Russian Cybercrime: A Profile and Comparison

As an increasing number of human activities take place in the digital sphere, criminal activity utilizing technological means is also beginning to flourish. After the end of the Cold War, tensions remained between the Russian Federation and the former Soviet republics on the one hand, and Western Europe and the United States on the other. Although many of the sentiments and conflicts from that period remain, now the arenas for these conflicts have shifted from missile silos and propaganda programs to cybercrime and cyber-terrorism. Cybercrime rapidly became the most popular way for individuals and governments to target their enemies for economic and political reasons. The rise of cybercrime is not a secret to anyone; and governments around the world now recognize the magnitude of cyber threats, pouring resources into defending themselves from organizations such as WikiLeaks and the hacker group Anonymous.

This paper aims to prove that the United States is falling behind the Russian Federation and other Russian speaking countries in the struggle for cyber-dominance, and that one of the primary reasons for this lapse is the United States’ smothering of entrepreneurship and innovation in young programmers through law enforcement and legislation. The paper will reveal the particular gaps and weaknesses of the United States, which have been exploited by hackers and criminals from across the globe. These hackers live in countries where they are not only allowed to experiment and perfect their hacking skills but, in fact are often encouraged by their respective governments to do so. For example, the government of the Russian Federation actively recruits educated programmers from universities as well as self-educated successful
hackers to deal with domestic issues, such as the organization of protests and anti-government meetings, as well as international matters of intelligence and even espionage. Through an analysis of Russian and American views on the issue of cybercrime, the longstanding traditions that influence these views, as well as each government’s public and private response to the domestic presence of skilled cybercriminals, I will show that the unbounded success of Russian-speaking hackers on the global scale and their innovative ability to consistently defeat their opposition is a product of the hackers’ national culture and the freedoms that they are granted.

Before discussing the impact of modern cybercrime and the differences between its Russian and American variants, it is important to understand the nature of cybercrime itself. Cybercrime can be defined as “criminal activities conducted in cyberspace by means of Internet technology”¹ and can be divided into two categories: “1) those involving unauthorized access to data and systems for criminal purposes, and 2) those involving fraud, falsification, diversion of funds, obtaining illicit content, or defamation via online services.”² Furthermore, it should be noted that, although cybercrime can be labeled as one of the newest waves in organized crime and does possess some entirely novel intricacies, “cybercrime is not an altogether new breed of crime… the crimes carried out by this new breed of criminal often reflect emotions as old as humankind.”³

Cybercrime is a relatively new and rapidly changing phenomenon, and for this reason it is defined somewhat differently in different countries. In spite of specialized definitions, however, the general idea of cybercrime remains relatively consistent. A. Shchetilov identifies three types of cybercrime in Russia: “illegal access to information stored in global computer

¹ Federal Research Division, 1.
² Ibid.
³ Brenner, vii.
networks; crimes using information in forms other than those that are computer-based; and crimes involving the distribution of harmful computer programs.”

In China, Sun Tianzhy and Cao Peizhong define cybercrime as “those crimes that use computers as the main tool, as well as those that have computer assets as their primary target.” In sum, cybercrime consists of either stealing information over the Internet or disrupting the use of a certain website or online service. While the public is quite familiar with certain types of infringements, such as “spam,” in the context of email, general public knowledge of cybercrime is relatively low. In turn, knowledge and familiarity with how cybercrime is committed is even more rare.

The five most common tools and methods utilized in cybercrime are keylogging, distributed denial of service (DDoS), pharming, phishing, and botnets. Keylogging is defined as “using software or devices to secretly monitor and record keystrokes, enabling espionage activities or the harvesting of personal data,” and it was among the first methods to be widely used by cybercriminals.”

Keylogging records each key pressed on a keyboard in sequence, allowing the owner of the keylogger to record every character typed, regardless of whether or not the character is displayed on the screen. Keylogging is also one of the most varied forms of cybercriminal activity. It includes programs that simply record all keystrokes in a text document, as well as more innovative devices, such as acoustic keyloggers, which record the sound of fingers typing on a keyboard and then, through analysis of these sounds, determine which key was pressed and in what order. Without any explicit application, the potential for keylogging is essentially endless, enabling anything from identity or password theft to government agency remote access. However, most applications of keylogging occur on a personal level, and Vanessa

---

5 Ibid., 2.
6 Ibid.
Vitaline “identifies keylogging as a general threat.”\textsuperscript{7} Keyloggers, much like Torrent clients, remain prominent because they are circulated by legitimate and malicious sources alike. According to the security website BullGuard.com, one of the reasons keyloggers continue to grow in sophistication is because some companies actually promote keyloggers “for benign purposes like allowing parents to monitor their children’s whereabouts on the Internet.”\textsuperscript{8} Like peer-to-peer downloading services, which are not innately illegal, keyloggers illustrate how a perfectly legal technology may be utilized for illegal purposes.

The second type of cybercrime is a distributed denial of service (DDoS) attack, or “inundating computer system resources with tasks sufficient to render them unavailable to authorized users.”\textsuperscript{9} DDoS attacks basically simulate or create enough traffic to a particular computer or network resource that it then becomes unavailable to legitimate users. In most cases, a DDoS attack simply aims to make a website or service inaccessible. DDoS attacks are one of the most potent and popular modern methods of cybercrime. They are used heavily by the hacker group Anonymous, for example, which was involved in a DDoS of the website of the International Federation of the Phonographic Industry (IFPI) in 2009.\textsuperscript{10} Due to the enormous potential of rendering a website or online service completely inaccessible, Vitaliy Vekhov confirms “the rapid growth, over the past 10 years, of DDoS crimes.”\textsuperscript{11} DDoS crimes have become increasing powerful as more and more financial institutions and civil services rely on the Internet and computer systems, which can then be targeted by criminal means such as a DDoS attack and rendered useless.

\textsuperscript{7} Ibid., 3.
\textsuperscript{8} BullGuard.
\textsuperscript{9} Federal Research Division, 2.
\textsuperscript{10} Leyden.
\textsuperscript{11} Federal Research Division, 3.
Additional cybercrime methods include pharming—“directing traffic from a legitimate Web site to a site controlled by a criminal hacker”\(^\text{12}\) and thus allowing the potential theft of personal information or the promotion of a certain ideal or information—and phishing—“illegally accessing an individual’s financial data to capture online banking and financial information”\(^\text{13}\) most often by way of email or instant messaging. Phishing and pharming as well as keylogging techniques represent a more passive movement in cybercrime as they seek to either steal information or control what an Internet user views. DDoS attacks, on the other hand, have the potential to lead to physical harm and property damage when the scope is widened to the control of power grids or Air Traffic Control Towers.

The newest and perhaps most powerful tools at cybercriminals’ disposal are botnets —“networks of infected machines, usually managed by a single command center, that are capable of causing serious damage to networked systems and enabling large-scale identity theft.”\(^\text{14}\) A botnet consists of a collection of computers that have been compromised, most often by a piece of malware, and then used as “bots” to carry out other tasks. Botnets have many different applications, but they are most often used to conduct very large DDoS attacks, using each “bot” as simulated traffic. They allow the originator of the attack to not only utilize the power of their machine, but of every machine they are able to convert into a “bot.”

Botnets and other cybercrime methods illustrate that “cybercrimes, uniquely different from traditional crimes, are often harder to detect and prosecute”\(^\text{15}\) and, thus, present a unique challenge to modern nations and individuals attempting to maintain tight security. Chen Junjing

\(^{12}\) Ibid., 2.
\(^{13}\) Ibid.
\(^{14}\) Ibid.
\(^{15}\) Ibid., 3.
“concludes that these [cyber] crimes are more widespread than traditional crimes and are increasing at a faster rate... Furthermore, cybercrime does greater damage to society than traditional crime and is more difficult to investigate.”¹⁶ Cybercrime mirrors a broader societal trend in which governments, corporations, and individuals rely more and more on technology. With the increase in cybercrime, governments and law enforcement agencies around the world must adapt to meet its evolving demands. This process, however, is slow and onerous because cybercrime presents a series of unique challenges that are not present in traditional crime.

First, cybercrime can be perpetrated both locally and remotely, the latter constituting “the majority of computer crimes”¹⁷ according to A. I. Zhurba, a Ukrainian researcher of cybercrime. N. N. Akhtyrskaya further states that “the process of investigating these [cyber] crimes is typically fragmentary, complex, and fraught with false leads.”¹⁸ In addition to being difficult to investigate, the scope of damage a particular act of cybercrime can range from hindering “the judiciary, . . . radio, and television broadcasters; and medical care providers” to “the sabotage of critical infrastructure, such as the supply of electricity or water,” according to a 2008 report by the Swedish Emergency Management Agency.¹⁹ Governments, therefore, need to pay particular attention to the trends of cybercrime, such as the “rapid growth of phishing since 2000”²⁰ discussed by Rodion Nasakin, and address the fact that “perpetrators of cybercrime are often more sophisticated in their methods than are the law enforcement agencies that investigate them.”²¹ Vanessa Vitaline, writing about cybercrime in France, “concludes that, despite

---

¹⁶ Ibid.
¹⁷ Ibid.
¹⁸ Ibid., 4.
¹⁹ Ibid., 4–5.
²⁰ Ibid., 3.
²¹ Ibid., 11.
countermeasures taken by governments and police authorities, cybercrime continues to grow exponentially.”¹² Vladimir Golubev and Timofey Saymarly at the Center for Research on Problems of Computer Crime in Ukraine provide an additional warning that “western countries currently have inadequate personnel trained to combat this type of [remote cybercrime] attack, a lack that they must remedy.”¹³ Remote attacks constitute the majority of all cybercrime and “are more dangerous than direct attacks, because [they] may have catastrophic global consequences.”¹⁴

Cybercrime is a relevant and pertinent issue for law enforcement around the world. Understanding the main methods and tools behind these crimes is important, but in order to accurately describe the nuance of international cybercrime, it is also necessary to discuss the differences between approaches to cybercrime in the United States and in Russia, as well as the effect of these approaches on national security and competitiveness.

In order to understand how cybercrime originating in Russia and other former Soviet countries relates to the United States, one must first determine the character of such cybercrime. In 2010 the entirety of global cybercrime garnered revenues of seven billion U.S. dollars, according to a presentation done by Group-IB. Out of that 7 billion, 1.3 billion dollars (approximately 19%) originated in Russia and 2.5 billion dollars (approximately 36%) came from Russian-speaking countries.¹⁵ In their report, members of Group-IB present the costs of various services including the “guaranteed hack of a mailbox (Yandex, Mail, Rambler, Gmail)” starting at 1500 rubles (approximately $50 USD) as well as a “mobile phone bug” starting at

---

¹² Ibid.
¹³ Ibid., 35.
¹⁴ Federal Research Division, 35.
¹⁵ Lipovsky, Matrosov, and Volkov.
around $5000. What makes such a wide array of services, illegal services, so readily available and affordable from Russian sources? Danny Lieberman, in an article published on the website Infosec Island, describes how “Russia has outstanding universities with world class specialists in mathematics, physics, and computer science... Russia, very simply, has very, very good raw material for hacking” and goes on to cite the entry on Wikipedia.com dedicated to Russian mathematicians. Lieberman adds, “having great talent is a great start for getting world-class results in any field.” Yevgeny Kaspersky, co-founder of the Kaspersky Lab, which specializes in computer and Internet security, describes “Russia as a nation of ‘super hackers.’” Kaspersky attributes Russian hacking prowess to “Russia’s technical education,” provided by certain universities around the country that specialize in teaching hacking—including the Institute of Cryptography, Telecommunications and Computer Science, which was co-sponsored by the Russian Ministry of Defense and the KGB, and a college in the Siberian city of Tomsk, where one in every five residents is a student. However, such a large talent pool does not necessarily encourage its members to participate in cybercrime.

Accordingly to a publication by the Center for Strategic and International Studies, after the Federal Agency for Government Communications and Information (FAPSI) disbanded in 2003, “many of the employees were recruited by hacker groups, while others joined the Russian security service successor of the KGB, the FSB.” To offer some insight into why young, educated, programmers would seek criminal work instead of legitimate occupations, Mark Galeotti, director of the Organized Russian and Eurasian Crime Research Unit at Keele

---

26 Lieberman.
27 Rainsford.
28 The Guardian.
29 Rifkind.
University, states that “for a lot of the Russian techies [crime] became very lucrative,” and criminal organizations “began to recruit top graduates from universities who could earn ten times what they would get in Russia and twice what they would get in the West.” With an ever-increasing number of young professionals graduating from professional schools with aspirations to work in the field of technology, one writer for TheAge.com.au draws a parallel between the creators of organizations such as the Russian Business Network (RBN) and the “young entrepreneurs from similar backgrounds [who] launched Google and eBay.”

In the struggle to find employment, large numbers of educated and skilled programmers in Russia end up working independently as hackers or cybercriminals, or for companies and organizations such as the Russian Business Network (RBN). The RBN is a Russian cybercrime syndicate that Wikipedia describes as “a multi-faceted cybercrime organization, specializing in and in some cases monopolizing personal identity theft for resale.” Utilizing tactics similar to those of the traditional mafia, the Russian Business Network does not always maintain a concrete identity. The Economist wrote in 2007: “in one sense, RBN (Russian Business Network) does not exist. It has no legal identity; it is not registered as a company.” Furthermore, much like the secretive crime syndicates of the past, “its senior figures are anonymous, known only by their nicknames... [I]ts web sites are registered at anonymous addresses with dummy e-mails.” So what, then, is the RBN? VeriSign, a prominent Internet security firm, identifies the network as “a for-hire service” that “cater[s] to large-scale criminal operations,” offering a range of services

---

30 Warren.
31 Ibid.
32 Wikipedia.
33 The Economist.
such as spamming, phishing, and bot-herding.\textsuperscript{34} The RBN occasionally works on a very large scale. For example, in 2006 it conducted one operation known as “Rock Phish,” which earned an estimated $150 million. VeriSign sets the organization apart from other, less reputable websites and Internet organizations by emphasizing that the “RBN is solely criminal,” even naming it “the baddest of the bad.” After hacking into an RBN computer, VeriSign operatives discovered that “every major Trojan in the last year links to RBN,” accounting for 30,000 entries of stolen data. The organization’s secrecy is as extensive as the scope of its operations—the number of employees can only be estimated, and only the most extremely powerful or vocal members of the group can be individually identified. “Flyman,” for example, is the alias of the head of the RBN, whose uncle is believed to be a senior politician in Saint Petersburg.

As with studies of other, more traditional criminal enterprises, the funding and support of cybercriminal organizations warrants scholarly attention. How and why do organizations such as the RBN flourish in Russia? In an interview with BBC reporter Sarah Rainsford, a former Russian hacker known only as “Andrei,” who started hacking at the age of 14, describes hacking as an intellectual exercise: “it’s like when you have a maths problem… you don’t know what tools to use, you know nothing. But you want to master it, understand it, and then use that knowledge in the future.”\textsuperscript{35} Although Andrei voices the opinion of many young computer programmers around the world, for some reason such hackers have become powerful and active in Russia and other Russian-speaking countries, but not in the United States. One student in Tomsk, Alexei, refers to hacking as “an art”\textsuperscript{36} and another, Zheniya, explains how requests for him to use his hacking knowledge quickly escalated from friends and relatives wanting to spy on

\textsuperscript{34} Ibid.  
\textsuperscript{35} Rainsford.  
\textsuperscript{36} Ibid.
neighbors, to “people who wanted me to infect a large number of users who were clients of a certain bank, so they could use their computers to transfer money.” These reports from Russian hackers indicate that Russia provides an environment that encourages aspiring programmers to “join the ranks of Russia’s hackers for hire,” as Rainsford puts it.

Young Russian hackers such as Zheniya and Alexei represent the cream of the crop of the hacking world, “consistently finish[ing] among the top three teams in international information protection contests.” Members of organizations such as the Russian Business Network reside at the top of the cyber food chain. The Economist notes that, “despite the attention it is receiving from Western law enforcement agencies, RBN is not on the run. Its users are becoming more sophisticated.” The majority of legal pressure on these hackers comes from the law enforcement agencies of Western countries, and even these efforts fail to halt or mitigate the illegal activities of the RBN. Not only are organizations like RBN not intimidated by Western law enforcement, they even retaliate against such efforts. In October 2006, when the National Bank of Australia moved against RBN’s “Rock Phish,” “RBN-based cybercriminals replied by crashing the bank’s home-page for three days.” Although the RBN may appear to be behind the majority of cybercrime, Dancho Danchev stresses: “the RBN is the tip of the iceberg... What about the hundreds of thousands other not so well known malware serving netblocks?”

As a large number of powerful and educated Russian hackers continue to find employment in hacking and committing cybercrimes, one question inevitably arises: what effect,

---

37 Ibid.
38 Ibid.
39 Ibid.
40 The Economist.
41 Ibid.
42 Danchev.
if any, has this phenomenon had on the United States? Is the United States prepared to deal with these syndicates? Perhaps American programmers are already working clandestinely for the US government, have less potential, or simply do not exist, but in any case, it is important to note that the majority of well-known hackers and cybercriminals are not American. The founders of the website The Pirate Bay, who have been involved in numerous lawsuits around the world, are Swedish and Finnish. The Pirate Bay is one of the most used torrent resources on the Internet and is actually planning “to launch airborne drones that act as proxy servers” in order to make it more difficult for law enforcement to shut down their website.\textsuperscript{43} The founder of the website Megaupload, Kim Dotcom, who was brought under charges for copyright infringement in January of 2012, is of German-Finnish origin. Perhaps the most well-known hacking group in the United States, Anonymous, maintains its members' anonymity, and Julian Assange, the founder of WikiLeaks, is Australian. The media typically portrays the United States as vulnerable to European and Australian cybercriminals, but the United States actually lags behind much of the world in cyber-capabilities. Delvin Barrett, writing for the Wall Street Journal, explains that “federal law-enforcement officials say they are concerned about cyber-retaliation”\textsuperscript{44} from Anonymous. What more encouraging message could a cybercriminal receive?

What, then, accounts for the disparity between the capabilities of Russian and American hackers? Perhaps the single most important factor affecting an American hacker’s ability to work, experiment, and grow is the controversial and suffocating anti-piracy legislation in the United States. Both legitimate and criminal organizations expressed outrage at the Stop Online Piracy Act (SOPA) from the United States House of Representatives and the Preventing Real

\textsuperscript{43} The Pirate Bay

\textsuperscript{44} Barrett, “Retaliation Fears.”
Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP) from the Senate. In protest, groups such as Anonymous launched cyber-attacks and organizations Google and Wikipedia encouraged a “deluge of phone calls and emails that hammered offices.”45 The presence of this legislation actively hindered the freedom of hackers to develop their skills. Shawn Henry, the FBI’s top cyber investigator, describes the American model of smothering hacking potential as “unsustainable” and, when referring to America’s ability to protect its own assets from computer hackers, adds: “We’re not winning.”46

One of the primary causes of this ineptitude is a failure to recognize and therefore completely understand the character and mentality of cybercriminals. For example, in order to find a definition of the term “fire sale,” one must now search the comments on private websites for its unofficial definition. Wikipedia indicates that the article “Fire sale (attack)” was marked for deletion, because, according to a Wikipedia editor, there is not enough evidence on fire sales to be “worth a separate article.”47 In response to the deletion, a user answered, “Do a search, and you will find the term used.” The editor responded, “I did that. Pretty much everything I found was either a blog (not a reliable source) or a reference to the movie.”48 While looking for accredited opinions on medical treatments or statistical information, a privately owned and run blog may not be the best source. However, when discussing a culture that lives on blogs, chat clients, and forums, labeling a blog as “not a reliable source” is counterproductive. At a time when Wikipedia, the younger generation’s go-to source for information, is deleting content

45 O’Brien.
46 Barrett, “U.S. Outgunned in Hacker War.”
47 JForget.
48 Ibid.
because it is primarily discussed in blogs, readers whose interest is national security must be
cautious and understand the importance of blogs in cybercriminal circles.

In contrast, Russian hackers do not face such restrictive legislation and are not compelled
to act in secret. On the contrary, “some activist groups are not supervised by the secret services,
but rather by the presidential administration.”\(^\text{49}\) According to a report published by Group-IB,
“the dollar-value of online criminal activity conducted by the Russian mafia and other criminal
organizations doubled in 2011.”\(^\text{50}\) Not only are Russian-speaking criminals already ahead of law
enforcement and their counterparts in the West, but they are continuing to flourish, partially as a
result of the lack of adequate Russian legislation: “The Group-IB report blamed lax Russian laws
for the expansion of cybercrime.”\(^\text{51}\) Group-IB officials go on to say that, “while the Russian
government has tried to tighten legislation aimed at preventing and punishing such activity, the
company said more was needed.”\(^\text{52}\) They also suggest that “the Kremlin either controls the
hackers or, more plausibly, turns a blind eye so long as they stop in to help when the government
calls.”\(^\text{53}\)

Cybercrime is a powerful and malicious reality of the modern world, and it is manifested
in such procedures as DoS attacks, phishing, and botnet herding. Russia stands out as a safe
haven for a large, capable, and active hacking community. It is home to many talented and well-
educated young professionals who may lack opportunities for legitimate employment, but are
allowed to practice cybercrime freely. Russia lacks legislation that prohibits or discourages
hacking and, in some cases, the government even supports and finances hackers’ education and

\(^{49}\) Soldatov.
\(^{50}\) Donohue.
\(^{51}\) [Radia].
\(^{52}\) Ibid.
\(^{53}\) Galeotti.
employment. Furthermore, the United States’ competitiveness in hacking is hindered by their devotion of resources to the enforcement of legislation aimed at limiting Internet and hacking entrepreneurship, which discourages talented individuals from developing their valuable skills. By focusing its resources on hackers’ education rather than on strict control of the Internet, Russia has progressed much further and faster than the United States in the increasingly important arenas of hacking and computer programming. According to a report by the Federal Research Division of the Library of Congress, the United States faces “a dilemma in balancing the need to gain access to personal data—both to prevent and to prosecute cybercrimes—with the need to protect the individual privacy and civil liberties.”54 Because the Russian Federation has yet to show that they are ready to legislatively protect civil liberties or prosecute cybercrimes, the United States and other Western powers face increasing numbers of capable Russian hackers.

However, it would not be completely accurate to paint such a bleak picture of the United States’ cyber security or exaggerate the ineptitudes of the U.S. government. It should be noted that “police officers from the UK, Germany, Netherlands, Australia, and other countries work alongside the FBI at the NCFTA [National Cyber-Forensics & Training Alliance].”55 In addition to international collaborations, companies based in the United States, either independently or through third parties, have begun to combat cybercriminals. “Once a company detects a network breach, rather than expel the intruder immediately, it can waste the hacker’s time and resources... Companies can also allow intruders to make off with bogus files or ‘beacons’ that reveal information about the thieves’ own machines.”56 While both law enforcement in the United States and private entities are dedicating time and resources to combating cybercrime, these

54 Federal Research Division.
55 Rushe.
56 Ibid.
defensive maneuvers, which companies are forced to use in order to stay in business, are “sometimes outside the law.” Western authorities also deserve credit for the extradition of Julian Assange and the arrest of Kim Dotcom—two large steps in combatting criminal enterprises on the Internet. The presence of “officials from the Department of Defense, the Department of Homeland Security and the National Security Agency” at the hacking conference DefCon in late 2011 and the “Meet the Feds” event they hosted are also steps in the right direction.

Western authorities must remain vigilant in their efforts to protect their citizens and infrastructure, but they must also recognize the shortcomings in their stifling approach to cybercrime. They must adapt to meet the nature of modern cyber criminals and hackers and dedicate resources to catch up to and surpass China and Russia in global cyber-dominance. In order to remain competitive in the rapidly developing world of cybercrime, the United States will need to find a workable balance between protecting civil liberties, privacy, and intellectual property rights on the one hand, and allowing talented hacking students to flourish as they do in Russia.

Works Cited


57 Ibid.
58 Smith.


