HV1-9960
UDC 329.61

Andrei FOMENKO
The South- Russia Institute of Management – branch of the Russian Presidential Academy of National Economy and Public Administration (RANEPA), Rostov-on-Don

Crimes in High Technology: Cyber-Terrorism as a Global Threat of Modern Society

ABSTRACT
Modern problems of public safety connected with the spreading of cyberterrorism will be reviewed under this report. The legal status of crimes in the high-tech industry is reviewed. Main characteristics of crimes in the high-tech industry and specific versions of cyberterrorism are herein described. Main risks of society connected with potential threat of cyberterrorism have been defined.
Key words: *cyberterrorism, crimes in the high-tech industry, hi-tech, information technologies.*

The actual stage of development of the world community is defined by rampant development of scientific and technical progress and introduction of modern high technologies into all spheres of human life and activities. There is a computerization of such vital fields of activity of society as communications, power industry, transportation, oil and gas transportation and storage systems, financial and bank systems, defence and national security, structures of ensuring the activity of the ministries and departments, transition to methods of electronic control of technological processes in everyday life and in industries. High technologies become quickly an important component of development of the world community. At the same time such introduction of high technologies is also accompanied by outburst in negative public outpouring, in particular in such as "crimes in the high-tech industry".

The term "crimes in the high-tech industry" is relatively new and debatable for the Russian criminal and legal reality. At that the discussions are held in two directions:

– First, criteria of rating the socially-dangerous acts in the high-tech industry to the group of so-called "computer crimes";

– Secondly, expediency of use of the term "computer crimes" is questioned, instead of it the terms "information crimes", "in the high-tech industry" (as a version — crimes in information sphere), "cybercrimes" etc. have been proposed.

Under the current Russian legislation such socially-dangerous acts are subject to regulation by statutory acts of various branches of law: administrative, civil, criminal. A number of the important provisions related to regulation in this area are contained in the following laws: "On information, information technologies and about protection of information", "On personal data", "On commercial secret", "Concerning Electronic Digital Signatures", "Concerning State Secrets". The criminal code of the Russian Federation also contains the regulations providing punishment for commission socially-dangerous actions in the sphere of computer information. Such norms are legal innovations in the Russian criminal legislation. Most likely, the definition "computer" with reference to information has arisen for the delimitation of this object of the offense from other crimes provided by other sections of the criminal code of Russian Federation at which commission high technologies are used.

So, Chapter 28 of the Criminal Code of Russian Federation "Computer information crimes" contains three articles: "Unlawful access to computer information" (Art. 272 of the Criminal Code of Russian Federation), "Creation, use and distribution of malware" (Art. 273 of the Criminal Code of Russian Federation), "Improper operation of means of storage, processing or transfer of computer information and telecommunication networks information" (Art. 274 of the Criminal Code of Russian Federation).

When high technologies are used, for example, only as the tool or means of commission of criminal activity, such crimes are qualified by the legislator as other, corresponding generic objects of crime: slander (Art. 128.1 of the Criminal Code of Russian Federation), violation of secrecy of correspondence, of telephone conversations, of post, cable or other messages (Art. 138 of the Criminal Code of Russian Federation), illicit trafficking of the special means intended for surreptitious obtaining of information (Art. 138.1 of the Criminal Code of Russian Federation), intellectual property rights and neighboring rights violation (Art. 146 of the Criminal Code of Russian Federation) is in the section " Offenses against person". Theft (Art. 158 of the Criminal Code of Russian Federation), fraud and its types (Art. 159 — 159.6 of the Criminal Code of Russian Federation), illegal organization and carrying out the gambling (Art. 171.2 of the Criminal Code of Russian Federation), manufacturing or sale of counterfeited credit or settlement cards and other instruments of payment (Art. 187 of the Criminal Code of Russian Federation) — in the section "Economic crimes" etc.

It should be noted, that exactly the term "crimes in the high-tech industry" should be considered as a criminal and legal category in the Russian and international criminal legislation.

Such position is subject to the following circumstances. If you refer to the definition of the term "technology", to its primary definition, so the purpose of technology would consist in resolving to components the process of achievement of any result. The technology is applicable everywhere where there is an achievement, aspiration to result, but intended use of a technological approach became an undoubted revolution. Before introduction of technology the art was dominated — a person did something, but

this something resulted only from him, it was as a blessing — is present or not. By means of technology all that what was available only to the elite, blessed (art) becomes available to everybody.

The latest and the most advanced technologies of the modern times are classified as high technologies (English term high technology, hi-tech), transition to use of high technologies and corresponding equipment is the most important link of scientific and technical revolution (NTR-scientific and technological revolution) at the present stage. New, most knowledge-intensive industries are usually classified as high technologies: microelectronics, computer facilities, robotics, nuclear power, space equipment, microbiological industry.

Information technologies are a wide class of disciplines and of the spheres of activity relating to technologies of management, accumulation, processing and information transfer. Computer technologies are mainly understood by information technologies. In particular, information technologies deal with use of computers and the software for storage, transformation, protection, processing, transfer and obtaining information.

Therefore, use of different types of computer equipment, technical means and specific technologies including the information technologies — all this as a whole builds up such capacious concept as "high technologies" as a set of methods and implementers of information processes in various areas of activity of the human beings, society and the state.

There are following characteristic feature of crimes in the high-tech industry:

– heterogeneity of object of the offense;

– acting of computer information both as object, and as crime instrumentalities;

– variety of subjects and means of criminal encroachment;

– acting of computer and other hi-tech equipment, both as a subject, and as the tool or crime instrumentalities.

The analysis of the existing criminal legislation, judicial and investigatory practice allows classifying the following criminal actions as crimes in the high-tech industry:

1. Criminal actions in the sphere of the high technologies, infringing the privacy, and also honour, dignity and business reputation;

2. Computer crimes (chapter 28 of the Criminal Code of Russian Federation):

– Unlawful access to computer information (Art. 272 of the Criminal Code of Russian Federation),

– Creation, use and distribution of malware (Art. 273 of the Criminal Code of Russian Federation),

– Improper operation of means of storage, processing or transfer of computer information and telecommunication networks information (Art. 274 of the Criminal Code of Russian Federation).

3. Telecommunication (computer) frauds and frauds with use of bank plastic and other settlement cards.

4. Criminal actions committed via Internet where the Internet acts as the environment and mean of the organization of criminal activity:

– The criminal actions connected with the data contents (pornography distribution);

– The criminal actions connected with promotion (justification), organization of terrorist or extremist activity.

The criminal actions connected with promotion (justification), organization of terrorist activity or "cyberterrorism" are the most injurious to the public expressions of crimes in the sphere of high technologies.

The analysis of development trends of modern terrorism allows predicting with great probability that "cyberterrorism" threat will only escalate from year to year.

Experience already gained by the world community in this area, clearly testifies the helplessness of any state against this sort of criminal threats, because the "cyberterrorism" has no state boundaries.

The analysis of judicial and investigatory practice and materials of periodicals allows allocating two types of cyberterrorism:

— commission of terrorism act by means of high technologies;

— use of high technologies for the purpose of terrorism.

Specific feature of the first type of "cyberterrorism": by using computer, computer systems or their network, by means of technological devices or telecommunication infrastructure it is possible to hack into computer networks, storage and databases processing system, to make changes to software and databases or to affect (destroy) the information storage and processing systems, to create and (or) to distribute the malware which activity will allow to disable control systems of critical public infrastructure and sources of increased danger that in turn will promote creating a risk of loss of life, of a significant property damage or ensuing of other socially harmful consequences, with a view of public safety violation, intimidation of the population or put pressure on decision-making by authorities.

Characteristical for this sort of "cyberterrorism" is that all these actions are carried out by use of various computer systems or networks. Network user community is not limited, and information safety is mainly provided by a system of administrative and technical measures. As a result the person which is carrying out an act of terrorism by means of high technologies — the cyberterrorist — has possibility to conduct his activities undisturbed, without being afraid to be exposed.

The second type of "cyberterrorism" means use of telecommunication systems by terrorist groups for creating conditions of development and implementation of terrorist activity:

1) creation of web-sites of the terrorist organisations or of web-sites propagating the terrorist ideas. The content analysis of these sites allows to allocate three audiences whereon these sites are appealed to: current and potential supporters; terrorist sites use slogans and offer for sale such products as badges, T-shirts, flags, videos, audiocassettes — all these products are intended for the sympathizers; formation of opinion of the international community. All this allows treating the Internet as a huge digital library. For example, about one billion pages of information, which could be of interest for the terrorist organisations, are mostly in a free access. It is possible to collect at least 80 % of necessary information about potential object of the offense (the potential opponent) using public sources openly without use of illegal means.

2) fund raising for financing of terrorist activity. As well as other political organisations, terrorist groups use the Internet for replenishment of their funds.

3) collecting and analysis of demographic data.

Demographic data of the Internet users (extracted, for example, from the personal information entered into the online questionnaire or while filling the order form) allow terrorists to identify the relation of audience to this or that problem.

4) recruitment of supporters. The Internet can be used not only for requests for donations from sympathizers, but also and for recruitment of supporters playing more active role in support of terrorist actions. Recruiters can use also more online technologies; move on chats and forums in search of the most susceptible members of audience, especially of young people.

It may be noted that that some potential supporters use the Internet for self-advertising to the terrorist organisations.

5) creation and organisation of a terrorist organisations network.

Free independent groups have possibility to maintain contact with each other and with other terrorist organisations via Internet.

6) distribution of information promoting organisation and carrying out acts of terrorism. The world wide web is the house of many sites containing information on creation of the chemical weapon and explosives.

7) planning and coordination during implementation of individual acts of terrorism. Terrorists use the Internet not only to learn, how to build explosive devices, but also to plan and co-ordinate certain attacks.

Thus, both versions of "cyberterrorism" as a sociopolitical phenomenon are characterised by a steady complex of signs (features) distinguishing it from other types of political violence, namely mobility and information support. Increase of level of information support in the terrorist organisations and with their partners allows intensive exchange of information. Today terrorists are capable to receive information practically in real-time mode and to respond quickly. Besides, there is an improvement of professional level of members of the terrorist organisations, the person possessing knowledge in the field of high technologies are recruited into ranks of terrorists and, as a result, there is a further strengthening and increase of organizational power of "cyberterrorism".

The above-stated characteristics of cyberterrorism put forward a "cyberterrorism" counteraction problem to the category of global problems and force people to look for new, more effective forms and methods of struggle against cyberterrorism.