Conference Paper

# Innovative Technologies in Combating Cyber Crime

**Azernikov A. D.[1], Norkina A. N.[2], and Myseva E. R.[3]**

[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Master, Kashirskoe shosse 31, Moscow, 115409, Russia
[2]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Candidate of Economic Sciences, assistant professor, Kashirskoe shosse 31, Moscow, 115409, Russia
[3]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), graduate, assistant, Kashirskoe shosse 31, Moscow, 115409, Russia

## Abstract

So far, development and enhancement of global communication networks, distribution of software, and upgrading of computer systems are accompanied by the evolution of criminal environment, with the latter evolving not only within one particular nation but throughout the international community. New opportunities in cyber crime translate into new threats for global information networks and community as a whole, which in terms of preventing and combating cyber crime requires substantial strengthening of information security measures and an approach that is completely different from that applied to combating common crime. The article presents innovative technologies in combating cyber crime and an ever-increasing significance of information security as a system of protecting private, public and state interests.

**Keywords:** cyber crime, cyber security, Internet, information security, innovative technologies, computer systems, information technologies (IT), cyber threats, cyber space.

Corresponding Author:
Chicherov K. A.
kirill.chicherov@me.com

Received: 11 December 2017
Accepted: 20 January 2018
Published: 13 February 2018

Publishing services provided by Knowledge E



Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.



## 1. Introduction

As information and telecommunication technologies develop and evolve, global availability of the Internet constantly increases, and hardware and software are upgraded and enhanced, criminal environment also evolves in the context of new opportunities for cyber criminals. All these factors determine the need for substantial strengthening of information security measures both within one particular nation and throughout the international community. Today no one is surprised by a steady growth in the news on cyber crime and the related court proceedings. As a consequence, cyber security representing one of the major components of any country's national security requires

innovative approaches to properly and efficiently fight cyber crime, and is of crucial importance all over the world.

Unprecedented, complex and diverse cyber threats are of equal relevance to all state agencies and private companies, political parties and nonprofit organizations, as well as the leading economies of the world.

## 2. Material and Theoretical Bases of Research

The definition of cyber crime is provided in the Convention on Cyber Crime (ETS No. 185) of the Council of Europe (signed 23 November 2001) [4, P. 187]. Cyber crime is defined as illegal actions committed using electronic operations that violate security of computer systems and that of data processed therein. It includes solely computer crime in the form of distributing viruses, hidden remote operation of computer systems (spamming, theft of information assets, channel congestion), interception of IP addresses and mobile traffic, stepping-up of tactical activities in cyber space, economic and financial crime in infosphere [7, P. 29]. In Russia, liability for cyber crime is stipulated in Chapter 28 and Article 159.6 of the RF Criminal Code. Cyber crime is also within the scope of other articles of the RF Criminal Code, yet, for 18 years from the moment of adopting the latter, no amendments or addenda have been introduced to the above-mentioned Chapter 28, which led to an increase in cyber crime in Russia due to almost total impunity of criminals as contemporary Russian legislation is absolutely unadapted to new types of crime in the IT sphere [3, P. 127].

Due to the lack of meaningful studies and an extremely high level of latency of cyber crime, current measures designed to prevent and combat computer crime proved to be completely inefficient. Therefore, when it comes to implementing innovative technologies to combat cyber crime in Russia, it is vitally important that Russia adopts best industry practices and experience of the leading Western economies. As a consequence, new bodies and organizations are to be established as soon as possible to coordinate combating computer crime and train Russian professionals in this area.

Thus, the main challenge in fighting cyber crime is anemic legislation that controls relations in the IT sphere; 'anemic' means not only a low level of technical expertise of the law enforcement personnel but also inadequate liability for criminals breaching the law [3, P. 128]. Moreover, in view of a wide geography of such crimes, limited jurisdiction of the law enforcement agencies and the lack of opportunity for investigations on the territory of other states, establishment of efficient international cooperation in this sphere appears necessary and appropriate [5, P. 208].

For example, a well-known Russian Kaspersky Lab collaborates both with the Interpol and the Multilateral Partnership Against Cyber Threats, a division of the UN International Telecommunication Union [6, P. 45]. Kaspersky Lab provides up-to-date technical data on malicious software most widely and frequently used by criminals. Such data may come in handy in the course of the Interpol and IMPACT cooperation aimed at investigating current crime and initiating new cases. Besides, Kaspersky Lab provides proprietary services and expertise in threat detection, its technology base shall be used by the digital criminal investigation unit for combating cyber crime in Singapore, with such unit to be established soon by the Interpol.

Group-IB received a grant from the Skolkovo Innovation Center for the development of CyberCop, a global system of cyber crime prevention, which comprises a whole set of instruments for detecting and neutralizing criminal activity in virtual space and offers, as the basis, a global technology of monitoring, collecting and analyzing data on the ways of preparing for and committing cyber crime, revealing trends and developing algorithms of preventive measures, as well as mechanisms of documenting facts and traces of crime on the Internet.

To illustrate innovative solutions in combating cyber crime as a part of cooperation of the law enforcement authorities and IT companies, the Microsoft Cyber Crime Center should be mentioned. The Center combats crime in virtual space, prevents intellectual property infringement and distribution of malware, etc. Divisions of the Center use all available Microsoft technologies to fight global cyber threats online. For example, the SitePrint technology makes it possible to track and detect cyber criminals' location; the use of a specialist PhotoDNA application helps protect children from prohibited Internet sites.

In any country cyber crime predominantly takes the form of cyber espionage, that is hacking into governmental servers and theft of classified information. This very threat is common for many countries, including Russia, and can be illustrated by numerous examples: Chinese NetTraveler hacked into about 350 computer systems in 40 countries all over the world, including Russia as well; bugs implanted in 2015 by the US intelligence organizations in information systems of Russian governmental agencies while the latter used foreign web-portals and search engines like Google, Yahoo, etc.; to spoof information, in 2015 the US hackers made an attempt to hack into the site of the RF Central Electoral Commission [1, P. 18]. The above examples prove a significant deficiency in information protection systems in Russia. Another striking example of cyber espionage is meddling in Hillary Clinton's electoral campaign in 2016 and server

hacker attacks, of which the State Department accused Russian intelligence organizations but did not supply adequate evidence and which caused the imposition of additional diplomatic and economic sanctions.

An innovative method of combating cyber crime in Russia will be the use of solely domestic search engines by Russian state officials for work-related purposes, such as Yandex, Rambler, Mail.ru, etc., and Russian web-portals.

Moreover, as mentioned before, highly qualified IT specialists should be trained to timely detect and define types of threats and promptly respond to them, develop advanced DoS-attack and virus protection software and applications, with their further upgrading and implementation. The ID system for employees who have access to sensitive and top-secret information needs to be improved and toughened; enhancement of the system to prevent unauthorized access to computer resources and local networks is also a must. Firewalls should be used to protect the network from external entries; regular network monitoring and audit should be organized; data repositories and backups should be arranged. To simplify fugitive retrieving and holding them liable, Russia should join the Convention on Cyber Crime.

Finally, the most dangerous form of cyber crime is cyber extremism which poses a grave threat to the youth and is actively promulgated via networks. This type of crime consists in placing policy documents of various groups, with such documents calling to the dismantlement of the statehood and overthrow of the legitimate authority; containing advocacy of racial or ethnic distinction and supremacy, religious intolerance and spreading of extremist ideology; promoting recruitment for terrorist and extremist groups prohibited in Russia; creation of so called 'groups of death', etc.

To prevent and fight these types of crime it is reasonable and appropriate to implement a whole package of measures, including, but not limited to, monitoring of social networks to identify extremist groups; organization of informant groups to gain live data on the intensification of crime and extremist forces in any social network group; promotion of patriotism and explanation of the essence of extremist ideologies, methods of recruitment for terrorist groups, history of genocide and other crime generated by extremism; familiarization of the youth with federal laws and the Federal List of Extremist Materials [2, P. 135].

## 3. Conclusion

Consequently, development and implementation of the package of measures, as well as application of innovative technologies in combating cyber crime, and improvement

of efficiency of cyber space defence will help successfully detect, forestall and prevent such offences. Each state must take relevant measures to detect hacker attacks of any type, attempts to hack into its systems from the Internet, unauthorized access to classified information, as well as all types of computer crime. And last but not least, special and immense attention should be paid to all aspects of information security as it represents a system of protecting private, public and state interests.

## Acknowledgements

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

## References

[1] Ryazhapov, N.Kh., Bodrova, K.N. Cyber Crime as a Pressing Threat for Russia // Academy for Civil Defense at the RF Ministry of Emergency Situations. – 2015. – No. 3 (13). – P. 18.

[2] Chernova, E.V. Social Networks and Cyber Extremism // Collection: Information Security and Issues of Cyber Extremism Prevention in the Youth Environment. 2013. – P. 132–136.

[3] Purtova, G.A. Prevention of Cyber Crime in Russia // Man, Society and State in the Contemporary World. Collection of Research Papers of the International Practitioners Conference (in 2 volumes). – 2016. – P. 126–129.

[4] Romanenko, A.S. Certain Aspects of Combating Cyber Crime // Current Issues of Law, Economy and Management. – 2015. – No. 11. – P. 187–188.

[5] Murashbekov, O.B. Certain Aspects of Combating Cyber Crime // Current Activity of Law Enforcement Agencies. Papers of the XIX$^{th}$ International Research and Practice Conference. – 2014. – P. 207–209.

[6] Nesmeyanov, A.A. Current Issues of Combating Crime in the High-Tech Sphere // Herald of the East Siberian Institute of the RF Ministry of Internal Affairs. – 2014. – No. 4 (71). – P. 43–48.

[7] Dubrovin, O.V. On the Issue of the State Cyber Security // Herald of the Urals Federal District: Infosphere Security. – 2013. – No. 3 (9). – P. 28–32.