforcement agencies arrested an eBay fraud ring in Chicago, which was traced to have connections with cybercriminals in Pitesti, Romania [112].

The operations of the money mules may warrant elaboration. Some transactions involve mules in multiple countries. In a case reported in Sullivan [100], an online CD and DVD retailer paid a ransom of US$ 40,000 to a hacker based in Balakov, Russia. The fund was wired to 10 accounts in Latvia. The mules then rewired the money to St. Petersburg and Moscow. Another set of mules brought the money to Balakov. The computer server used to launch the attacks was in Houston.

The push and pull factors related to cybercrimes

Since prior researchers have emphasized the needs for exploration of causes and motivations of consumer frauds [47] and the structure of opportunity associated with various crimes [13], in this section, we seek to find answers to the following questions in the context of cyber-frauds associated with FSU&CEE: What are the push and pull factors for individuals engaged in the cybercrime industry in the region? Among the important pull factors that encourage individuals to engage in cybercrimes, it is important to understand the region’s endowment in IT skills and existing criminal networks. Push factors which motivate going outside the formal economy include a small and under-developed IT industry.

Criminal networks expanding to the online world

Organized cybercrime groups in FSU&CEE are able to benefit from criminal activity due to their endowment with superior criminal skills. As evident in cyber-extortion cases, such skills are transferable to the cyber-world. Many cybercrime victims are extorted by these groups. In the late 2003 and early 2004, the FBI and National Hi-Tech Crime units discovered that hackers employed by FSU&CEE organized crime groups launched a DOS attack on Worldpay System that affected thousands of online casinos. For instance, in 2004, online sports books, BETWWTS, reportedly paid East Europe-based extortionists thousands of dollars [107]. They carefully plan attacks in terms of the target, the time, and the amount of extortion. They often demand much less than the costs to repair a hacked site. Many firms choose to comply with their demand rather than taking the risk of attack and losing customers and profits.

Cybercrime firms in these economies combine a sophisticated mix of technical and social engineering competencies. For instance, it is reported that, Romanian scammers have hired English speakers to improve communications, which helped them appear legitimate [36]. Problems such as broken English, typos, grammar, misspellings and wrong tenses that made phishing emails less convincing are no longer a problem. Davis and Joan [27] observes: “In Eastern Europe and especially in the former Soviet republics, organized criminal groups are perfecting phishing with breathtaking speed. Not only have the pitches become more convincing (the spelling and grammatical errors that belied early phishing e-mails are less frequent, for instance), but the technology used to trap your account numbers and passwords has grown viciously sophisticated”. Rock Phish, which was believed to be a Russian group, was estimated to be responsible for over half of all phishing sites worldwide sent convincing messages in perfect English as well as French, German and Dutch [39]. It used counterfeit designs of brand logos and styles of financial companies, retailers, and government agencies [22].

In many FSU&CEE economies, crime seems to pay because the benefits often far outweigh the costs. It was reported that in the post-Soviet years of the 1990s, many top athletes joined the organized crime industry after retirement [80]. Former law enforcement agents are also allegedly engaged in organized crimes. After the fall of the communism, Bulgaria’s secret service agents were accused of being engaged in organized crimes [21]. Russian hack rings are allegedly operated by former KGB agents [11]. Russian organized crime groups arguably include “underworld” criminals as well as “overworld” figures from the former Communist Party [82].

IT skills

Students in FSU&CEE are good at mathematics, physics, and computer science. Consider the U.S. National Security Agency-backed “hacking” competition of 2009. Four thousand two hundred programmers from all over the world participated in algorithm coding and other contests. Of the finalists, ten were from Russia, and two were from the U.S. [23]. Speaking of the emphasis on mathematics in Romania, a scientist in Bucharest put the issue this way: “The respect for math is inside every family, even simple families, who are very proud to say their children are good at mathematics” [112].

High school students with computer literacy reportedly engage in seemingly harmless activities such as cracking a licensed program or breaking into SN accounts of classmates [106]. In many cases, these activities provide the foot-into-the- door to financially motivated cybercrimes.

In the FSU economies, computer specialists gained experience in “disassembling, examining and hacking American systems to see how they worked in order to make them functional on Soviet systems” [93]. Hackers in FSU economies arguably possess capability to do sophisticated attacks with limited resources. Observers have noted that Russian hackers are highly skilled and “subtle” [104] and know how to “get in and out without a trace” [107]. Specialized training schools reportedly teach hacking skills. Eighty-two percent of respondents participating in a worldwide poll indicated that Russia had the world’s best computer hackers. The corresponding proportion was 5 % for the U.S. [107].

Lack of legitimate jobs

FSU&CEE economies are too small to absorb the existing talent, which has forced educated workforce to the electronic underground. They lack an equivalent of the U.S. Silicon Valley. Beyond all that, a 1998 financial crash left many programmers unemployed [93]. A lack of English language proficiency limits access to the Western labor market [80].

In Russia and other FSU&CEE economies, top university graduate are reportedly paid by organized crime groups up to ten times as much as from legitimate jobs [24,108]. A self-described hacker from Moscow confessed: “Hacking is one of the few good jobs left here” [107]. Regarding computer attacks originating from Romania, the U.S.-based Internet Fraud Complaint Center noted: “Frustrated with the employment possibilities offered in Romania, some of the world’s most talented computer students are exploiting their talents online.”

Some with employment in legitimate companies have also found attractive to join the cybercrime industry. In January 2012, Microsoft announced that a former employee of an antivirus software firm was allegedly involved in writing or creating the Kelihos botnet [10]. At one point, the Kelihos botnet infected 41,000 computers worldwide and sent 3.8 billion spam e-mails a day [75]. Likewise, analysts suspected that hackers in Ukraine worked with top ISPs [80].

High likelihood of getting away with cybercrimes

As is the case of white-collar crimes [105], cybercrimes are complex and require substantial amounts of investigative and prosecutorial efforts. Resource limitations are thus of particular concern for cybercrimes. In Russia, for instance, most hackers are young, highly educated, and work independently and thus do not fit the conventional Police profiles of criminals [58].

Many FSU&CEE economies lack law enforcement agencies with high-tech crime-fighting abilities, which have led to cybercriminals’ high likelihood of getting away with cybercrimes. For instance, consider Ramnicu Valcea town of Romania, where a large number of eBay fraud cases originate. At one point in 2005, two law-enforcement officers in the town were dealing with over 200 eBay cases with a 9-year-old computer with no Internet connection. To go online, they used the cafes that were used by cybercriminals [112]. Likewise, eBay’s Albena Spasova, who worked in promoting law reform in Moldova and Bulgaria, was quoted as saying: “Even in 2001, I was meeting judges who thought cyber-crime was someone stealing a computer” [112].

Government agencies are also characterized by an apparent lack of ability to defend themselves cyber-attacks. There is a lack of knowledgeable computer experts in law enforcement agencies. When the popular Ukrainian file-sharing website, EX.ua was shut down in February 2012 on alleged piracy issues, governmental websites, including SBU’s web portal experienced cyber-attacks [80].

Observers note that since Russian cybercriminals mostly target banks and institutions in the West rather than in Russia, it is less of a concern for local law enforcement. To take an example, while Russia has strict laws controlling the media, Hacker Magazine published an article in August 2010, which explained how to crack the NATO website, with screenshots and step-by-step instructions [96].

Case studies of FSU&CEE-based cybercrime firms

Case 1: rove digital

An example of a highly globalized cybercrime firm is Tartu, Estonia-based Rove Digital (RD), which was seemingly legitimate IT Company. According to a Manhattan federal court indictment in November 2011, an alleged international crime ring associated with RD used malware to hijack more than 4 million computers in over 100 countries. When victims visited certain websites or downloaded software to view videos online, the malware was installed on the computers [17].

It was one of the biggest criminal-owned botnets. The ring included six Estonians and one Russian and was estimated to generate at least US$ 14 million in profits. About 500,000 of the hijacked computers were in the U.S. including those used by educational institutions, nonprofit organizations and government agencies such as NASA. The malware had infected the websites of about half of the Fortune 500 companies and at least 26 U.S. government agencies [7]. According to Media reports, Vladimir Tshastsin, the alleged ringleader transferred some of his assets to his father, who was Estonia’s 283rd richest person [6]. The law-enforcement operations in 2011 also led to a seizure of the gang’s 150 properties.

RD and shell companies

The crime ring was organized and operated as a traditional business but profited illegally. Its subsidiaries included Esthost, a webhosting services reseller, Estdomains, Cernel, and UkrTelegroup and many less well known shell companies. RD and its shell companies had faced legal problems and received media attention earlier. For instance, Esthost went offline, when the San Francisco-based Atrivo, which hosted Esthost's servers, was suspected to engage in criminal activities. RD was forced to stop the hosting services offered by Esthost [35].RD learned its lesson. The company expanded its command-and-control (C&C) infrastructure all over the world. It also moved a significant proportion of the servers from Atrivo to Pilosoft datacenter in New York [35].

In 2008, Estdomains also lost its accreditation from the Internet Corporation for Assigned Names and Numbers (ICANN) as its owner; Tsastsin was convicted in Estonia. Tsastsin was charged by an Estonian court for online fraud, money laundering and forging of documentation [6]. Despite RD's heavy involvement in cybercrimes, the company operated openly for many years.

The fraud scheme

RD's click hijacking scheme started in 2007 and ran until November 2011. The group had 100 C&C servers worldwide including one each in New York and Chicago [92]. The ring also claimed that it ran legitimate online advertising firms and the schemes principally operated through RD.

The "click hijacking" malware changed Domain Name Server (DNS) system and users of infected computers were given an incorrect address and unknowingly redirected to rogue computer servers controlled by the gang [48]. A simple way to understand the DNS system would be to view it as the Internet's "built-in phone book". Note that in order to find a website such as Google, Yahoo or Wikipedia, a computer reaches out to the DNS to find a numerical address also known as the IP address. The malware also prevented victims from connecting with their antivirus software providers and updating software.

Most traditional malware is designed to steal valuable personal information. This scheme was different and thus was not easily detected for a long time. Experts considered this as a very clever tactic as it manipulated the infrastructure of the Web involved in doing one of the most popular activities: display advertising [92]. Part of the problem also lies in the fact that some legitimate companies benefit from such frauds.

The indictment describes several examples of cyber-frauds including two principle strategies: traffic redirection and ad replacement:

Traffic redirection

The virus altered search engine results so consumers who clicked links of companies such as Apple's iTunes, Netflix, IRS.gov, www.ESPN.com, Amazon, www.WSJ.com and other popular websites would be directed to fake sites designated by them. When a user searched a term, the search results would normally return a website but the malware would force a redirect to a different website when the user clicked on the link. The indictment cited an example in which when a user searched for the "IRS" at www.Yahoo.com and clicked on a link for the Internal Revenue Service, the user was redirected to an H&R Block tax preparation website. Likewise, in searching "itunes," the results would display the official website but would take the user to a different website purporting to sell Apple software but not affiliated with Apple. Users were similarly rerouted to unaffiliated sites when searching for the official websites of Netflix and other companies, according to the indictment.

Users were also redirected to websites dealing with illegal and extra-legal products and services, such as those selling fake Louis Vuitton, replica watches and fake anti-virus software. The sites to which users were directed would pay a referral fee.

Ad replacement

When an infected computer was used to visit a website, the malware would replace regular ads with other ads from which the criminals would generate revenue through affiliate arrangements [31]. They also designed mimicked sites, which are doctored websites of legitimate organizations for replacing ads controlled by the hackers. The indictment cited an example: when users clicked on an American Express ad for the Plum Card on the Wall Street Journal's home page, it was instantly replaced by an ad for "Fashion Girl LA" [48]. Likewise, the group swapped legitimate display ads of Dr. Pepper on www.ESPN.com by a vacation timeshare ad [71]. In addition, clicking on these ads would often download malware to the user's computer.

Operation ghost click

In November 2011, the scheme was dismantled by U.S. federal agencies with the help of private companies and some universities. The two-year FBI investigation was codenamed "Operation Ghost Click". Two data centers in New York City and Chicago were raided by federal agents, who seized servers and IP addresses used in the DNS Changer malware and shut down more than 100 servers [48].

The FBI worked closely with the Estonian Police and Border Guard, the Dutch National Police, and NASA's Office of the Inspector General. Trend Micro tracked the activities of RD and its subsidiaries and helped the FBI. University of Alabama at Birmingham's (UAB) Spam Data Mine, which contained 550 million junk e-mail messages in its database as of November 2011, was used to analyze activities such as targeted versions of phishing (spear phishing), advertising fraud, and identity spoofing [70]. Other organizations helping in the operations included Georgia Tech University, the Internet Systems Consortium, security firm Mandiant, Spamhaus, Team Cymru and the DNS Changer Working Group. In February 2012, an Estonian court ruled that Estonia can extradite four persons to the U.S. The court had made similar decisions on two other persons [7].

Case 2: innovative marketing Ukraine (IMU)

IMU was a pioneer of fake antivirus software, also known as scareware, founded by a Swedish, a Canadian and an American. IMU exhibited many features of a legitimate company. The organization and its employees had LinkedIn profiles [81]. It was incorporated in Belize and its main offices were located in Ukraine's capital, Kiev. McAfee's Dirk Kollberg estimated that IMU employed more than 600 employees in Kiev and subsidiaries in India, Poland, Canada, the U.S., Argentina and other countries in posts such as receptionists, financial managers, webmasters and R&D engineers [81]. Paget [81] found 396 employees' names, analyzed the professional records of 180 of them. 100 of them worked for at least a year. Most were college students [37].

Business models of scareware programs are centered on infusing fear and anxiety to sell fake software. A typical scareware would pretend to scan a computer for malware, and would tell the user that the machine is infected. In IMU's case, the goal is to persuade the victim to voluntarily provide credit card information to pay US$ 50–80 for the scareware.

Scareware has become one of the fastest-growing, and most prevalent, types of internet fraud [37]. According McAfee there was a 400 % increase in scareware incidents in 2009. The company predicted that scareware would infect about 1 million computers a day in 2010 generating illegal global profits of over US$ 300 million [67]. According to Symantec, there were 250 varieties scareware products in 2009, which were installed in tens of millions of computers [87].

The modus operandi

IMU's products were superficially similar to genuine anti-virus products. For instance, its Win Antivirus looked like Microsoft security software. Another product, DriveCleaner, identified 179 visits to adult websites no matter which computer it was installed on. The fake software was designed to tell users that their PCs were working properly once they had paid. IMU relied fear and intimidation to assure compliance rather than product sophistication.

IMU invested heavily in call center facilities in Ukraine, India and the U.S., which responded to about 2 million calls in 2008 [41]. When people made calls to complain, agents would ‘guide’ them through the steps needed to make those messages appear [37]. In many cases, that also required disabling legitimate anti-virus software. A McAfee researcher listened to digitized audio recordings of customer service calls that IMU kept on its servers at the Ukraine offices. The researcher found that most customers seemed to be happy and satisfied at the end of the call [37].

IMU hired many young employees, who did not seem to care about ethical behaviors, practices and standards. They knowingly refused to acknowledge the scareware’s harm to consumers. A former IMU employee, who later joined a Kiev bank, put the issue this way: “When you are just 20, you don’t think a lot about ethics. I had a good salary and I know that most employees also had pretty good salaries” [37].

According to a McAfee researcher, IMU received approximately 4.5 million orders in the 11 months of 2008, which amounted to US180millionattherateofUS 40 each. IMU sold programs in at least two dozen countries [37].

IMU also created dummy ad agencies to place bogus and innocent-looking ads for reputed businesses without their permission on popular websites. Ads for businesses were placed on the websites of National Hockey League, The Economist, Major League Baseball, Priceline, Career Builder, the National Association of Realtors, E-Harmony and others [67]. A click on such ads triggered automatic bogus scans, which showed that the PCs were virus-infected. The PCs made sales pitch involving false promises for a clean-up and directed users to purchase IMU’s scareware [1].

IMU’s affiliates and business partners

In an attempt to ‘recruit’ business partners (e.g., credit card processors), IMU created subsidiaries, which were designed to hide its identity. A high proportion of IMU’s victims complained to their credit card companies to obtain refunds on purchases, which deteriorated the relationships with merchant banks that processed the transactions. IMU was forced to switch from a bank in Canada to one in Bahrain.

In 2005, the Bahrain-based Bank of Bahrain & Kuwait terminated ties with an IMU subsidiary. Then IMU had no credit card processor for 5 months. Following that it established a relationship with Singapore’s DBS Bank, which showed willingness to handle IMU accounts. DBS Bank processed IMU’s tens of millions of dollars in backlogged payments [37].

For infecting each machine, IMU paid affiliates 10 cents and generated average returns in the range of US$ 2–5 through software sale and product promotion. Affiliates loaded software by hijacking legitimate websites, setting up corrupt sites for spreading viruses, attacking social networking sites and other methods. One affiliate recruiting site, www.earning4u.com, reportedly paid US$ 6–180 for every 1,000 infected PCs [37].

IMU and its affiliates also rewarded the top performers. Panda Security reported that it found pictures of a party organized in March 2008 in Montenegro by KlikVIP, an IMU affiliate, to reward scareware installers. One picture showed a briefcase full of euros given to the top performer [37].

The fallout

More than 1,000 people complained against IMU to the U.S. Federal Trade Commission (FTC) [41]. The FTC's investigation lasted more than a year, which led to a federal lawsuit to shut down IMU. Reportedly IMU's servers were not password-protected. McAfee's Kollberg collected more than 67 GB of data from IMU servers [81]. Kollberg forwarded the information to the FTC and the FBI, which helped build the case against IMU.

According to a May 2010 announcement by the U.S. Attorney's Office, the three people charged in the IMU case allegedly cheated customers in 60 countries with about US$ 100 million [74]. The U.S. government retrieved US$ 117,000 by settling charges against one of the defendants, who ran a customer support center in Cincinnati [37]. Profiles posted on LinkedIn indicated that some of the former IMU employees were working at leading banks, consulting companies and other Kiev-based antivirus companies [81].

Case 3: Russian business network (RBN)

RBN allegedly offered spyware, Trojans, and botnet command and control systems and also laundered money [108]. The virus creation tool Mpack was its flagship product, which was designed to extract data from infected PCs. It was packaged with personal tech support from RBN and cost US$ 500–1,000. Mpack exploited known software security holes in browsers [54].

Cybercriminals hacked websites and installed malicious programs created with Mpack. When someone visited such sites with a browser unequipped with software security updates, a password-stealing program was installed on the visitor's computers. It then scanned the computer for vulnerabilities [50]. The stolen data were forwarded to a "drop site" in RBN servers. Mpack monitored the success of its operation through various metrics on its online, password protected control, and management consoles [102].

RBN also sold website hosting services to criminals. Krebs [54] quoted an analyst with the anti-virus firm, Kaspersky Lab: "They make money on the services they provide . . . the illegal activities are all carried out by groups that buy hosting services . . . .RBN, . . . does not violate the law. From a legal point of view, they are clean."

Observers noted that RBN seemingly had a political protections [108]. According to the Serious Organized Crime Agency (SOCA), RBN allegedly bribed local police, judges, and government officials [66]. An Economist.com article [29] noted:

Despite the attention it is receiving from Western law enforcement agencies, RBN is not on the run. Its users are becoming more sophisticated, moving for example from simple phishing (using fake e-mails) to malware known as "trojans" that sit inside a victim's computer collecting passwords and other sensitive information and sending them to their criminal masters.

RBN stopped operations in 2007. Some analysts suspected that "whatever protection RBN enjoyed was withdrawn because the group had overreached itself" [30]. It was also suggested that the group operating RBN may have shifted its operations to Asian countries [15].

Understanding FSU&CEE Economies' approaches to cybercrime and cyber-security: institutional and IR/IPE explanations

The low prosecution and conviction rates of cyber-offenders in some FSU&CEE economies and regional variation in such rates can largely be explained by two different but interrelated phenomena: modernization of legislative and institutional frameworks and cooperation and integration with the West. As presented in Table 2, FSU&CEE economies differ in their membership status in various supranational organizations, which partly explains their varying response to cybercrimes.

Table 2

Membership status of FSU&CEE economies in various supranational organizations

Supranational organizations	**Member countries**
Shanghai Cooperation Organization (SCO)	Kazakhstan, Kyrgyzstan, Russia Tajikistan, Uzbekistan
OECD	Czech Republic, Estonia, Hungary, Poland, Slovak Republic, Slovenia
EU	Bulgaria, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovak Republic, Slovenia

Supranational organizations	**Member countries**
NATO	Albania, Bulgaria, Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovak Republic, Slovenia
Signatories in the Council of Europe Convention on Cybercrime	Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Georgia, Hungary, Latvia, Lithuania, Moldova, Montenegro, Poland, Romania, Serbia , Slovak Republic, Slovenia, The former Yugoslav Republic of Macedonia, Ukraine

As Table 3 indicates, the degree of integration with the West contributes to but does not fully explain the modernization of broader institutional frameworks. This can be illustrated by comparing Russia and Ukraine. While Russia has established distance with the West, Ukraine has shown more willingness to cooperate and integrate (Table 3). The Council of Europe Convention on Cybercrime (CoECoC) has been ratified by Ukraine. Since 2009, the FBI has stationed a special agent at the U.S. Embassy in Kiev for assisting cybercrime investigation [51]. The Ukrainian law enforcement agencies have also cooperated with the West. In 2010, the SBU arrested five alleged kingpins of a criminal group, which stole US$ 70 million from U.S. bank accounts [80]. Likewise, formal NATO-Ukraine relations started in 1997 with the Charter on a Distinctive Partnership and establishment of the NATO-Ukraine Commission (NUC). Ukraine is also showing interest in, and enthusiasm for a deeper European integration.

Table 3

A comparison of FSU&CEE economies in terms of the modernization of institutional frameworks and integration with the West

Degree of modernization of broader legislative and institutional frameworks ⟹	**High**	**Low**
Willingness to cooperate and integrate with the West ⇓		
High	OECD and/or EU members (e.g., Estonia, Romania)	Ukraine
Low	No example among the economies studied in this paper	SCO economies

Despite the progress, some argue that Ukraine is slipping into reverse gear in democracy related matters due to the institutional inertia [18]. President Viktor Yanukovych's current government is not seeking NATO membership. Critics also argue that Yanukovych's government has done little to further European integration. Despite international cooperation, crime fighting efforts are hindered by underdeveloped and outdated institutional framework. For instance, the five kingpins detained in 2010 were freed immediately without a court trial. It is also argued that foreigners also account for international cybercrimes originated from Ukraine [95]. Corruption has enabled and generally encouraged them to obtain the right to reside and operate criminal activities in the country. The IMU case provides evidence to support this hypothesis.

Just like the white-collar cases [105], cybercrime cases are complex and thus require substantial resources to investigate and prosecute. Using the system capacity argument, while most white-collar crimes have a substantial cost to the local economy and thus their low indictment rates due to limited resources are unjustifiable [105], this may not be the case for cybercrimes associated with FSU&CEE. This is because most cybercrimes associated with these economies target international victims and cost little to the local economy. Likewise, while caseload pressure is obviously a concern [86], it is evident that the lack of incentives and interest in fighting cybercrimes originated from the region has become a more serious issue.

As noted above, resource limitations are of particular concern for investigating and prosecuting cybercrimes due to their complexity [105]. However, a significant proportion of cybercrime activities originated from the FSU&CEE harm the West. According to leaked WikiLeaks documents, U.S. diplomatic cables shed light on the cybercrime industry in Bulgaria, which is arguably one of the "growth areas" of criminal activities with a potential to have an impact on the U.S. if political and legal institutions fail to take effective countermeasures. This indicates the importance of cyber-security in IR/IPE as suggested by prior research [60,61]. The West is also in a position to expend more resources to investigate cybercrimes and has a vested interest in helping FSU&CEE increase system capacity and legal response.

Formal institutions

At the outset it must be noted that, many FSU&CEE economies have enacted laws and regulations to enhance cyber-security and there have been some indicators of enforcement success. In an attempt to control spam, Russia introduced regulations to tighten up domain registrations in 2010. The new regulations require copies of passports or legal registration papers for businesses to register a .ru domain. Before this regulation came into effect, domains were set up without any checks [65]. Similarly, the Romanian Directorate for Investigating Organized Crime and Terrorism (DIICOT) reported that it investigated 1,157 cybercrime cases in 2010. Likewise, in March 2012, Ukraine shut down the website of VX Heavens, a forum operating for a long-time to exchange tips on writing malware [51].

Despite the progress, unclear, outdated or impractical regulatory frameworks pose significant challenges. In Russia and Ukraine, it is unconstitutional to extradite their citizens to other countries [79]. Some countries' laws fail to account for the realities of cybercrimes. For instance, Romanian law requires cybercrime victims to send police a signed complaint and be represented at the hearing [112]. It is thus impractical for foreign victims to bring a case in the Romanian courts. Some government officials have publicly recognized the need for modernization of the Soviet-era legislation and institutional structure.

A piecemeal and fragmented approach to law enforcement is also reflected in cyber-security. The Interior Ministry's Directorate K is the lead agency to deal with cyber-security. The lack of cooperation and turf wars between the Directorate K and local agencies are clearly visible [109].

There was also an accusation that Russian cybercriminals have been co-opted by the intelligence agencies. The intelligence agencies allegedly use criminals' expertise or their networks of virus-infected computers for political purposes [53]. Many believe that whoever opposes the government and supports the opposition faces cyber-attacks. Russian websites that are related to organizations with anti-government positions have been victims of DDoS attacks. A 2002 attack on Kavkaz.org, the website of Chechen separatist fighters, was among the first indications of such approach, in which students of the Tomsk city were reportedly involved. The local department of the Federal Security Service was apparently aware of the perpetrators, which issued a press release describing the attack as an "expression of their position as citizens, one worthy of respect" [97]. Since then the so called "hacker patriots" have allegedly launched DDoS attacks against independent media sources in Russia as well as at government agencies in Estonia, Georgia, and Lithuania [97].

Informal institutions

North [77] noted that "although formal rules may change overnight as the result of political and judicial decisions, informal constraints embodied in customs, traditions, and codes of conduct are much more impervious to deliberate policies". Cultural acceptability of hacking also deserves mention [85]. Many economies in the region have no negative connotation of activities such as hacking and piracy. Actually, the opposite holds. Blau [16] documented how a Russian hacker-turned-teacher and his friends hacked programs and distributed them for free during their childhood: "It was like our donation to society, it was a form of honor; [we were] like Robin Hood bringing programs to people.

Russian elites feel some degree of sympathy for the cybercriminals. Dmitry Zakharov, director of Communications at The Russian Association of Electronic Communications (RAEC) noted: "The problems at the moment is that we are not able to offer talented technology people jobs so they get involved in illegal activity. Not many want to be gangsters but Russia is relatively young as a capitalist economy and there are not enough normal and civilised occupations" [65].

Russian cybercriminals thus also enjoy a degree of informal legitimacy. Experts also say that programs to raise awareness and educate the youth are largely missing [26].

Variation across FSU&CEE economies in cooperation and integration with the west

For some FSU&CEE economies, international pressures have led to the modernization of Soviet–era legislative framework and institutional structures. Economies such as Estonia, Hungary, Poland, Slovak Republic and Slovenia were constantly monitored as part of the process of attaining memberships of international organizations such as the EU, NATO and the OECD. The governments in these economies are becoming more effective in fighting crimes thanks to broader institutional changes such as Slovenia's establishment of a coordinating anti-corruption commission and specialized law enforcement units to combat serious economic crimes and Estonia's principles of "Honest State" program started in 2004, which has a number of components to reduce corruptions.

A related point is that these international organizations have well developed mechanisms and infrastructure for strengthening member countries' cyber-security orientations as well as improving international cooperation. For instance, the Italy-based European Electronic Crimes Task Force, which has dedicated personnel from the countries involved to investigate and prosecute cybercrimes, provides a forum for law enforcement agencies, the private sector and academia from the U.S. and EU nations.

The FBI announced in 2009 that it would permanently base a computer crime expert in Estonia to help fight international cybercrimes [4]. Similarly, Romania's DIICOT reported that it exchanged information with law enforcement agencies from more than 50 countries including the U.K.'s SOCA and the U.S. FBI [26]. There has been a close collaboration between the Romanian police and FBI agents since the early 2000s. As of 2008, Romania's national police and the FBI arrested 90 Romanians engaged in cybercrimes. Western multinationals have also helped to strengthen cyber-security related institutions. To take an example, eBay has been educating Romanian prosecutors about cybercrimes including explaining to a judge using layman's language [112].

On the other hand, the environments of tension, distrust, and conflict, which characterized the U.S.-Soviet cold war relationship, have been the typical features of U.S.-Russia relationship on cyber-security. This must be seen against the backdrop of the emergence of cyber-security as a hot-button issue in international discourses [60,61]. Some U.S. observers believe that Russia has trained hackers in Internet warfare and the country is systematically probing the computer networks in the U.S. to find weaknesses [14,64]. Russia, on the other hane, is arguably concerned about the U.S. superiority in the cyberspace [2,68]. The two countries have planned a dialogue which would include discussions about how each side's military views the Internet and an effort to establish a hot line that could be used during cyber-security crises [91].

The U.S.-Russia difference in the approach to cyberspace is also reflected in their memberships in different international alliances related to cyber-security. Russia and its allies (Table 2) consider important to focus on the broader problem of information security rather than the narrower cyber-security. In 2008, the Shanghai Cooperation Organization (SCO) Agreement in the field of International Information Security emphasized on and expressed concerns about the 'digital gap' between the West and the East. The SCO economies and Western countries also exhibit a wide divergence over issues related to Internet control. The SCO economies have been particularly concerned about the West's monopolization in ICT products and less developed countries' dependence on the West. They like to control information that is likely to provoke the three "evils" (terrorism, extremism, separatism). They also consider important to prevent other nations from using technologies to disrupt economic, social and political stability and national security. For instance, Russia arguably is concerned about the dissidents' and human rights groups' mobilization on the Internet and possible "non-violent Color Revolutions" and the West's ability to support such mobilization [2,68]. Western countries, on the other hand, maintain that too much government regulations may harm cyber-security and emphasize the importance of the private sector [52].

SCO states believe that the CoECoC fails to take into account a number of issues and would create adverse impacts such as cyber-security abuses and cyber-conflict. Russia's SCO National Coordinator described the CoECoC as less than satisfactory [52]. Russia has rejected the CoECoC arguing that it violates the country's Constitution by permitting foreign law enforcement agencies to conduct Internet searches inside its borders.

In 1998, Russia first introduced a draft resolution to the U.N. Security Council, entitled "Developments in the field of information and telecommunications in the context of security". In September 2011, China, Russia, Tajikistan and Uzbekistan submitted a draft code of the International Code of Conduct for Information Security before the 66th UN General Assembly Meeting.

The above differences have contributed to the lack of U.S.-Russia cooperation in cyber-security. Russia has signed agreements to help the U.S. in investigating some crimes but not on cybercrimes. An example to illustrate this would be the FBI's handling of two Russian hackers in 2000, who were lured to the U.S. with job offers. FBI Agents also downloaded data from the hackers' computers in Chelyabinsk, Russia. In 2002, Russia filed hacking charges against the FBI arguing that it was illegal to download data from computers in Russia [59]. Likewise, in 2001, the U.S. DoJ requested the assistance from Russian authorities, but there was no response [63].

Subsequently some degree of cooperation emerged between Russia and the West. In 2004, collaboration between British and Russian police led to arrests of an online extortion ring's members accused of blackmailing online sports betting websites that cost British companies US$ 120 million [98]. In 2005, U.S. law-enforcement officials reported that they received help from their Russian counterparts on about one out of six cybercrime-related requests [20]. Russian cyber-security agents were also trained in the U.S. [101]. Perhaps the most important sign of cooperation was Russia's arrest of a St. Petersburg-based hacker, who was indicted by the U.S. for stealing US$ 9 million from the Royal Bank of Scotland in 2006. However, the U.S. expressed frustration and disappointment when he received only a six-year suspended sentence [73,96].

When Vladimir Zdorovenin, a Russian citizen was extradited to the U.S. by Swiss authorities for his alleged involvement in security fraud, computer hacking and ID theft in January 2012, Russian authorities complained that the Swiss and U.S. authorities did not notify them. A Russian Foreign Ministry spokesman commented: "Unfortunately, this is not the first time when U.S. special services organize the detention of our nationals in third countries, often on dubious grounds and by provocative methods. What we're looking at is the unlawful exterritorial application of U.S. laws against Russian nationals" [88]. Likewise, in response to U.S.-based security researchers' findings that a group of five men based in St. Petersburg, Russia was responsible for spreading the Koobface worm, the Russian Embassy in the U.S. reacted that it had no information regarding that group. It further noted that U.S. law enforcement officials had never contacted the embassy about the group [89].

As a further example, investigation conducted by Facebook and other independent researchers indicated that five men based in St. Petersburg, Russia were responsible for spreading the Koobface worm on Facebook and other social networking sites. The researchers' study revealed that the group made at least US$ 2 million a year during its three and a half years of its existence [89]. Facebook and IT security firms provided detailed intelligence to the authorities in the West and in Russia. However, no action was taken against the Koobface gang [111].

Discussion and implications

In this paper, we applied and extended theories in white-collar crimes in the context of international cybercrimes. A theoretical contribution is the observation that emerging economies' international cooperation and integration would help them enhance system capacity and law enforcement performance to deal with cybercrime. Another contribution is the demonstration that cyber-offenders are less likely to be jurisdictionally shielded in such economies.

As discussed above, the masterminds in the Zeus case and the creators of Koobface were jurisdictionally shielded in Ukraine and Russia respectively. Why Russia- and Ukraine-based cyber-offenders are often not criminally prosecuted is not because alternative sanctions are applied as predicted by the alternative sanctions argument [94], but no sanctions are actually imposed. In this regard, while the organized crime groups which include "underworld" criminals as well as "overworld" figures from the former Communist Party are in "organizationally shielded" positions as proposed by organizational advantage argument [46], most international cybercriminals can “jurisdictionally shield” themselves just by operating from economies with a low degree of cooperation and integration with the West. Moreover, the primary reason they are not prosecuted is not because of the difficulty in obtaining direct evidence against them as argued by the system capacity approach [105]. This is in a large part due to outdated regulative institutions and the unwillingness of law enforcement agencies to pursue cyber-fraud cases as the criminals mainly victimize foreigners. When cybercriminals from Russia travel to many of the Western countries, however, they may no longer hide behind the jurisdictional shield of Western law enforcement authorities.

Cyber-security has become one of the most prominent IR challenges for Russia and the U.S. Allegations and counter-allegations, which have been persistent themes in dialogues and discourses in the U.S.-Russia relationship in cyber-security, can be linked to the lack of an extensive cooperation. Despite some progress in the past, the Russia-U.S. cooperation has been on ice for some time. U.S. law enforcement agencies seem to think that Russian authorities are often indifferent and uncooperative in fighting cybercrimes. This is in sharp contrast to the deeper and stronger collaborations and partnerships between the U.S. and EU countries.

As noted above, cybercrime cases are complex and thus require substantial resources to prosecute. Using the system capacity argument, while most white-collar crimes have a substantial cost to the local economy and thus their low indictment rates due to limited resources are unjustifiable [105], this may not be the case for cybercrimes, most of which, as noted above, target international victims and thus cost little to the local economy.

FSU&CEE economies’ system capacity to deal with cybercrime is a matter of concern for the governments as well as private sector players in the West. Western countries have also provided cyber-security related resources, training and expertise that have helped enhance the system capacity of some countries. Private sector players that are affected by cybercrimes associated with FSU&CEE economies also investigate such crimes. For some economies in the region, however, incentives and pressures have not been significant enough to overcome the institutional inertia.

While the West faces significant jurisdictional challenges in investigating and prosecuting international cybercriminals, such challenges are more pronounced in dealing with economies with low degrees of modernization of institutional frameworks and/or low degree of cooperation and integration with the West. For instance, in Estonia and Romania, which are among the countries most integrated with the west (Table 2), cybercriminals are jurisdictionally “less shielded” compared to those in Russia.

Commenting on the January 2012 extradition of a Russian, who allegedly engaged in cybercrime activities, an FBI Assistant Director warned that cybercriminals cannot “hide behind the safety and anonymity of a Russian IP address” and they would be brought to justice [34]. This probably is an over-statement, however in light of the fact that the cybercrime ecosystem in Russia is relatively well preserved and virtually untouched.

Most FSU&CEE economies have enacted cyber-security related laws and regulations. There are also some motivated law enforcement officials. Their efforts, however, have been hindered by the outdated legislation and lack of resources. What is of concern is the substantial gap between law in the book and law in action. More attention needs to be given not just on the narrow aspects of cyber-security related legislations, but also on the broader institutional and political context in which they are introduced. With increased digitization, FSU&CEE economies themselves are likely to be victimized. It is thus more important in the future for the governments in these economies to work with the private sector and international partners, addressing systemic problems and developing system capacity as well as building specific areas of law enforcement.

Limitations and future research

Several limitations of this research must be recognized in a balanced discussion of its findings. One limitation of our study is that, we primarily used English literature sources. This may have led to some western bias in defining cybercrime and cyber-security issues in the region as well as the institutional contexts. An additional limitation is that it lacks first-hand, primary source materials.

Both the contributions and limitations of this research merit attention and afford directions for future work. In future research, scholars need consider academic literature and popular press articles published in local languages and collect primary materials from businesses and consumers affected by cybercrimes which would help to fully recognize and appreciate differing perspectives and viewpoints about cybercrimes associated with the region and the impacts on the local economy and society.

In future conceptual and empirical work scholars need to compare and contrast broader contexts associated with cybercrime and cyber-security issues in selected FSU&CEE economies with other socialist and post-socialist economies. For instance, while both China and Russia are SCO members, they differ widely in terms of the institutional contexts associated with cyber-security. This is because a society’s power structure and the vested interests of powerful societal actors have an enormous impact on the way crimes in general and cybercrimes in particular are defined, conceptualized, theorized, measured, responded to and policed [19,61]. Different social and political contexts in China and Russia are likely to translate into different patterns and structures of cybercrime and cyber-security landscape.

References

Acohido, B. (2010). ‘Scareware’ ads proliferate across Internet. USA Today.

Adams, J. (2001). Virtual defense. Foreign Affairs, May/June 98–112.

Andreas, P., & Price, R. (2001). From war fighting to crime fighting: transforming the American National Security State. International Studies Review, 3(3), 31–52.

Associated Press Worldstream. (2009). FBI to station cybercrime expert in Estonia, http://www.msnbc.msn.com/id/30683801/ns/technology_and_science-security/t/fbi-station-cybercrime-expert-estonia/#.T3dS7tnLuZQ.

Baker, S. (2004). Gambling sites: this is a holdup. Business Week, August 9. http://www.businessweek.com/magazine/content/04_32/b3895106_mz063.htm.

balticbusinessnews.com (2011). FBI arrest may lead to Estonia’s largest asset seizure, November 11, http://balticbusinessnews.com/article/2011/11/11/fbi-arrest-may-lead-to-estonia-s-largest-asset-seizure.

balticbusinessnews.com (2012). Estonian court approves extradition of six persons to US for cybercrime, February 21, http://balticbusinessnews.com/article/2012/2/21/estonian-court-approves-extradition-of-six-persons-to-us-for-cybercrime.

Baumol, W. J. (1990). Entrepreneurship: productive, unproductive, and destructive. Journal of Political Economy, 98(5), 893–921.

bbc.co.uk (2011). Spammers sought after botnet takedown. March 25. http://www.bbc.co.uk/news/technology-12859591.

bbc.co.uk (2012). Microsoft names ex-antivirus employee as botnet ‘suspect’, January 24, http://www.bbc.co.uk/news/technology-16700192.

Bell, R. E. (2002). The prosecution of computer crime. Journal of Financial Crime, 9(4), 308–325.

Benson, M., Cullen, F., & Maakestad, W. (1990). Local prosecutors and corporate crime. Crime and Delinquency, 36, 356–372.

Benson, M.L., Madensen, T.D., & Eck, J.E. (2009). White-collar crime from an opportunity perspective. The Criminology of White-Collar Crime Part III, 175–193.

Bickers, C. (2001). Combat on the Web. August 16, Far Eastern Economic Review, 30–33.

Blakely, R., Richards, J., Halpin, T. (2007). Cybergang raises fear of new crime wave. The Times (London), 13.

Blau, J. (2004). Viruses: from Russia, with love? IDG News Service. http://www.pcworld.com/news/article/0,aid,116304,00.asp.

Bray, C. (2011). Seven accused of infecting computers with malware in more than 100 countries, http://online.wsj.com/article/SB10001424052970204358004577028090371514700.html.

brookings.edu. (2011). Can Ukraine Join Europe as Yanukovych moves away from EU Values?, July 28, http://www.brookings.edu/research/opinions/2011/07/28-ukraine-pifer.

Brownstein, H. (2000). The social production of crime statistics. Justice Research & Policy, 2(2), 73–89.

Bryan-Low, C. (2005). Digital trails: in Eastern Europe, a gumshoe chases internet villains; Microsoft deploys Mr. Fifka to hunt cyber felons amid rise in online crime; tailing 'Benny' in a Czech city. September 1, Wall Street Journal, A.1.

Bulgaria Political Risk Yearbook (2007). Bulgaria: political risk yearbook: Bulgaria country report, January. New York: The PRS Group.

Bulkeley, W. M. (2008). Quiz; tech IQ: how well do you know…the digital world. Wall Street Journal, R.14.

Cetron, M. J., & Davies, O. (2009). Ten critical trends for cybersecurity. Futurist, 43(5), 40–49.

Claburn, T. (2009). Facebook wins $711 million from spammer. Information Week, October 30, http://www.informationweek.com/news/global-io/security/showArticle.jhtml?articleID=221400140.

Collins, A. (2003). Security and Southeast Asia: Domestic, regional, and global issues, Lynne Rienner Pub.

Constantin, L. (2011). Romania's anti-cybercrime efforts lack a social component, September 26, http://www.csoonline.com/article/690521/romania-s-anti-cybercrime-efforts-lack-a-social-component.

Davis, K., & Joan G. (2005). Can you smell the phish?, Kiplinger's personal finance magazine. February. http://www.kiplinger.com/magazine/archives/2005/02/phish3.html?kipad_id=2.

Ducklin, P. (2011). Busted! Ukrainian cybercrime duo who ripped off $4.5 million sent to prison in UK, November 2, 2011, http://nakedsecurity.sophos.com/2011/11/02/busted-ukrainian-cybercrime-duo-who-ripped-off-4-5-million-sent-to-prison-in-uk/.

Economist.com. (2007). Global agenda. A walk on the dark side. August 30 ,Europeview, 1.

Espiner, T. (2007). Cracking open the cybercrime economy. ZDNet News. December 14, http://news.zdnet.com/2100-1009_22-180416.html. Accessed 2 October 2008.

Esposito, R., & Lee, F. (2011). Feds: cyber criminals hijacked 4 million computers, November 9, http://abcnews.go.com/Blotter/feds-cyber-criminals-hijacked-million-computers/story?id=14915648.

Faas, R. (2012). Lessons for IT, Apple in Flashback brouhaha, Computerworld, April 16, http://www.macworld.com/article/1166254/what_you_need_to_know_about_the_flashback_trojan.html.

Farrell, G., Riley, M., Sheridan, B. (2011). From want ads to posters. Bloomberg Businessweek, August 8, 38–39.

Fbi.gov (2012). Manhattan U.S. Attorney and FBI assistant director in charge announce extradition of Russian citizen to face charges for international cyber crimes, January 17, http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-extradition-of-russian-citizen-to-face-charges-for-international-cyber-crimes.

Ferguson, P. (2011). Esthost taken down—biggest cybercriminal takedown in history, http://blog.trendmicro.com/?p=38093.

finextra.com. (2011). Hackerville: the epicenter of Romanian hackers. March 26. http://www.finextra.com/community/fullblog.aspx?blogid=5140.

Finkle, J. (2010). Inside a global cybercrime ring, http://www.reuters.com/article/idUSTRE62N29T20100324.

Fitzgerald, P. (2008). Crash of civilizations. September/October. Foreign Policy, 122.

Fong, C. (2008). Fighting the agents of organized cybercrime. May 8, www.CNN.com.

Foreign Policy. (2005). Caught in the net: Australian teens, March/April, 92.

Giles, J. (2010). Scareware: the inside story new scientist. 205(2753), 38–41.

Goldman, L. (2004). Cybercon. Forbes, 174(6).

Goodman, M. (2011). What business can learn from organized crime. Harvard Business Review, 89(11), 27–30.

Granovetter, M. (1985). Economic action and social structure: the problem of embeddedness. The American Journal of Sociology, 91(3), 481–510.

Greenberg, A. (2010). Massive U.S. Cybercrime bust mostly nabbed exchange students, September 30, http://blogs.forbes.com/andygreenberg/2010/09/30/massive-u-s-cybercrime-bust-mostly-nabbed-exchange-students/.

Hagan, J., & Parker, P. (1985). White-collar crime and punishment: class structure and legal sanctioning of securities violations. American Sociological Review, 50, 302–316.

Holtfreter, K., Slyke, S. V., & Blomberg, T. G. (2005). Sociolegal change in consumer fraud: from victim-offender interactions to global networks, Crime. Law and Social Change, 44(3), 251–275.

Hurtado, P., & Michael R. (2011). Hackers hijack millions of computers in 'Massive' Fraud Case, November 09, http://www.businessweek.com/news/2011-11-09/hackers-hijack-millions-of-computers-in-massive-fraud-case.html.

Ismail, I. (2008). Understanding cybercriminals. February 18, New Straits Times (Malaysia), 12.

Kendall, N. (2009). What the cybercrime fraudsters get up to. August 1, Times Online. http://www.timesonline.co.uk/tol/news/uk/crime/article6735761.ece.

Kirk, J. (2012). Ukraine shuts down forum for malware writers, http://www.computerworld.com/s/article/9225693/Ukraine_shuts_down_forum_for_malware_writers.

Kizekova, A. (2012). The Shanghai Cooperation Organization: challenges in Cyberspace – Analysis, http://www.eurasiareview.com/27022012-the-shanghai-cooperation-organisation-challenges-in-cyberspace-analysis/.

Kramer, A. E. (2010). E-mail spam falls after Russian crackdown, October 26, http://www.nytimes.com/2010/10/27/business/27spam.html.

Krebs, B. (2007). Taking on the Russian business network. October 13, http://blog.washingtonpost.com/securityfix/2007/10/taking_on_the_russian_business.html. Accessed 27 October 2008.

Krebs, B. (2010).U.S. Charges 37 alleged money mules. http://krebsonsecurity.com/2010/09/u-s-charges-37-alleged-money-mules/.

Krebs, B. (2011). Ukrainian general arrested in cyber heists, December 16, http://krebsonsecurity.com/2011/12/ukrainian-general-arrested-in-cyber-heists/.

Kshetri, N. (2005). Hacking the odds. May/June, Foreign Policy, 93.

Kshetri, N. (2006). The simple economics of cybercrimes. IEEE Security and Privacy, 4(1), 33–39.

Kshetri, N. (2010). The global cyber-crime industry: Economic, institutional and strategic perspectives. New York: Springer.

Kshetri, N. (2013a). Cyber-victimization and Cybersecurity in China, Communications of the ACM (forthcoming).

Kshetri, N. (2013). Cybercrime and cyber security in the global south. Houndmills: Palgrave Macmillan.

Kuznetsova, N. F. (1994). Crime in Russia: causes and prevention. Demokratizatsiya, 2(3), 443–449.

Lemos, R. (2001). FBI "hack" raises global security concerns. CNet News, May 1, http://news.com.com/2100-1001-950719.html.

Lenzner, R., & Vardi, N. (2004). The next threat. September 20, Forbes, 70.

Leyden, J. (2010). Russian trade body aims to fight cybercrime: Russia no safe haven for spammers and cybercriminals, April 12, http://www.theregister.co.uk/2010/04/12/russia_cybercrime_feature/.

Leyden, J. (2009). FBI and SOCA plot cybercrime smackdown. October 22, The register. http://www.theregister.co.uk/2009/10/22/soca_fbi_cybercrime_strategy/ Accessed 27 October 2009.

Marson, J. (2010). Small victory in the fight against global cybercrime, June 21, http://www.time.com/time/business/article/0,8599,1998055,00.html.

Maurer, T. (2011). Cyber Norm emergence at the United Nations: an analysis of the UN's activities regarding cyber-security, discussion paper #2011-11, explorations in cyber international relations discussion paper series, Belfer center for science and international affairs, Harvard Kennedy School http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

McDougal, T. L. (2011). Predation and production in a Core-Periphery model: a note, peace economics, peace science and public policy: 17(1), Article 2, doi:10.2202/1554-8597.1219: http://www.bepress.com/peps/vol17/iss1/2.

Mello, J. (2011), Spam researchers help bust global cybercrime ring, PCWorld, Nov 12, http://www.pcworld.com/article/243748/spam_researchers_help_bust_global_cybercrime_ring.html.

Menn, J. (2011). US uncovers alleged 'click fraud' ring, November 9, http://www.ft.com/intl/cms/s/0/96c244ae-0b16-11e1-ae56-00144feabdc0.html#axzz1dEthASN1.

Menn, J. (2012). Bank security: thieves down the line, January 2, http://www.ft.com/cms/s/0/951f0efe-2d60-11e1-b985-00144feabdc0.html#axzz1iRw53Er3.

Moscaritolo, A. (2010). Prison sentence for RBS hacker suspended in Russia, September 10, http://www.scmagazine.com.au/News/231634,prison-sentence-for-rbs-hacker-suspended-in-russia.aspx.

Mullins, R. (2010). Did the government sit on the ‘scareware’ case too long?: Critic says authorities took too long to break cyber ring, June 21, http://www.networkworld.com/community/blog/did-government-sit-scareware-case-too-long.

Naraine, R. (2012). Microsoft: ‘Kelihos’ botnet master worked for AV vendor, January 24, http://www.zdnet.com/blog/security/microsoft-kelihos-botnet-master-worked-for-av-vendor/10195.

news.am (2011). Pornography distribution - most common type of cyber crime in Armenia, http://news.am/eng/news/85030.html, Accessed 08 December, 2011.

North, D. C. (1990). Institutions, institutional change and economic performance. Cambridge: Cambridge University Press.

O’Grady, J. D. (2011). MacDefender taken down in raid by Russian authorities?, August 4, http://www.zdnet.com/blog/apple/macdefender-taken-down-in-raid-by-russian-authorities/10777.

ohchr.org (2007) Report by the Kharkiv human rights protection group about Ukraine’s compliance with the convention against torture and other cruel, inhuman or degrading treatment or punishment. April, http://www2.ohchr.org/english/bodies/cat/docs/ngos/khrpg.doc Accessed 27 October 2009.

Onyshkiv, Y., & Bondarev, A. (2012). Ukraine thrives as cybercrime haven, March 8, http://www.kyivpost.com/news/nation/detail/123965/.

Paget, F. (2010). McAfee Helps FTC, FBI in case against ‘Scareware’ Outfit, June 1, http://blogs.mcafee.com/mcafee-labs/mcafee-helps-ftc-fbi-in-case-against-scareware-outfit, Accessed 26 January 2011.

Paoli, L., & Fijnaut, C. (2006). Organized crime and its control policies. European Journal of Crime, Criminal Law & Criminal Justice, 14(3), 307–327.

Parto, S. (2005). Economic activity and institutions: taking stock. Journal of Economic Issues, 39(1), 21–52.

Perlroth, N. (2012). Traveling light in a time of digital thievery, February 10, http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?pagewanted=2&_r=1&ref=technology&src=me.

Peterson, D. J. (2005). Russia and the information revolution, RAND corporation http://www.rand.org/pubs/monographs/2005/RAND_MG422.pdf.

Pontell, H., Calavita, K., & Tillman, R. (1994). Corporate crime and criminal justice system capacity: government response to financial institution fraud. Justice Quarterly, 11, 385–410.

Reuters. (2009). Fake security software in millions of computers, October 20, p. A43, http://www.reuters.com/article/2009/10/19/us-cybersecurity-symantec-idUSTRE59I0A520091019.

RIA Novosti (2012). Moscow slams hacker's extradition to U.S. January 20, http://en.rian.ru/russia/20120119/170850006.html.

Richmond, R. (2012). Web gang operating in the open, January 16, http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html.

Rock Center. (2012). University professor helps FBI crack $70 million cybercrime ring, March 21, http://rockcenter.msnbc.msn.com/_news/2012/03/21/10792287-university-professor-helps-fbi-crack-70-million-cybercrime-ring?chromedomain=worldnews.

Segal, A. (2012). Chinese computer games. Foreign Affairs, 91(2), 14–20.

Sengupta, S., & Jenna, W. (2011). 7 Charged in web scam using ads. November 9, http://www.nytimes.com/2011/11/10/technology/us-indicts-7-in-online-ad-fraud-scheme.html.

Serio, J. D., & Gorkin, A. (2003). Changing lenses: striving for sharper focus on the nature of the 'Russian Mafia' and its impact on the computer realm. International Review of Law, Computers and Technology, 17(2), 191–202.

Shapiro, S. (1990). Collaring the crime, not the criminal: reconsidering the concept of white-collar crime. American Sociological Review, 55, 346–365.

Shelley, L. I. (1999). Organized crime and corruption are alive and well in Ukraine. Transition, 10(1), 6–7.

Shuster, S. (2010). The Russian hacker bust: is the FBI chasing mules?, Oct. 05, 2010, http://www.time.com/time/world/article/0,8599,2023391,00.html.

Soldatov, A. (2011). Vladimir Putin's cyber warriors, December 9, http://www.foreignaffairs.com/articles/136727/andrei-soldatov/vladimir-putins-cyber-warriors.

sophos.com. (2004). Police crack suspected online extortion ring. July 23, Sophos reports. http://www.sophos.com/virusinfo/articles/extortion.html.

Sullivan, B. (2004). Foreign fraud hits US e-commerce firms hard. MSNBC. http://www.msnbc.msn.com/id/4648378.

Sullivan, B. (2007). Who's behind criminal bot networks? April 10, http://redtape.msnbc.com/2007/04/whos_behind_cri.html.

Swartz, J. (2004). Crooks slither into Net's shady nooks and crannies crime explodes as legions of strong-arm thugs, sneaky thieves log on. October 21, USA Today. www.usatoday.com/printedition/money/20041021/cybercrimecover.art.htm.

Symantec. (2007). Symantec reports cyber criminals are becoming. September 17, http://www.prwire.com.au/pdf/symantec-reports-cyber-criminals-are-becoming-increasingly-professional.

The Economist. (1999). Crime without punishment: special article. Russian Organized Crime, 352(134), 17–19.

The Economist. (2009). International: it may make life easier and cheaper. East Africa gets broadband., 391(8636), 46.

Tillman, R., Calavita, K., & Pontell, H. (1996). Criminalizing white-collar misconduct: determinants of prosecution in savings and loan fraud cases. Crime Law and Social Change, 26(1), 53–76.

Voice of Russia. (2011). Real punishment for virtual criminals, January 31, http://english.ruvr.ru/2011/01/31/42167678.html.

Walker, C. (2004). Russian Mafia extorts gambling websites. June, http://www.americanmafia.com/cgi/clickcount.pl?url=www.americanmafia.com/Feature_Articles_270.html.

Warren, P. (2007). Hunt for Russia's web criminals the Russian business network

Warren, P. (2011). Russia proposes new plan to defeat online hackers, December 22, http://www.telegraph.co.uk/sponsored/russianow/technology/8972805/Russia-plan-defeat-online-hackers.html which some blame for 60 % of all internet crime – Appears to have gone to ground. November 15.

Wenping, H. (2007). The balancing act of China's Africa policy. China Security, 3(3), 32–40. summer.

Williams, C. (2011). Cybercrime gang 'responsible for a third of data thefts'. Jan 27 http://www.telegraph.co.uk/technology/8283882/Cybercrime-gang-responsible-for-a-third-of-data-thefts.html.

Wylie, I. (2007). Internet; Romania home base for EBay scammers; the auction website has dispatched its own cyber-sleuth to help police crack fraud rings. December 26, Los Angeles Times, C.1.