


# Criminological Forecasting of Cross-border Digital Crime on Sustainable Development of Business: Criminal Law, Criminological and Organizational Aspects

Gennady P. Starinov <sup>a</sup>

*Faculty of Social and Humanitarian Studies, Komsomolsk-na-Amure State University, Lenin's Street 27, Komsomolsk-on-Amur, Russian Federation*

**Keywords:** Delictual Management, Genetic Fingerprinting, Right on Name, Transnational Crime, Delictual Security of the Business Environment.

**Abstract:** The article analyzes the factors affecting the delictual security of the business environment. The operational and procedural forms for investigation of the contract murders of entrepreneurs are considered. The foreign experience of the effective implementation of criminological policy in the People's Republic of China under implementation of the social trust program is given. Structural analysis of the legal framework of national and international legislation on information security has identified the need to use the criminological analysis of the effectiveness of law enforcement agencies for prevention of crimes that use IT technology. The obtained analytical data allows interpreting them for criminological forecasting of risks and threats of delictual security of the business environment. By improving the operational and procedural forms of investigation of contract murders of entrepreneurs, the study conducted by the author made it possible to specify legal proposals for improving the operational and procedural forms for investigation of the contract murders of entrepreneurs. The author examined conditions of the effectiveness of criminological forecasting to prevent digital crime and improve digitalization of both law enforcement agencies and private organizations. Legal mechanisms to improve the forecasting of criminogenic performances will allow increasing the effectiveness of the state policy to ensure security in the field of legal business operation.

## 1 INTRODUCTION

For the development of forecasts to prevent digital crime in the field of business operation, the fact of defining the necessary and sufficient amount of social and legal information - the digital space is of particular importance.

The Federal Law "On Information, Computerization and Data Protection" dated 02.20.1995 N 24-FZ, as well as the Federal Law "On Information, Information Technologies and Data Protection" dated 07.27.2006 N 149-FZ, allow predicting forms of the digital crime prevention based on the integrated use of public and private information relations (Novichkov, 2017).

The scientific and technological progress, which allows the direct implementation of information and communication technologies in the business sector, is


an important factor influencing the level of criminological forecasting (Sanders and Sheptycki, 2017).

The low level of professional training of law enforcement officers and private security agencies predetermined the inefficiency of counteracting new forms of economic crimes in the digital business environment:

1 cyber espionage by criminal communities carried out on the basis of illegal access to protected information through circumventing the computer security systems of a business entity;

2 operation of illegal business through the use of the Internet including electronic trading and financial services;

3 business crime based on the illegal export of capital, "laundering" of criminal revenue using mining farms, cryptocurrencies, in the form of non-fiat (private) electronic money (Izborsk Club, 2017).

<sup>a</sup> <https://orcid.org/0000-0001-7748-8954>

## 2 METHODS

The adoption of the new Doctrine of Information Security of the Country (ConsultantPlus, 2016) based on the Development Strategy of the Information Society in the Russian Federation (ConsultantPlus-1, 2017) and the new Strategy for the Economic Security of the Russian Federation (ConsultantPlus-2, 2017) will allow creation of a legal framework for counteracting economic digital crime (Ovchinsky, 2017).

This indicates a steady tendency in recent years to reduce the number of recorded digital crimes of an economic nature with an increase in the share of economic crimes committed on a large and especially large scale. This is largely due to the mechanism of established corruption relations worked out to date within the economic and digital sphere (Tikhomirov, 2017).

Therefore, cross-border high-tech digital crime realizes its criminal capabilities beyond any state borders using software as a crime tool.

As an example, the Watson Discovery Advisor cloud technology, which was previously created by the government for scientific development and analytical research, and is currently being used to solve criminal tasks, in particular, the development of new types of firearms (Weaponland, 2012).

It is no wonder that criminal statistics began to record unlawful acts committed with the use of computer and communication technologies from the beginning of 2017 taking into account crimes of an economic nature (2572 crimes were detected in January-March). These indicators do not take into account the level of latency and the colossal victimization factor (Ministry of Internal Affairs of Russia, 2017).

In this case, the interaction of representatives of legal business, who hire high-tech criminals to purloin intellectual property or discredit competitors, erases the borders and legalizes money obtained by criminal means at the same time actively, on an ever-increasing scale.

The introduction of cryptocurrency into the financial turnover, which allows international crime to engage in cyber blackmailing offenses, facilitates the criminal legalization of funds. In particular, in May 2017, the WannaCru ransomware “attacked” computers in 150 countries of the world, with the subsequent solicitation of \$3,000 in bitcoins to unlock computer networks.

During the 4 months of 2017, more than 50 banks around the world fell victim to the banking Trojan GM Bot, which disguised as their official

applications. The customers of Citibank, ING, Bank of America mobile applications, as well as other large-scale banks in the United States, Canada, Australia and Europe were among the victims of the malware.

Kaspersky Lab registered 205 thousand attempts to infect user resources in 2013, 1.8 million in 2016, and more than 1.65 million during the first eight months of 2017.

In February 2018, a cryptocurrency miner launched on more than 4 thousand Internet sites around the world, including American, Australian and UK Internet resources, which illegally used up to 40 % of the computing power of visitors (Professionals.ru, 2018).

Cybercrime can be associated with not only information security problems, but also with threats to statehood, the military-industrial and industrial complex, and life support infrastructure (CRN, 2017; Tseveleva and Starinov, 2020).

The criminal legal risks and threats caused by new forms of economic crime implemented using digital technologies are so diverse that the only way to counter them is with the joint efforts of the whole society (Ovchinsky and Larina, 2017).

Moreover, under the agreement of the Shanghai Cooperation Organization in 2009, a legally binding mechanism was formulated that restricted the activities of states in the use of information technologies, but most of its norms have not received practical development (Professionals.ru, 2017). Therefore, now, criminological prerequisites have appeared for forming of international legal acts and for organizing of appropriate fiscal structures that could counteract transnational crime.

In addition, we are talking about international cooperation of states in countering “transnational crime, including coordination of legal policy, unification of legal norms, conclusion of relevant international agreements and mutual legal assistance” (Nomokonov, 2010).

In this connection, a foreign experience is of interest in the effective implementation of criminological policies in the People's Republic of China as part of the implementation of a social trust program for each citizen. In 2014, the State Council of the People's Republic of China introduced the “Program for creating a social credit system (2014–2020). The system is already operating in pilot mode in about thirty cities of China (Carnegie Moscow Center-1, 2017).

High-ranking holders will enjoy various social and economic benefits. However, those who with a rating that does not meet the requirements will have

to suffer – the full power of administrative sanctions and legal restrictions will fall upon them.

The main goal of the criminological policy of the Chinese leadership is to improve both the mechanism for encouraging law-abiding and conscientious citizens, and the mechanism for punishing those who violate the law and lose confidence, so that a person does not even dare and simply cannot lose public confidence.

Mr. Deng Yuwen, the Chinese political scientist, analyzing the current situation in the People's Republic of China, wrote as follows. "A society in which ethical boundaries are constantly blurred, a personality breaks up, there aren't even elementary restraints what is virtue, what is dishonor, when the whole nation is driven by criminal interests only, such a society degrades to the level of the struggle for existence, to the animal level." (Carnegie Moscow Center-2, 2017).

### 3 RESULTS

Having studied the features and characteristics of new types of crime, a criminological analysis of the work of law enforcement agencies to prevent crimes using digital technologies will allow us to predict the risks and threats of a criminal type that our society will have to deal with.

Moreover, it is important to bear in mind that the risks and threats caused by digital cybercrime will be so diverse in future, that confronting them only with the capabilities of law enforcement agencies will be unrealistic.

In particular, the COVID-19 global pandemic swept the whole world in 2020, bringing unprecedented pressure on state institutions, applying an additional burden on the health care system. Criminals quickly acted on the opportunity to use the threat to the global economy, adapting their criminal methods or developing new forms of digital criminal activity. Cybersecurity risks for business operation have increased.

Cybercriminals will continue to improve criminal schemes in order to deploy various packages of malware and ransomware associated with the COVID-19 pandemic. They will be able to expand their criminal activity by including other types of online attacks.

We predict the introduction of new fraudulent schemes to increase the number of further victims of cybercrime. The possible transfer of some of the most qualified specialists in the field of information

technology to the criminal sphere may deteriorate preventing cybercrime in business.

In particular, N. Kasperskaya, the board chairman of the "Motherland's Software" (ARPP) software developers' association, warned Mikhail Mishustin, the Russian Prime Minister, about the risk of mass emigration of Russian IT specialists in the coming years.

According to her preliminary assessment, about 10 thousand to 15 thousand programmers in the field of information technology can leave Russia in the period from 2020 to 2021 (RUSSOFT, 2020).

We agree with V. S. Ovchinsky (2017), that modern digital technology contributes to the fact that not only business, but also criminal activity can use almost all computer programs and new information and communication technology solutions.

Effective crime prevention in the digital space will be ineffective without creating mutually beneficial public-private partnerships, based on the systematic use of practical experience and technological knowledge owned by the business sector.

Only in this case, delictual management as a control system for preventing crime in the field of digital technologies will be more pre-emptive in criminal realities than in response (Ovchinsky, 2017). Prevention to the future crime, committing crimes in the field of digital technologies, will be effective only if it becomes the affair of the whole society and of the most active, advanced including in terms of technology its members, entrepreneurs in particular (Ovchinsky and Larina, 2017).

The Decree of the President of the Russian Federation dated March 11, 2019 No. 97 approved the attached "Fundamentals of the state policy of the Russian Federation in the field of chemical and biological safety for the period until 2025 and beyond". The Decree is of great practical interest, as it will help to improve the further criminological forecast for effective crime prevention using digital technologies (ConsultantPlus-1, 2019).

### 4 DISCUSSION

Special aspects of the application of digital technologies in practice related to the creation of a unified system for genetic fingerprinting is determined not only by emergency situations of a non-criminal nature with human victims, but also by the facts of abduction of business representatives, followed by an infringement on their lives (latent crime).

According to official statistics, 25711 missing person cases were registered to identify citizens by unidentified corpses in the territory of the Russian Federation for 2016, 21463 missing person cases in 2017, 7894 missing person cases in 2018, and 14,794 missing person cases for January-September of 2019 (EMISS, 2020).

Comparative data on the results of the identification of unidentified corpses in the regions of the Khabarovsk Territory for the period 2016 - 2020 show that the law enforcement agencies work at an insufficiently effective level. The percentage of identification of the unidentified corpses found is 60% approximately.

Moreover, the identification of unidentified corpses terminates as statute-barred after 10 years, which gives reason to believe that there is a violation of constitutional human rights, a violation of the right on name in particular when burying. Indeed, the main goal of law enforcement agencies to identify unidentified corpses is to protect such non-material values as name, dignity and inviolability of a person in the end.

The right to receive a name is formed on the basis of article 24, part 2 of the International Covenant on Civil and Political Rights, which fixes the fact that "every child must be registered immediately after his birth and must have a name" (Consultant Plus-2, 2020). As well as paragraph 1 of Article 58 of the Family Code of the Russian Federation, which stipulates the right of a child to the first name, patronym and last name (ConsultantPlus, 2012).

## 5 CONCLUSIONS

The basis for ensuring the safety of each individual is the norms of criminal law aimed at protecting against criminal attacks on the name, life, health, freedom belonging to a citizen from birth until his death.

Unfortunately, the right to the name of every citizen of the Russian Federation should be enshrined in the norms of Constitutional law.

In particular, we propose, paragraph 1 of article 23 of the Constitution of the Russian Federation: "everyone has the right to the name, privacy, personal and family secrets, legal protection of his good name in all non-prohibited ways."

It could be argued with certainty that the identification of unidentified bodies was a legal tool for the implementation of criminological versions aimed at the procedural investigation and prompt disclosure of murders committed for hire.

In this case, the practical implementation of Part 2 of Article 178 of the Hugo-Criminal Procedure Code of the Russian Federation, aimed at genomic registration of unidentified corpses, will be one of the legal mechanisms governing the state policy of the Russian state to ensure the chemical and biological safety of our society from criminal encroachments" (ConsultantPlus-1, 2019).

The use of digital technologies in the process of implementing forensic and biological examinations will allow the investigative body to identify the identity of unidentified corpses, with the aim of effectively investigating and revealing the serious elements of the crime - hiring killings committed against business representatives.

In order to improve the operational and procedural forms of following contract killings of business entities, we propose:

1 Part 2 of article 2 of the Law "On Operational Search Activities," which regulates the main tasks of carrying out the operational search for fugitives from the justice system, be supplemented with the phrase - as well as the search for missing persons and identification of unidentified corpses (ConsultantPlus-2, 2019);

2 Paragraph 2 of the "Fundamentals of the state policy of the Russian Federation in the field of ensuring chemical and biological safety for the period up to 2025 and the future" - be supplemented with the phrase - in order to protect the life and health of other persons their rights and legitimate interests, ensure the defense of the country and the security of the state (ConsultantPlus-1, 2019);

In this case, Bill No. 759897-7 of the Federal Law of the Russian Federation, related to the formation of a single information register, will also be implemented in order to protect the rights and legitimate interests of both Russian citizens and foreign citizens located in our country, "and will be a legal tool for criminological forecasting of digital crime in our society (Rossiyskaya Gazeta, 2020).

We believe that consistent activities related to the implementation of the listed legal proposals for improving predictive forecasting will ultimately contribute to the effective provision of criminological safety in entrepreneurial activity.

It was clear that the objectives of criminological forecasting to counter digital crime could not be achieved without the political will of public authorities and governments to improve digitalization, both of law enforcement agencies and private organizations, which ensured the tortological security of the entrepreneurial environment.

## REFERENCES

- Berk, R. and Bleich, J. (2013). Statistical procedures for forecasting criminal behavior. In *Criminology and Public Policy*, 12 (3): 513-544.
- Consultant Plus, 2012. Federal Law of 25.06.2012 N 87-FZ "On Amending Article 178 of the Code of Criminal Procedure of the Russian Federation": [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_131582/](http://www.consultant.ru/document/cons_doc_LAW_131582/).
- Consultant Plus, 2016. Decree of the President of the Russian Federation dated 05.12.2016 N 646 "On Approving the Doctrine of the Information Security of the Russian Federation". URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_208191](http://www.consultant.ru/document/cons_doc_LAW_208191).
- Consultant Plus-1, 2017. Decree of the President of the Russian Federation dated 09.05.2017 N 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017 - 2030". URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_216363/](http://www.consultant.ru/document/cons_doc_LAW_216363/).
- Consultant Plus-1, 2019. Decree of the President of the Russian Federation dated 11.03.2019 N 97 "On the Fundamentals of the state policy of the Russian Federation in the field of ensuring chemical and biological safety for the period up to 2025 and beyond". <https://www.garant.ru/products/ipo/prime/doc/72092478/>.
- Consultant Plus-1, 2020. Federal Law of 05.23.2020 N 151-FZ "On the Extension for 2020 of an Experiment on Voting at Digital Polling Stations at Additional Elections of Deputies of the State Duma of the Federal Assembly of the Russian Federation of the Seventh Convocation and Elections to State Bodies authorities of the constituent entities of the Russian Federation". [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_353203/](http://www.consultant.ru/document/cons_doc_LAW_353203/).
- Consultant Plus-2, 2017. Decree of the President of the Russian Federation of 05.13.2017 N 208 "On the Economic Security Strategy of the Russian Federation for the period up to 2030". URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_216629/](http://www.consultant.ru/document/cons_doc_LAW_216629/).
- Consultant Plus-2, 2019. Federal Law of 08.08.1995 N 144-FZ "On operational search activity", art. 2 (as amended on August 02, 2019). [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_7519/2aa4e34ca71a259391d2b346d591ab588c7d7863/](http://www.consultant.ru/document/cons_doc_LAW_7519/2aa4e34ca71a259391d2b346d591ab588c7d7863/).
- Consultant Plus-2, 2020. International Covenant on Civil and Political Rights (Adopted on December 16, 1966 by Resolution 2200 at the 1496th plenary meeting of the UN General Assembly. URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_5531](http://www.consultant.ru/document/cons_doc_LAW_5531).
- CRN, 2017. Mitin, V. Seven definitions of the digital economy. [https://www.crn.ru/news/aetail\\_php.ID116780](https://www.crn.ru/news/aetail_php.ID116780).
- EMISS, 2020. Total cases of identification of citizens by unidentified corpses registered. <https://fedstat.ru/indicator/36190.do>.
- Glazyev, S. (2017). Izborsk Club. The Great Digital Economy. <https://izborsk-club.ru/14013>.
- Legislative support system, 2020. Bill No. 759897-7. URL: <https://sozd.duma.gov.ru/bill/759897-7>.
- Lem, S. (1964). *Summa Technologiae*, Wydawnictwo Literackie. Kraków.
- Nomokonov, V. A. (2010). *Transnational Organized Crime*, Publishing House of the Far Eastern Federal University. Vladivostok.
- Novichkov, V. E. (2017). Forecasting the crime prevention and improving the management of law enforcement practices in applying criminal law measures on crime and criteria for their effectiveness. In *Izvestia of Southwestern State University*, 21(5(74)), p. 204-211.
- Ovchinsky, V. S. (2017). *Virtual Shield and Sword - USA, PRC and Britain in Digital Wars of the Future*, Book World. Moscow.
- Ovchinsky, V. S. and Larina, E. S. (2017). *Crime of the Future is already here. Izborsk Club Collection*, Book World. Moscow.
- Professionals.ru, 2017. Bogdanov, A. Russian hackers will penetrate international law. URL: [https://professional.ru/Soobschestva/biznes-klub/rus-skie-hakery-proniknut-v-mezhdunarodnoe/?utm\\_source=NewTopics&utm\\_medium=email&utm\\_campaign=10-12-17](https://professional.ru/Soobschestva/biznes-klub/rus-skie-hakery-proniknut-v-mezhdunarodnoe/?utm_source=NewTopics&utm_medium=email&utm_campaign=10-12-17).
- Professionals.ru, 2018. FSO and the Ministry of Internal Affairs were threatened by a call to miners. URL: [https://professional.ru/Soobschestva/biznes-klub/fso-i-mvd-ugrozhal-prizyv-v-majnery/?utm\\_source=NewTopics&utm\\_medium=email&utm\\_campaign=4-03-18](https://professional.ru/Soobschestva/biznes-klub/fso-i-mvd-ugrozhal-prizyv-v-majnery/?utm_source=NewTopics&utm_medium=email&utm_campaign=4-03-18).
- Rossiyskaya Gazeta, 2020. Zamakhina, T. A law on a unified register of information on the population of Russia has been adopted. URL: <https://rg.ru/2020/05/21/priniat-zakon-o-edinom-registre-svedenij-o-naselenii-rossii.html>.
- RUSSOFT, 2020. Russia is on the threshold of mass exodus of IT personnel abroad. URL: <https://russoft.org/news/o-chem-dumaet-biznes-internet-veshhej-umnye-goroda-korporativnaya-mobilnost-netapp-novoe-v-shd-bezopasnost-tsifrovaya-transformatsiya-it-v-gossektore-it-v-bankah-it-v-torgovle-telekom-internet-it-bizn/>.
- Sanders, C. B. and Sheptycki, J. (2017). Policing, crime and 'big data'; to-wards a critique of the moral economy of stochastic governance. In *Crime Law Soc Change*, 68, p. 1-15. DOI: 10.1007/s10611-016-9678-7
- The Carnegie Moscow Center-1, 2017. Kovacic, L. Big Brother 2.0. How China is building a digital dictatorship. <http://carnegie.ru/commentary/71546>.
- The Carnegie Moscow Center-2, 2017. Denisov, I. E. China after the XIX Congress of the Communist Party: what's next? URL: <http://imi-mgimo.ru/en/mneniya-ekspertov/38-tsentr-issledovaniy-vostochnoj-azii-ishos/denisov-igor-evgenevich.html?start=6>.

- The Ministry of Internal Affairs of Russia, 2017. The state of crime in Russia for January-March 2017. [http://static.mvd.ru/upload/site1/document\\_file/sb\\_1703\\_1.pdf](http://static.mvd.ru/upload/site1/document_file/sb_1703_1.pdf).
- Tikhomirov, Yu. A. (2017). *Legality: Theory and Practice*, Contract Law Firm LLC. Moscow.
- Tseveleva, I. V. and Starinov, G. P. (2020). Exercising Digital Rights in Procedural Law of Russian Federation. In *Advances in Economics, Business and Management Research*, 138: 469-473. DOI: 10.2991/aebmr.k.200502.077
- Weaponland, (2012). Ronin The society is concerned about the possibility of manufacturing weapons using 3D printers. URL: [http://weaponland.ru/news/obshhestvo\\_obespokoeno\\_vozmozhnostju\\_izgotovlenija\\_oruzhija\\_s\\_pomoshhju\\_3d](http://weaponland.ru/news/obshhestvo_obespokoeno_vozmozhnostju_izgotovlenija_oruzhija_s_pomoshhju_3d).

