The European Review of Organised Crime

Debate

Russian-speaking Cyber Crime: Reasons behind Its Success[1]

Lucie Kadlecová*

Abstract: Cyber crime has become a key challenge to international security. Although there are active groups of cyber criminals all over the world, Russia and other post-Soviet countries have been considered traditional hotspots for cyber organised crime. The aim of this article is to examine the factors that might have facilitated the empowerment and global reach of hackers trained in the post-Soviet space. The article argues that the particular strength of Russian-speaking criminals must be perceived as the result of a combination of various factors that developed after the dissolution of the USSR. The alleged cooperation between the government and illegal criminal groups in cyber space is usually regarded as a powerful explanation; however, this article proposes that such a relationship could only have been established after the criminal structures had achieved a certain level of professional development.

Keywords: Cyber crime – Russian Federation – Post-Soviet region – Organised crime

*Lucie Kadlecová is PhD Candidate at Institute of International Studies, Charles University, Prague, Czech Republic.
Email: Lucie.Kadlecova@fsv.cuni.cz

The European Review of Organised Crime 2(2), 2015, 104-121
ISSN: 2312-1653

[1] The author wishes to stress that the paper was written before her possible affiliation with the National Cyber Security Centre of the Czech Republic and the author's views do not represent statements or opinions of the Centre.

Introduction

Modern cyber crime and its quick growth over the last two decades has become one of the key challenges to international security and has created a new frontier for the world of organised crime. No other type of illegal activity has such low requirements for participation while yielding such high profits. In addition, the prevention of cyber crime is still quite underdeveloped. Although there are active groups of cyber criminals all over the world, the Russian Federation and other post-Soviet countries have been centres for cyber organised crime in the recent years. Translated into numbers, according to official estimates published by Russian cyber security company Group-IB (2011: 6), the turnover of Russian-speaking criminals reached $4.5 billion in 2011, while Russian national-only cyber criminals' revenues were $2.3 billion, doubling the $1.2 billion from the previous years. Moreover, the annual turnover of cyber crime in Russia fulfilled the expectations of increased annual growth, as suggested in Group-IB's reports from recent years (cf. Group-IB, 2014).

The increasing economic success of Russian-speaking cyber crime business, despite the world's economic crisis, further proves its evolutionary trend over the last few years. Rather than the chaotic cyber crime market of earlier years, the current structure has become more organised, resulting in criminal groups that can often resemble a structured company with coordinated operations and clear goals (Paganini, 2012). The professionalisation and commercialisation of cyber crime in the post-Soviet space may have potentially dangerous consequences in the future as attacks may become more sophisticated.

Russia has been identified as a place of origin for at least one third of the most dangerous malicious software worldwide (Mwangi, 2014). This was confirmed by Kyle Wilhoit, a cyber security researcher for American Trend Micro, who stated that "in terms of sophisticated types of malware, Russia leads the way" (Plesser, 2014). Similarly, according to Russian cyber analyst Vitaly Kamluk, "if you look at the quantity of malware attacks, the leaders are China, Latin America and then Eastern Europe, but in terms of quality then Russia is probably the leader" (De Carbonnel, 2013). Troels Oerting, Head of Europol's European Cybercrime Centre (EC3), further corroborated the prevalence of Russian-speaking cyber crime when he stated that "85 per cent of [Europol's] cases are Russian-speaking organised cyber groups" (Brewster, 2014).

The theft discovered by American company Hold Security in August 2014 serves as an example of recent Russian-speaking illegal activities with a universal impact. Hold Security revealed that a Russia-based criminal ring of hackers succeeded in collecting confidential data from approximately 420,000 websites, including 1.2 billion unique sets of passwords and user names and 500 million email addresses. Even more astonishing are the details about the attackers themselves: Hold Security reported that the group had its headquarters in a small city in south central Russia near the border with Mongolia and Kazakhstan, and consisted of less than a dozen young men in their twenties (Perlroth and Gelles, 2014). Since the cyber criminals targeted essentially every website they could, ranging from big corporations to small companies and even households, their attacks amounted to such a magnitude that the data breach was labelled "the largest known collection of stolen Internet credentials" (Perlroth and Gelles, 2014; see Hold Security, 2014 for more details).

Russian-speaking cyber crime has a prevalent and dominant position in this field. Subsequently, the question emerges: what are the key factors which have enabled cyber crime in the post-Soviet space to gain such a dominant position on the global market with illegal goods and services? The aim of this paper is to examine the factors that might have facilitated the empowerment and global reach of hackers raised and educated in countries within post-Soviet space. This paper argues that the main cause is a combination of conditions that developed after the dissolution of the USSR. The key reasons include legal loopholes in the Criminal Code of the Russian Federation, low legal employability of young IT experts, and the low cost of cyber services provided by criminal groups. The alleged reciprocally beneficial relationship between the Russian government and organised crime groups might also be a factor; however, the argument is based on the assumption that this relationship, which has not been directly proven by experts yet, could be established only after the criminal structures had achieved a certain level of professional development.

This argument will be presented in five steps. Firstly, the paper will assess the conditions and development of cyber crime in the immediate post-Soviet era. Secondly, the recent evolution and the current practice of Russian-speaking cyber crime will be examined. Thirdly, the paper will discuss the drawbacks of legal practice in the Russian Federation and the supposed cooperation between the Kremlin and the cyber underworld. Some of the above-mentioned arguments will be further illustrated using the case of the Russian Business Network (RBN). Finally, this study will critically evaluate the discussed factors and their role in establishing the Russian-speaking cyber mafia in the global market.

While reading this paper, the reader should bear in mind the volatile nature of the topic, which is also projected in the selection of information sources. In an attempt to work with the most updated and relevant information, the paper builds upon information retrieved from the mainstream media (e.g., CNN, BBC, The Guardian, The New York Times) or specialised online magazines (e.g., Computer World, Network World, Wired, ZDNet). In order to balance these sources and support their reliability, the paper also benefits from contributions by world-recognised cyber security experts and analysts (e.g., Dmitri Alperovitch, Jeffrey Carr, Max Goncharov) or reports by international companies specialising in cyber security or cyber crime (e.g., Trend Micro, Group-IB, Hold Security). In some cases, the analysis relies heavily on a single source as the relevant information might be included in a very small number of publications. In such cases, there has been an attempt to work with the most relevant and reliable sources of information, Group-IB's reports in this instance.[2]

It is also important to clarify the terminology used in order to minimise the possible misinterpretation over the terms "Russian" and "Russian-speaking" criminals. Russian experts usually prefer "Russian" cyber crime as the ones committed solely by Russian citizens. Nevertheless, in American and European resources, the term "Russian" very often refers to persons originating from Russia as well as all citizens of the former Soviet Union area, including hackers from Ukraine or Baltic and central-Asian republics (Group-IB, 2011). This paper makes an effort to differ between these two terms by referring to the "Russian" cyber crime market as the one exclusively committed by Russian citizens; "Russian-speaking" will then refer to citizens of countries of the post-Soviet space who speak the Russian language and can use it for their criminal activities. However, this issue may still be convoluted at times since these two terms strongly overlap and some sources simply do not differentiate between the terms based on their interconnectedness.

Evolution of Russian-speaking Cyber Market in the Post-Soviet Era

The volatile socio-political conditions, which occurred after the dissolution of the Soviet Union, were convenient to initiate effective and potent cyber criminal activities. The power vacuum contributed to a severe lack of legal enforcement and investigative focus on illicit cyber operations. An unstable economic environment and limited lawful working opportunities resulted in highly educated and technologically competent individuals who could start using their capabilities to conduct criminal activities in cyber space. This initial combination of factors in the immediate post-Soviet era, supported by a long tradition of Russian organised crime, caused a sense of impunity to prevail and thus thousands of citizens joined online criminal groups and their crime milieu during the late 1990s and early 2000s (Alperovitch, 2009).

Until 1994, cyber crime in the post-Soviet republics was particularly rooted in software piracy. The key turning point came with the breach of the computerised systems of Citibank by Russian-speaking hackers. Vladimir Levin, the main figure behind the attack, and his group of hackers were able to wire transfer sums of money ranging

[2] As mentioned in the methodology section of the Group-IB's report from 2013, the figures published by the company are based on extrapolation of information gained by Group-IB's expert team during their day-to-day investigation and analysis of cyber crime. The automated cyber threat monitoring systems used to obtain the data were, for instance, Fraud Monitoring, Threat Centre or Bot-Trek. In order to examine the methodology used for the statistical calculations, see the Group-IB's reports. (Group-IB, 2013)

from several thousands to tens of thousands of dollars to their accounts in the U.S., Europe or Indonesia simply using stolen user IDs, passwords and key codes. As a result, Levin and his accomplices accessed around $10 million in total on Citibank accounts via the telephone system in only a couple of weeks in 1994. Levin was eventually arrested in London in the spring of 1995 (Kabay and Guinen, 2011a). This was the first time that post-Soviet cyber crime showed its true potential.

In the late 1990s hacker Roman Vega of Ukraine, who went by the alias Roman Stepanenko or simply Boa, was one of the first individuals to create a sustainable illegal online business. Vega established the so-called "Boa Factory" website which served as a clearing house for the purchase and distribution of various goods produced by cyber criminal activities. These ranged from bank and credit card information to forged passports and traveller's checks. Vega was finally arrested in Cyprus in February 2003, extradited to the U.S. and charged with, amongst others, trafficking stolen credit cards, money laundering, and wire fraud (Alperovitch, 2009).

Preceding his arrest in 2003, Roman Vega was involved in another well-organised illegal cyber enterprise called "CarderPlanet". This organisation was founded in May 2001 and was supposedly based in Odessa, Ukraine. The CarderPlanet forum was a place for buying and selling illegal online goods and services together with sharing hacking know-how and offering tutorials for newcomers who wanted to get a quick initial guide to cyber fraud principles. Misha Glenny (2012: 68) describes the dangerous nature of the website as follows: "[i]t is no exaggeration to say that its creators were responsible for the emergence and consolidation of an entirely new method of engaging in major criminal activity: fraud that could be perpetrated on a huge scale with minimal resources and minimal risk". To demonstrate the large-scale worldwide ambitions of its administrators, the CarderPlanet forum also existed in an English-language mutation alongside the original Russian version for the final two years of its existence. The website was eventually disbanded by its own administrators in August 2004 after some of its key members, including Roman Vega, had been arrested earlier that year (Glenny, 2012; Kabay and Guinen, 2011b).

According to the U.S. Secret Service Assistant Director for Investigations Michael Merritt, "[t]he network created by the founders of CarderPlanet, including Vladislav Horohorin, remains one of the most sophisticated organisations of online financial criminals in the world. This network has been repeatedly linked to nearly every major intrusion of financial information reported to the international law enforcement community" (U.S. Department of Justice, 2010). This FBI press statement was released when Vladislav Horohorin, alias BadB, another founding father of CarderPlanet, was arrested in France in 2010. Horohorin continued to sell stolen data of credit cards even after the CarderPlanet had been shut down. In order to promote his services on his website, such as badb.biz, Horohorin also posted his own animated cartoons with highly controversial themes. For instance, one of them showed Russian president Vladimir Putin awarding medals to cyber criminals while claiming that thanks to these hackers, "citizens [of the U.S.] have no more money to pay their debts". The cartoon then transforms to state "Carders need you", accompanied by The Imperial March music theme from the Star Wars movie series (Metzger, 2010). After his arrest in 2010, Horohorin was described as one of the top five global cyber criminals because of his illegal online activities that included identity theft and access device frauds (Kabay and Guinen, 2011b).

Another case that illustrates the conditions and environment occurring in the post-Soviet territory in the late 1990s and early 2000s is the story of Dmitry Golubov. Golubov was involved in the CarderPlanet business as one of its senior members, and was identified as the hacker Script, a key figure in the hierarchy of the whole CarderPlanet (Munns, 2008). According to Misha Glenny (2012: 65) Script even organised the First Worldwide Carders' Conference in Odessa in 2002 to celebrate the CarderPlanet website and its first anniversary. The Ukrainian police eventually arrested Golubov in Odessa in the summer of 2005. However, in less than four months several Ukrainian members of parliament persuaded the local legal authorities that there was no substantial evidence that Golubov actually was Script or that he possessed any stolen data. His case was subsequently fully dismissed and Golubov was released from prison. A turning point arose when Golubov publicly claimed that he had been a victim of identity theft and announced the establishment of a new political party named the Internet Party of Ukraine (Glenny, 2012; Alperovitch 2009). The main political platform of this party focuses on fighting corruption and crime on the Internet.[3] Golubov's case is one of the first instances of alleged relations between the cyber underworld and state authorities in the region.

In summary, the above-mentioned cases of the late 1990s and early 2000s marked the initial trends in the evolution of post-Soviet cyber crime, which further developed in the following years. After the first years of relative power vacuum, online illegal activities in the post-Soviet area became a real threat that received more attention from international security agencies as seen in the cases of CarderPlanet or Boa Factory. The fear of international retribution forced a number of "casual" hackers to leave the illegal business and resulted in post-Soviet cyber crime gradually becoming more professionalised, commercialised and underground.

Recent Developments and Current Situation

The second half of the 2000s marked Russian-speaking cyber crime's transition tothe current model. The key trend of this time period was projected by the consolidation of

[3] Official website of the Internet Party of Ukraine, accessible from: http://ipu.com.ua/.

the online market through the creation of a few major cyber crime organizations capable of consistent operations. This transformation illustrates a shift from previous disintegrated market structures with illegal cyber activities towards the formation of efficient organisations with centrally managed structures. Furthermore, the newly created groups have often interlinked to share data or provide botnets in order to increase their profits on a mutually beneficial basis (Group-IB, 2011).

This crucial shift in organisational structure has been further accompanied by two supplemental trends in the evolution of Russian-speaking cyber crime. Firstly, the cyber crime business has been penetrated by groups of traditional organised crime with the intention to grasp control over the process of illegal activities in cyber space. By allocating necessary resources from more traditional areas of interest of organised crime towards cyber crime, these organisations have the potential to significantly increase the number of attacks on financial institutions. Secondly, the flow of funds into cyber crime has resulted in the market being penetrated by technically non-educated individuals whose specific interests are in capital investments. The combination of these factors has led to the relative stabilisation of the market and a boom in the internal cyber crime market, reflected by increased cooperation among various criminal organisations (Group-IB, 2011).

The professionalisation and stabilisation of cyber crime groups in Russia and other post-Soviet Republics resulted in increased capabilities of criminals and allowed such groups to concentrate more deeply on operations on a broader scale and extent while increasing their profits. This is reflected by the proportions of different types of cyber criminal activities on the market. According to the data from the second-half of 2013 and the first-half of 2014, online banking fraud has significantly decreased from $942 million in 2011 (when it was counted as the most successful sector of the Russian illegal cyber market) to $425 million. On the other hand, spam fraud has kept its stable position inrecent years with $841 million in revenues during the same period in 2013 and 2014 (Group-IB, 2014). Furthermore, other illegal activities such as credit card fraud, the internet market, or so-called cyber crime to cyber crime services, and distributed denial of service attacks (DDoS) are other popular and highly profitable means of income for Russian-speaking criminals in cyber space.

Besides the above-mentioned traditional illicit activities, the cyber gangs seek to keep up with progressive trends and explore new methods of moneymaking in cyber space. Recently, the growing popularity of crypto currencies among Russian-speaking hackers has been reported (Group-IB, 2013). Cyber criminals use the digital currency in two possible ways. Firstly, the crypto currencies have become a popular new target for cyber thefts. Secondly, this new kind of alternative currency has gained wide popularity among the hackers themselves, as they oftentimes use it for online transactions and payments in shops of the shadow Internet (Group-IB, 2014). To summarise, the commercialisation and professionalisation of cyber crime further builds up its highly dangerous nature, which is characterised by its adaptability and innovation.

Another argument in favour of the dominant position of Russian-speaking cyber crime may be the relatively inexpensive prices of the services advertised online. With the growing number of websites offering hackers' services and products, the competition has grown, which in turn caused the prices to lower. The prices vary depending on the type of service and the actual market demand and supply; for example, hacking a Facebook account cost $200 in 2011, whereas three years later a customer would spend half the amount. Generic spamming was priced at $13 per 10,000 messages in 2011 while $5 was enough for the same service in 2014. Similarly, a VPN-server hosting on average cost $22 in 2011 but in 2014 such a service could be bought for only $15 (Goncharov, 2014: 16–18). These services and products are easily accessible on various forums that are created with the intention to buy or sell hackers' wares. Max Goncharov (2012), an expert from Trend Micro, has even developed a list of the ten most popular forums used for these illegal purposes, including antichat.ru, xeka.ru and carding-cc.com as the top three. Goncharov (2014) further explains the tricky nature of the forums, as the number of Russian-speaking underground portals and forums has grown in recent years. From time to time, they have to be removed; however, the most popular ones simply change their domain names and host service providers while keeping their devoted customers. Goncharov also estimates that the most visited forums can have up to 20,000 loyal members.

From the above-mentioned conditions and developments, it is apparent that Russian-speaking cyber crime has recently experienced a dynamic transformation from a more quantitative model based on a chaotic structure to the one that reflects its broader stabilisation and professionalisation. This development further contributes to the strengthening of the position of Russian-speaking cyber crime on the global market.

Moreover, it appears that the long standing Soviet-era tradition of highly talented and technically educated individuals, so indispensable for the cyber criminal business, will be carried on even further into the foreseeable future. The continuing trend of putting emphasis on technical education in countries of the post-Soviet area is still substantial today. It comes as no surprise that Russian teams won the prestigious ACM International Collegiate Programming Contest (ACM-ICPC) six times in the past 10 years. ACM-ICPC is the oldest and most prestigious programming competition in the world, which annually features teams of three students from more than 2,300 universities from 91 countries, who compete in broad ranges of hacking and programming abilities. Moreover, the Russians confirmed their dominant position in the competition's 2014 round held in Ekaterinburg when three teams coming from universities in St. Petersburg and Moscow won 1st, 2nd and 9th place. Other Russian-speaking hackers from outside of the Russian Federation, however, do not fall far behind, as Belarusians and Ukrainians tend to be placed among the top finalists as well.[4]

One could assume that this talented and educated youth finds its place in global IT corporations that often have branches in big cities across the region. Two problems can be identified within this context. Firstly, a counter-argument can be made through a simple market calculation, as the supply of well-educated individuals might significantly exceed the demand of the IT companies. Secondly, a great drawback is that in comparison to their Western counterparts, Russian-speaking cyber experts are very poorly paid in exchange for their knowledge and skills. If the high price of living in cities such as Moscow or St. Petersburg is also taken into account, one can hardly wonder as to why such young individuals are turning their backs on legal regulations and entering the ranks of cyber criminals. Therefore, it appears that the human potential of the present generation of highly technically educated individuals assures the continuation of the cyber criminal trend further into the future.

Legal Loopholes and Relationship with Political Elite

The last argument which generally supports the idea that Russian-speaking cyber crime is successful on the global market is linked to the weak legal enforcement and supposed political backing of organised crime. The absence of efficient laws on cyber crime in the post-Soviet territory has been a significant drawback since the first roots of the illegal business became obvious in the 1990s. The weakness oflegal enforcement in Russia has various elements which may be addressed to support the fight against cyber crime.

The penalties for crimes committed by means of computer technologies as they are defined in Articles 272, 273 and 274 of Chapter 28 of the Criminal Code of the Russian Federation are generally considered weak (Alperovitch, 2009; Paganini, 2012; Group-IB, 2013). For example, Paragraph I of Article 273 *Creation, Use, and Dissemination of Harmful Computer Programmes* reads:

> [c]reation, dissemination or use of computer programmes or other computer information, which are knowingly intended for unsanctioned destruction, blocking, modification or copying of computer information or for balancing-out of computer information security facilities shall be punishable by restraint of liberty for a term of up to four years, or by compulsory labour for a term of up to four years, or by deprivation of liberty for the same term with a fine in the amount up to 200 thousand roubles, or in the amount of a wage/salary or any other income of the convicted person for a period up to 18 months (WIPO, 2014).

[4] For more details see the official website of ACM International Collegiate Programming Contest http://icpc.baylor.edu/ and the official website of the year 2014 http://www.icpc2014.ru/en.

Similarly, Paragraph III of Article 272 on illegal access to computer information states that the punishment of such a criminal activity

> committed by a group of persons by previous concert or by an organised group, or by a person through his or her official position shall be punishable with a fine in the amount of up to 500 thousand roubles, or in the amount of the wage or salary or any other income of the convicted person for a period of up to three years with deprivation of the right to hold specified offices or to engage in specified activities for a term of up to three years, or with restraint of liberty for a term of up to four years, or with compulsory labour for a term of up to five years, or with deprivation of liberty for the same term (WIPO, 2014).

Group-IB (2013: 64–66) provided readers of its report on threat intelligence in Russian-speaking countries for the year 2012 and first-half of 2013 with a brief list of examples of cyber criminals comparing their sentences for illicit activities committed in Russia, the U.S., the UK, and China. This short overview illustrates that common punishment in Russia in comparison with other countries is rather moderate, usually amounting to short prison terms or small fines. It seems that the cyber criminals thus do not have to fear serious punishment. In recent years there has been an increased adoption of legal amendments with some positive tendencies towards increasingly severe penalties and aggravating circumstances in the Russian Criminal Code regarding cyber crime. However, critics claim that the amendments to Chapter 28 were not created with enough consultation with experienced law enforcement authorities, creating potentially controversial issues in the Criminal Code. In addition, the language and wording of the current laws on cyber security is not clear enough since various terms such as "computer information" often do not reflect their nature in full (Group-IB, 2011).

Other countries also emphasise the lack of training of Russian law enforcement personnel concerning key cyber security issues (Paganini, 2012). Law enforcement would be significantly improved if training programmes on federal and regional levels were organised. The programmes should address the training of all agencies involved in the cyber crime persecution process, ranging from the judicial and prosecutorial sector to the investigation of illicit activities. This training would not only contribute to the strengthening of domestic law enforcement but could also slowly contribute towards international cooperation.

The borderless nature of cyber space requires involved countries in which illegal cyber activities are committed to take necessary legislative measures on an international level together. Therefore, there is an obvious need for enhanced international cooperation on the issue of crime in cyber space. In this light, Moscow might for instance reconsider signing the Budapest Convention on Cyber Crime under the Council of Europe's auspice or encourage the development of a new document which would establish the framework for coordination of international persecution of cyber crime. Russia has recently expressed a general interest in greater cooperation with international law enforcement agencies. However, as Troels Oerting from Europol points out, this progress is likely to be significantly hindered or even put on hold by the current development on the international stage of the Ukrainian crisis and the subsequent sanctions imposed by the E.U. and the U.S. against Russia (Brewster, 2014).

Despite the adoption of positive developments by the Russian State Duma in recent years in the form of amendments to Chapter 28 on cyber crime of the Criminal Code of the Russian Federation, the legal enforcement and the force of penalties still requires improvement in order to meet the standards in other developed countries. The proper exercise of the law is further severely hindered by the apparent insufficient training of involved law enforcement entities and the lack of international cooperation between the Russian domestic authorities and international bodies in charge of cyber criminal investigation. These conditions and gaps in the legal framework provide cyber criminals with enough manoeuvring space for their illicit activities.

The argument of weak legal enforcement is closely linked to the alleged reciprocally beneficial relationship between the political elite and the Russian-speaking cyber underworld. Kyle Wilhoit from Trend Micro states that "hackers only really get prosecuted when they attack targets inside Russia" (Plesser, 2014). As long as the hackers' illegal activities are aimed at targets overseas, the authorities let them do their business and possibly use their services for their own interest in return. Jeffrey Carr (2012: 123 and 130) argues that the Russian government has infiltrated structures of organised crime in certain regions by providing protection in return for favours. These might vary from earning money to promoting state interests. He further claims that although the relationship between government and cyber crime is not well documented, it is simply a continuation of the well-known link between the political establishment and organised crime transferred to the area of cyber space.

Previous incidents have confirmed potential indications of this alleged cooperation. For instance, the Russian parliamentary elections in 2011 and presidential elections in 2012 demonstrated that politically motivated DDoS attacks blocking out blogs or media sites of political opponents have recently gained increased popularity (Essers, 2012). More importantly, the cyber attack on Georgia during the Russian military campaign in August 2008 is commonly mentioned. Although no direct evidence can be provided, a combination of factors suggests there is a relationship between the government and the cyber underworld. According to the U.S. Cyber Consequences Unit report (2008), the attack was coordinated and supported by Russian criminal organisations since various web servers and addresses as well as botnets employed in the attack were ones that had been previously used by criminal groups. Moreover, the organisers of the cyber campaign had deep knowledge of the Kremlin's military attack and the timing of the operation on the ground. This might suggest that the cyber attackers benefitted from close cooperation with state organs (U.S.-CCU, 2008; Rutherford, 2009).[5] Therefore, further general investigation into the supposed relationship between the government and illegal cyber groups is essential in order to support this argument.

The Case of the Russian Business Network

To illustrate some of the recent developments in practice, the case of the Russian Business Network (RBN), "the baddest of the bad" (The Economist, 2007), can serve as a clear example of a criminal cyber organisation operating in the time of market transformation. The roots of the RBN can be traced to the second half of the 1990s. As Roland Heickerö (2010) claims, its structures developed into a more centrally organised group in 2002, while also increasing and broadening its portfolio of criminal activities. Shortly afterwards, the RBN started building its criminal prestige as, for instance, when it was accused of an attack on the U.S. Department of Defence and Russian Department of the Treasury in 2003. Heickerö (2010) believes that when the RBN was reaching the peak period in its activities between 2006 and 2007, it was involved in almost 60 percent of all cyber crime.

As a cyber crime service provider, the RBN was an intermediary for a full range of malicious activities in cyber space ranging from malware hosting, spamming, and phishing to pornography and gambling (Bizeul, 2007). The profit of the RBN's services, however, widely differed; for example, a single fraud business called Rock Phish dishonestly obtained a huge number of internet users' personal financial data in 2006, earning up to $150 million in profit. The case of Rock Phish also further illustrates that the RBN was a stable and living criminal organism. After the Rock Phish fraud was committed, the National Bank of Australia took the necessary measures against the criminal group through the Australian anti-phishing group. The RBN quickly reacted by crashing the bank's homepage for three days (The Economist, 2007).

Nevertheless, the well-organised and efficient structure of the RBN might not have been the only reason for its success. As different resources have claimed, the RBN establishment was closely linked with Russian political elite that could provide a certain level of protection. For example, David Bizeul (2007) stated that a hacker called Flyman, supposedly a key figure in the RBN leadership, had strong political protection since he was generally known for his illegal activities that he has pursued while avoiding serious sentences. Jeffrey Carr (2012: 125) goes even further when he narrates the

[5] One might think in the similar direction about the notoriously known politically motivated cyber attacks against Estonia from 2007. The cyber campaign against Georgia, however, is more transparent in this sense since it was waged simultaneously to and in coordination with the conventional attacks on ground.

following story in his book. After the RBN had received enough attention from media coverage, FBI officials arrived to Russia in order to seek the assistance of their colleagues from the Russian Federal Security Services (FSB) to discuss possible countermeasures against the cyber crime group. According to Carr, the FSB officials left the meeting for half an hour and upon their return assured the FBI officers that there must be a misunderstanding since RuNet[6] did not include any of the domains which the FBI had mentioned. Once the FBI undertook an immediate investigation, it realised that the public domains which they had linked with the RBN were moved to new IP addresses.

The RBN publicly vanished in the autumn of 2007; however, according to some sources, they have still been operating in secret (Kabay and Guinen, 2011c; Carr, 2013). For instance, an extraordinary attack on the WorldPay system of The Royal Bank of Scotland (RBS) in November 2008 is often attributed to the RBN. The cyber criminals hacked the WorldPay's sophisticated encryption system that was used on payroll debit cards and then used the stolen data in order to create fake ATM debit cards. Subsequently, these cards were used to withdraw the maximum amounts of money permitted with the original debit cards. The criminal group stole about $9 million from over 2,100 ATMs in almost 300 cities all over the world in less than 12 hours. In this case justice worked swiftly, as less than two years later one of the accused hackers, Sergei Tsurikov from Tallinn in Estonia, was extradited to the U.S. On the other hand, Viktor Pleschuk, who was allegedly the boss of the criminal ring, received just a four-year suspended sentence from a Russian court and had to financially compensate RBS WorldPay (Kabay and Guinen, 2011c).

While there is still no specific evidence regarding the cooperation between the RBN and the state elites or whether the cyber criminal organised group survived and still continues with its illicit activities in cyber space, suspicions still prevail. What is more important, however, is the overall picture RBN's story gives. Its continuous development from the early stages to the well-structured, sustainable and reactive organism features are all signs of the above-described elements and conditions necessary for a successful cyber criminal business. Of course, the alleged relationships with political elites might have played its role; however, the case of the RBN can also illustrate that it is unlikely that the political establishment would have gotten involved if it had not been professionalised first.

Conclusion

Russian-speaking cyber crime has recently gone through a dynamic transformation, resulting in a more qualitatively focused and stable model. The importance of criminal ac-

[6] The term RuNet, also known as Russian Internet, refers to the Internet written in Russian language. It does not necessarily relate only to the Internet in Russia but also to other countries where Russian is widely spoken.

tivity coming from post-Soviet territory has been proved by its dominant share in the global cyber crime market. This study has examined the main arguments that are most often discussed in relation to the success of Russian-speaking organised crime in cyber space. The paper has identified three broad arguments. These are the roots of cyber crime and its development in the immediate post-Soviet era, the recent transformation and professionalisation and loopholes in Russian law and the alleged relationship with state apparatus.

Our analysis suggests that there is not one single prevailing factor behind the dominant position of Russian-speaking cyber crime. The online illegal activity has its roots in the 1990s and early 2000s supported by a power vacuum, high unemployment of technically educated individuals and a promising financial return. Later on in the 2000s, the criminal structures developed into a more organised and highly sustainable organism capable of conducting a wide range of illegal activities, as was reflected in the case of the RBN. The stabilisation of the market has also brought about the relatively low prices of online criminal services and products. Weak penalties and legal loopholes in the Russian Criminal Code further motivate criminal organisations in their activities. A certain role might have also been played by the alleged relationship between the Russian-speaking cyber underworld and Russian state elites. Nevertheless, further investigation into the speculative link between these two entities needs to be undertaken since no direct evidence has been revealed thus far. For all the discussed reasons, this paper argues that the peculiar strength of Russian-speaking cyber crime must be perceived as the result of a combination of various factors and conditions that gradually developed after the dissolution of the USSR on its territory.

Acknowledgement

The author would like to express her gratitude to Dr Tomáš Weiss for his guidance in the final stage of the research, to professor Thomas Rid for his comments on the initial version of the manuscript, and, finally, to King's College London and Charles University for their creative environment.

References

ACM-ICPC. Retrieved from: http://icpc.baylor.edu/ (accessed 16 December 2014).

Alperovitch D (2009) *Fighting Russian cybercrime mobsters: report from the trenches.* Presented at Black Hat USA 2009. Retrieved from: http://www.blackhat.com/presentations/bh-usa-09/ALPEROVITCH/BHUSA09-Alperovitch-RussCybercrime-PAPER.pdf (accessed 12 November 2014).

BBC (2014) Only 100 cybercrime brains worldwide says Europol boss. October, 10. Retrieved from: http://www.bbc.com/news/technology-29567782 (accessed 15 December 2014).

Bizeul D (2007) Russian Business Network study. *Bizeul.org*. November, 20. Retrieved from: http://www.bizeul.org/files/RBN_study.pdf (accessed 12 November 2014).

Brewster T (2014) Trouble with Russia, trouble with the law: inside Europe's digital crime unit. *The Guardian*. April, 15. Retrieved from: http://www.theguardian.com/technology/2014/apr/15/european-cyber-crime-unit-russia (accessed 16 December 2014).

Carr J (2012) *Inside cyber space: mapping the cyber underworld*. 2nd ed. Sebastopol: O'Reilly.

Carr J (2013) RBN connection to Kaspersky's Red October espionage network. *Jeffrey Carr's blog*. January, 15. Retrieved from: http://jeffreycarr.blogspot.co.uk/2013/01/rbn-connection-to-kasperskys-red.html (accessed 10 November 2014).

De Carbonnel A (2013) Ex-Soviet hackers play outsized role in cyber crime world. *Reuters*. August, 22. Retrieved from: http://www.reuters.com/article/2013/08/22/net-us-russia-cybercrime-idUSBRE97L0TP20130822 (accessed 15 December 2014).

Essers L (2012) Russian cybercriminals earned $4.5 billion in 2011. *Computer World*. April, 24. Retrieved from: http://www.computerworld.com/s/article/9226498/Russian_cybercriminals_earned_4.5_billion_in_2011 (accessed 11 November 2014).

Glenny M (2012) *Dark Market*. London: Vintage Books.

Global Programming Championship. The 2014 ACM International Collegiate Programming Contest World Finals. Retrieved from: http://www.icpc2014.ru/en (accessed 16 December 2014).

Goldman D (2011) The Cyber mafia has already hacked you. *CNN Money*. July, 27. Retrieved from: http://money.cnn.com/2011/07/27/technology/organized_cybercrime/index.htm (accessed 13 November 2014).

Goncharov M (2012) *Russian underground 101*. Research Paper Trend Micro. Retrieved from: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf (accessed 11 December 2014).

Goncharov M (2014) *Russian underground revisited*. Research Paper Trend Micro. Retrieved from: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf (accessed 11 December 2014).

Group-IB (2011) *State and trends of the Russian digital crime market 2011*. Research Paper Group-IB. Retrieved from: http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf (accessed 12 December 2014).

Group-IB (2013) *Threat intelligence report 2012-2013 H1*. Research Paper Group-IB. Retrieved from: http://report2013.group-ib.com/ (accessed 16 December 2014).

Group-IB (2014) *The Hi-Tech crime trends 2014*. Research Paper Group-IB. Retrieved from: http://report2014.group-ib.com/ (accessed 16 December 2014).

Heickerö R (2010) *Emerging cyber threats and Russian views on information warfare and information operations*. Stockholm: Swedish Defence Research Agency.

Hoffman S (2009) BlackHat USA 2009: Russian's organized crime heritage paved way for cybercrime. *CRN*. July, 29. Retrieved from: http://www.crn.com/news/security/218800207/blackhat-usa-2009-russians-organized-crime-heritage-paved-way-for-cybercrime.htm?itc=refresh (accessed 13 November 2014).

Hold Security (2014) *You have been hacked!*. August, 5. Retrieved from: http://www.holdsecurity.com/news/cybervor-breach/ (accessed 16 December 2014).

Kabay M E and Guinen B (2011a) The Russian cybermafia: beginnings. *Network World*. March, 21. Retrieved from: http://www.networkworld.com/newsletters/sec/2011/032111sec1.html (accessed 10 November 2014).

Kabay M E and Guinen B (2011b) The Russian cybermafia: Boa Factory & CarderPlanet. *Network World*. March, 23. Retrieved from: http://www.networkworld.com/newsletters/sec/2011/032111sec2.html (accessed 10 November 2014).

Kabay M E and Guinen B (2011c). The Russian cybermafia: RBN & the RBS WorldPay attack. *Network World*. March, 28. Retrieved from: http://www.networkworld.com/newsletters/sec/2011/032811sec1.html (accessed 10 November 2014).

Metzger T (2010) Alleged cybercriminal, cartoonist arrested in France. *CreditCards.com*. August, 12. Retrieved from: http://www.creditcards.com/credit-card-news/carderplanet-badb-data-thief-cybercriminal-arrested-1282.php (accessed 10 November 2014).

Munns D (2008) The Secret history of CarderPlanet.com and Dmitry Ivanovich Golubov. *CreditCards.com*. May, 8. Retrieved from:

http://blogs.creditcards.com/2008/05/secret-history-of-carderplanet.php (accessed 10 November 2014).

Mwangi L (2014) The Shocking state of cybercrime in Russia. *Security Gladiators.* October, 16. Retrieved from: http://securitygladiators.com/2014/10/16/shocking-state-cybercrime-russia/ (accessed 9 November 2014).

Nusca A (2012) 7 things you didn't know about Russia's cybercrime market. *ZDNet.* November, 5. Retrieved from: http://www.zdnet.com/article/7-things-you-didnt-know-about-russias-cybercrime-market/ (accessed 13 November 2014).

Official website of the Internet Party of Ukraine. Retrieved from: http://ipu.com.ua/ (accessed 12 December 2014).

Paganini P (2012) Russian cybercrime, not only a localized threat. *Security Affairs.* April, 25. Retrieved from: http://securityaffairs.co/wordpress/4686/cyber-crime/russian-cybercrime-not-only-a-localized-threat.html (accessed 9 November 2014).

Paganini P (2013) Red October, RBN and too many questions still unresolved. *Security Affairs.* January, 17. Retrieved from: http://securityaffairs.co/wordpress/11779/cyber-crime/red-october-rbn-and-too-many-questions-still-unresolved.html (accessed 12 November 2014).

Perlroth N and Gelles D (2014) Russian hackers amass over a billion Internet passwords. *New York Times.* August, 5. Retrieved from: http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=1 (accessed 16 December 2014).

Plesser B (2014) Skilled, cheap Russian hackers power American cybercrime. *NBC News.* February, 5. Retrieved from: http://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-american-cybercrime-n22371 (accessed 15 December 2014).

Rutherford M (2009) Russian mob aided cyberattacks on Georgia. *C-Net.* August, 18. Retrieved from: http://news.cnet.com/8301-13639_3-10312708-42.html (accessed 14 November 2014).

Steadman I (2012) The Russian underground economy has democratised cybercrime. *Wired.co.uk.* November, 2. Retrieved from: http://www.wired.co.uk/news/archive/2012-11/02/russian-cybercrime (accessed 13 November 2014).

Stilgherrian (2012) Cybercrime and the Russian mob. *ZDNet.* March, 5. Retrieved from: http://www.zdnet.com/cybercrime-and-the-russian-mob-1339333020/ (accessed 13 November 2014).

The Economist (2007) A Walk on the dark side. August, 30. Retrieved from: http://www.economist.com/node/9723768?story_id=9723768 (accessed 10 November 2014).

U.S. Department of Justice (2010) *Alleged international credit card trafficker arrested in France on U.S. charges related to sale of stolen card data.* August, 11. Office of Public Affairs. Retrieved from: http://www.fbi.gov/atlanta/press-releases/2010/at081110.htm (accessed 11 November 2014).

U.S.-CCU (2008) *Overview by the U.S.-CCU of the cyber campaign against Georgia in August of 2008.* Special report U.S. Cyber Consequences Unit. Retrieved from: http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf (accessed 14 December 2014).

World Intellectual Property Organization (WIPO). The Criminal Code of the Russian Federation. Retrieved from: http://www.wipo.int/wipolex/en/text.jsp?file_id=277023 (accessed 14 December 2014).