PONARS Eurasia
NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

Russian ITC Security Policy and Cybercrime

PONARS Eurasia Policy Memo No. 601
July 2019

Alexander N. Sukharenko[1]
National Security Study Center (Vladivostok)

The fast expansion of information-communication technology (ITC) as a requisite factor of economic development and improvement of public institutions inevitably creates new opportunities for criminals. Hundreds of thousands of cybercrimes are registered annually with associated financial losses estimated at several billion dollars. The Russian government has been trying to counter cybercrime through legislation and cooperative initiatives, as outlined in this policy memo. However, the number of persons prosecuted in Russia is insignificant compared to the scale of this segment of crime. The main reasons for the lack of arrests are its transnational nature and certain technical features of cybercrime (notably, its lack of material traces and the anonymity of Internet users), along with a dearth of qualified law enforcement officers and investigative techniques. An outcome of this challenge is a new cooperative agreement among members of the Commonwealth of Independent States (CIS) that is meant to serve as an updated framework to counter cyber-criminality. In the meantime, several case studies, as well as key recommendations for ITC-oriented policymakers, are condensed and outlined here. Successfully apprehending perpetrators and safeguarding critical information infrastructure on which national economies increasingly rely is both a global and local mission that calls for cooperation across governmental bodies.

Scope of Cybercrime in Russia

Statistical analysis highlights the high rate of criminalization of the digital sphere in Russia. Over the past 17 years (2001-2018), the general number of crimes committed using computerized telecommunications technologies increased from 1,300 to 174,674. This dynamic does not look like it is changing: to date in 2019, 97,524 such crimes were registered, which is 53 percent more than it was in 2018 (see **Table 1**). The majority of them are listed as fraud (52 percent), theft (19 percent), and drug trafficking (11 percent). Additional common crime types are unauthorized access to computer information,

[1] Alexander N. Sukharenko is Director of the Center for the Study of New Challenges and Threats to the Russian Federation, Vladivostok, Russia. *Note:* This policy memo is partially a result of the U.S. Department of State's annual International Visitor Leadership Program (IVLP), Towards a More Safe and Secure World.

creation and distribution of malicious software, encroachments on electronic payment systems, and the distribution of pornographic materials involving minors. [2]

Table 1. Registered ITC Crimes in Russia (2011-2018)

Year	2011	2012	2013	2014	2015	2016	2017	2018
Number of crimes	7,974	10,227	11,104	10,968	43,816	65,949	90,587	174,674

Source: Main Information and Analysis Center of the Ministry of Internal Affairs, Form 1-VT.

The rise in cyber-criminal developments stems from the dynamic expansion of the Internet, e-commerce, and networked digital systems. Russia saw a significant increase in the number of Internet users from 35 million in 2007 to 92.8 million in 2018, or from 25 percent to 76 percent of the country's population. Last year, the contribution of the Russian Internet (RuNet) to the national economy amounted to 4 trillion rubles ($60 billion), according to the Russian Association of Electronic Communications.

However, crimes identified by law enforcement agencies illustrate only the surface of this dark iceberg. According to a poll of 500 Russian companies from eight federal districts by the National Agency for Financial Research (NAFR), half faced cyber threats. Twenty-two percent of them reported financial losses, followed by issues of virus infections, extortions, hackings of email accounts, fraud, unauthorized access issues, and theft of personal data of clients. Russian companies lost at least 116 billion rubles ($2 billion) in 2017.

Certainly, the rapid domestic expansion of non-cash digital banking and payment settlements led to an increase in the number of cases of money theft or the unauthorized transfer of funds. According to the Central Bank of Russia, in 2018 the volume of unauthorized operations involving payment cards issued by national banks reached 1.3 billion rubles ($19 million), which is 44 percent more than it was in 2017. The total number of these types of illicit transactions increased over the same time by 31.4 percent, from 317,000 to 417,000. In the vast majority of cases (97 percent), scammers used deception, abuse of trust, and social engineering methods to access accounts and steal funds. According to the Central Bank, criminals attempted to steal another 1.5 billion rubles ($23 million) from corporate accounts through remote banking services and systems.

Modern Combat Against Cybercrime

According to the "Digital Economy of the Russian Federation" program, which was approved on July 28, 2017, the main challenges that impede the development of the digital

[2] Crime in Russia for January-May 2019," Main Information and Analysis Center of the Ministry of Internal Affairs, Moscow, 2019, p. 7.

economy are the growth of cybercrime domestically and internationally, the increased capabilities of external actors, and the lack of qualified ITC security experts. The program suggests that both system and government operators should take certain basic, compulsory measures:

- Increase the security of critical information infrastructure and the stability of its functioning;
- Develop mechanisms for detecting and preventing cyber threats and eliminating their consequences;
- Increase the protection of citizens and territories against an emergency caused by information technology hacks on critical infrastructure;
- Improve crime prevention pertaining to ITC and counteract any such violations (via Russia's Doctrine of Information Security, 2016).

In June 2015, the Central Bank of Russia organized a Financial Sector Computer Emergency Response Team (FinCERT). Its main tasks were to analyze data on cyberattacks (means and methods), provide recommendations about securing money transfers, and coordinate information exchange between law enforcement and financial institutions. Today, FinCERT unites 718 different organizations, including 517 banks. In 2018, FinCERT created an automated incident processing system (ASOI) to simplify the process of information exchange as well as to increase the efficiency and level of network security. This year, it will put into operation its "Antifraud System," which is intended to track unauthorized money transfers. In essence, cybercrime falls under Chapter 28 of the Russian Criminal Code (Articles 272-274.1). Federal Law No. 111 (April 2018) established criminal liability for fraud using electronic payment methods (credit/debit cards) as well as other "computer frauds" (Articles 159.3 and 159.6 of the Criminal Code, respectively).

Of importance, in September 2018, the National Coordination Center (NCC) was established under the control of the Federal Security Service (FSS) to deal with computer incidents and protect national information resources. In effect, the FSS is the primary body responsible for detecting and preventing cyberattacks. Under the FSS/NCC, the GosSOPKA program is meant to connect companies to detection systems that are geared to prevent and eliminate computer attacks.[3] In 2018, GosSOPKA identified over 4.3 billion cyberattacks on Russian critical information infrastructure (CII), of which more than 17,000 were labeled as serious dangers.

The laws that aim to establish the organizational and legal framework for securing CII include Federal Law No. 187 (July 2017) "On the Security of the Critical Information Infrastructure of the Russian Federation." This law, which entered into force on January 1, 2018, defines a computer attack as a targeted threat or the actual impact of software or

[3] The acronym for GosSOPKA (*ГосСОПКА*) stands for "Preventing and Eliminating the Consequences of Computer Attacks on Russia's Information Resources."

hardware on a telecommunication network with the purpose of violating or ending its functionality. Federal Law No. 194 (also July 2017) introduced criminal liability on those that cause harm to CII (Article 274.1 of the Criminal Code).

In May 2019, President Vladimir Putin signed the "Internet isolation bill," which is meant to provide for the stable operations of the RuNet in case it is disconnected from the World Wide Web. The new measure, which is supposed to go into effect on November 1, 2019, requires Internet providers to install equipment to route Russian web traffic through domestic servers. Although it may serve to protect digital assets from criminal elements, it might also curtail Russians' access to the international information space and allow average citizens to be tracked and identified online.

Critical Information Infrastructure

CII entities are the information systems and telecommunication networks of the government and government-linked agencies. They are a top focus to safeguard for high level policymakers. (Just this month, *The New York Times* called attention to the "persistent presence" of both Russian and American malware in each other country's electricity grids and power plants.) CIIs constitute the automated technical process management systems (ATPMS) that are active in the defense, healthcare, science, communications, transport, credit/financial, energy, nuclear, space/rocket, metallurgical, chemical, fuel, and mining industries. About 10,000 fields or subfields are listed as linked to Russian CII. Attachments to the aforementioned Federal Law No. 187 contains rankings of the social, political, and economic importance of CII entities according to their strategic importance for national defense, state security, and law and order. According to the law, unauthorized access to protected data stored at a CII is punishable by imprisonment for two to six years with a fine of 500,000 to 1 million rubles (Article 274.1 of the Criminal Code).

Under the law, industries and entities themselves are obliged to inform the authorities promptly about computer incidents, render assistance to FSS or FinCERT officials, and install applications that can detect, prevent, and eliminate cyberattacks. The specific CII security applications should be able to prevent unauthorized access to information, recover a facility's critical information (ensure that there are backups), and have continuous interaction with the NCC. For its part, the NCC is supposed to perform information security monitoring, forecast cyber threats, ensure cooperation between telecom operators and information resource owners, and pinpoint the cause of cyber incidents. (Click here (securitylab.ru) to see an operational flow chart of the NCC/GosSOPKA.) In 2018, NCC specialists stopped more than 20,000 cyberattacks at the source and analyzed over 100 samples of malware.

International Cooperation

For Russia, and assuredly for all states, the international approach to the issue poses benefits and downsides. Russia is the only nation participating in the Council of Europe that did not sign the Budapest Convention on Cybercrime (EST No. 185, 2001). The main reason was that paragraph 32 of the Convention had language allowing for trans-border access to stored computer data during cybercrime investigations by the intelligence services of other nations. In 2017, the Russian Foreign Ministry prepared and offered new conventions to the UN General Assembly on countering digital crime. In December 2018, the Assembly adopted two Russian-proposed resolutions (both supported by India, a major ITC provider) under the titles: "Developments in the field of information and telecommunications in the context of international security" and "Countering the use of information and communications technologies for criminal purposes." The resolutions aim to safeguard a state's so-called privileged data while promoting global consensus and working out concrete and practical approaches to countering cybercrime. The Russian proposals helped open a new chapter in the global discussion and supervision of ITC security.

On another, similar track, in recognition of the transborder nature of cybercrimes, a new agreement between members of the Commonwealth of Independent States (CIS) on "Cooperation in Combating Cybercrime" was signed in September 2018.[4] This document replaces the previous such agreement that was adopted in 2001. In order to ensure effective prevention, detection, and investigation of cybercrimes, the main forms of mutual cooperation are now defined as: exchange of information on committed crimes and the persons involved in them, execution of requests for information to assist crime-solving, planning and conducting coordinated special operations, and assistance in training/professional development of law enforcement personnel.

Judicial Enforcement

Despite the dynamic growth of cybercrime, prevailing Russian judicial practices are not encouraging. The number of persons prosecuted every year remains low in comparison to the growth of intrusions. Over 2011-2018, law enforcement registered 18,333 cybercrimes (under Chapter 28 of the Russian Criminal Code) but were able to identify only 4,100 offenders.[5] This dynamic does not look like it is changing; to date in 2019, 1,139 crimes were registered but only 111 persons were identified.[6] According to the Judicial Department of the Supreme Court of Russia, over 2013-2018 only some 1,300 persons were

[4] The CIS consists of Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, and Uzbekistan.
[5] "Crime in Russia for 2001-2018," Main Information and Analysis Center of the Ministry of Internal Affairs, Moscow, 2019, pp. 23-24.
[6] "Crime in Russia for Jan-May 2019," Main Information and Analysis Center of the Ministry of Internal Affairs, Moscow, 2019, p. 24.

convicted for cybercrimes. Most of the offenders received suspended sentences because they had no criminal record or agreed to compensate for the damages. In addition, some 600 people were convicted for the specifics of "computer fraud" (under Article 159.6). This testifies to the high latency of such crimes.

For years, the U.S. authorities have faced challenges in capturing and convicting Russians accused of hacking crimes. Russian cybercriminals operate with relative impunity inside Russia as long as they do not breach targets in their own country. In return for such immunity, cybercriminals are often tapped to work for Russia's intelligence agencies. It is only when Russian hackers travel abroad that they can be detained. They are therefore wary of going to states that have extradition treaties with the United States.

Several cases are briefly mentioned here of U.S. prosecutions of Russian nationals that stand as good examples of successful efforts to catch overseas cybercriminals.

- In April 2017, Roman Seleznev, originally from Vladivostok, was arrested in 2014 in the Maldives and sentenced to 27 years in prison in the United States for hacking and credit card fraud that caused more than $169 million worth of damage to 500 businesses and 3,700 financial institutions. He was a member of the criminal ring known as Carder.su focused on identity theft and credit card fraud. The authorities found about 2 million stolen credit card numbers on his laptop. In December 2017, Seleznev received a further 14 years in prison for the racketeering in Nevada and another 14 years for bank fraud in Georgia. The April 2019 court memorandum stated, "Seleznev's long sentence is not substantively unreasonable given the harm that he undoubtedly caused to many businesses, the large sums he gained from this scheme, his general lack of remorse, the need to deter other offenders who may consider similar schemes, and the sentences received by similarly situated defendants."

- Mark Vartanyan, originally from Moscow, was extradited from Norway in 2016 and sentenced to 5 years in prison in July 2017 in connection with his role in developing, improving, and maintaining the "Citadel" malware tool designed to infect computer systems and steal financial account credentials and personally identifiable information. His partner, Dmitry Belorossov, originally from St. Petersburg, was extradited from Spain in 2014 and was subsequently sentenced to 4.6 years in a U.S. prison for conspiring to commit computer fraud.

- In August 2017, Maxim Senakh, originally from Veliky Novgorod, was arrested in 2015 in Finland and sentenced to 4 years in a U.S. prison in 2017 for his participation in a criminal enterprise that installed and exploited the "Ebury" malware tool on tens of thousands of computer servers throughout the world and which generated millions of dollars in fraudulent payments.

- Vladimir Drinkman, originally from Syktyvkar, and Dmitry Smilianets, originally from Moscow, were arrested in 2012 in the Netherlands and sentenced in February 2018 in the United States to 12 and 4 years in prison, respectively. Their crimes were worldwide hacking and data breach schemes that targeted major corporate networks, compromised 160 million credit card numbers, and resulted in $312 million in losses—one of the largest such schemes ever prosecuted. Three other defendants in this case, Alexandr Kalinin of St. Petersburg, Roman Kotov of Moscow, and Mikhail Rytikov of Odessa, Ukraine, remain at large.

Today, 19 Russian nationals are among the 69 most wanted cybercriminals in the United States. Even if they cannot be caught, the publicizing of their case details has an effect due to today's global media consumption environment. This alone—increasing awareness of threats—is the widely accepted first key factor in tackling the issue.

Conclusions

According to a summation of measures compiled from recommendations by Group-IB (a Russian computer forensics and information security firm), the Russian Internet Initiatives Development Fund (IIDF), and Microsoft, some simple, effective measures to prevent cybercrime include:

1) Increasing cyber literacy (awareness of threats and ways to protect systems);
2) Mandatory disclosure of information about cyber incidents;
3) Improving international mutual legal assistance procedures and national legislation on elements of cybercrimes and investigative procedures;
4) Expansion of three-way partnerships between companies/organizations, cyber security experts, and law enforcement bodies.

Certainly, tiers of legal frameworks to counter cybercrime have been under discussion or are already in place in Russia, the Eurasian region, and abroad. However, the main reasons for the lack of arrests persist: its transnational nature (anonymity), evolving criminal technical toolkits, a lack of ITC-qualified law enforcement officers, and thorough, fast, cooperative investigative techniques. This means that ever-increasing domestic attention and global cooperation—both of which Moscow is trying to do—are required to minimize the scale of cyber threats that plague the ITC environments around which modern national economies revolve.

PONARS EURASIA NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA
Elliott School of International Affairs
THE GEORGE WASHINGTON UNIVERSITY