Challenges of Modern Era: Cyberterrorism and Cybercrime

Alexander A. Galushkin

Department of Judicial Authority, Law-Enforcement and Human Rights Activity of the Peoples' Friendship University of Russia;
International Institute of Informatization and Public Administration named in the honor of P.A. Stolypin;
Moscow State University of Psychology and Education
Moscow, Russia

ABSTRACT— ***In the present article questions of cyberterrorism and cybercrime counteraction in the XXI century are discussed. Reasons for the new types of crimes from the theoretical and practical point of view and explains why new types of crime, including terrorism are so important for study and law-enforcement are discussed. During discussion author presents opinions of scientists and specialists in the sphere of information technologies, law and security. Different meanings of the terms "Cyberterrorism" and "Cybercrime" are discussed and analyzed. Differences and similarities of the terms "Cyberterrorism" and "Cybercrime" are presented. Characteristics of "Cyberterrorism" and "Cybercrime" in terms of actions are presented. In the conclusion author present opinion that without appropriate legal regulation of activities in the Internet it would be impossible to protect rights of persons and organization. Author explains that due to the fact that Internet is global (more than 150 countries are connected to) it would be appropriate to regulate Internet activity on the international level.***

Keywords— cyberterrorism, cybercrime, Internet, legislation, law, law-enforcement

1. INTRODUCTION

With the development of new information technologies population of the world got many new instruments of making persons everyday life easier and to work more efficiently. Modern technologies combined made it possible to make microprocessor computers, operation systems and other useful hardware and software. Different equipment and software combined made it possible to create networks, incusing the word wide network – Internet

Nowadays we can say that Internet is accessible on regular bases in most parts of the modern world, including territory of 150 countries. It is important to point out that acts of international, national and local level, as well as corporate norms and self-regulatory acts regulate certain aspects of Internet activities. Some scientists and practitioners believe that organizational and legal bases of ensuring information security and appropriate legal order fall under norms of the real rights. Current practice shows that many norms of international law are very week in regulation and enforcement. Theoretically each country is able to adopt own national laws to regulate certain Internet activity, however in many countries such regulations do not exist or are not appropriate enough.

Like any other aspect of persons life and action activities in the Internet should be appropriately regulated to have appropriate criminal and administrative measures applied. Practice show that legal aspects of computing, including what is sometimes is called "Information Law", as well as counteraction to cybercrimes and questions of bringing offenders to criminal and administrative penalty is becoming more and more actual. It is impossible and unreasonable to stop progress. Active development of information technologies may be considered as a factor of modern middle class development.

"Interest of the person for manufacturing development and services providing is an effective basis for the middle class emergence. An ideal civil society is open, democratic, social market society where there is no place for personal authority, a totalitarian modes, violence over people and where full respect of law and morals exist, principles of humanity and justice are exercised by every person. Civil society can't be treated as an antithesis to state because civil society and the state are objectively closely interconnected and interdependent social, political and legal phenomena (a kind of tandem where ideally the leading role has to be on the civil society side" [1]. There are different forms of civil society activity, including activity in the global network – Internet. Civil society is not without criminals and other persons ready to violate law. Actions of such people may be done in person or in the Internet. Such online offences, in difference from the classical offenses made usually in a concrete place in space, are often not attached to a concrete geographical point, what makes in very hard, or even impossible or to determine in which country they are made. Such difference combined make it extremely hard to regulate activity under national laws and norms of self-regulation. Even more challenging are organizational and legal questions of law-enforcement.

2. RESEARCH METHODOLOGY

In the present article author present summery of conducted research, where research problem was formulated, a good empirical base accumulate, an opportunity to focus on the research process and to draw conclusions that would reflect the real situation in the best possible way using: introduction – hypothesis, deduction – predictions, observation – nest of predictions, etc. was given.

3. RESULTS AND DISCUSSION

In spite of the fact that many people and organizations choose communication services that are provided by large companies providing different telecommunication services, including services of the Internet Service Provider, communication services and data transmission services completely officially and openly, there is a significant amount of organizations providing services anonymously and sometimes illegally.

Generally, organizations, rendering such services are small data-centers (sometimes even in-house), hosting companies and small Internet service providers who are officially, quasi-official, or unofficially provide different services. Such services include services of connection anonymizing (VPN, Proxy, Socks, etc.), a no abuse virtual hosting, and virtual private server, rent out the equipment and communication channels that are in operation of such organizations.

Obviously prices for such services are much higher than prices for similar "white services" (services provided by companies that trace purposes of their services use and reasonably reacting on the abuse letters).

For some people it is not obvious who and why may need such services. However the reason is simple. Some people are ready to pay more for anonymity and actual impunity from almost any responsibility. If we talk about services of masking IP address through (VPN, Proxy, Socks, etc.) often it is done to hide real identity and often makes it almost impossible for law-enforcement officials to identify the real person who is conducting actions. If we talk about services of no abuse virtual hosting, virtual private server and privet server it is often used for the web-sites that would be illegal in certain country placement (casino, drugs trading, porno) or for publication of slander materials (especially during the election periods) and for the variety of different reasons combination.

Instrument for conducting cybercrimes and cyberterrorism vary, however many of them are available to most specialists. Instruments of hiding identity in the Internet are the same for everyone and users of such services are numerous. Often in cases of anonymizing services use even when a fact of cybercrime and cyberterrorist act exists there is often impossible from appropriate governmental authorities to find the real person, who conducted illegal actions. And even if it becomes possible it takes a great amount of time and the result is often unpredictable. In the modern era a lot of companies are ready to have almost any client, no matter of the ethical aspects.

Author feels important to point out that cybercrime and cyberterrorism is not only subject to using Internet technologies for conducting crime. Cybercrime types include hacking of communication channels to get illegal access to Internet or other network, to make phone calls including masking or falsifying caller identity.

Nowadays there are much more cell phones in use than it was just 10-15 years ago. With the popularization of GSM technologies cell phones are now used much more often than stationary phones. Until recently procedure of the cell phone connection to the mobile network was a pretty long procedure that was accompanied by many legal components.

Today it became much simpler. Now it is even sometimes easier to get the SIM card registered on the figurehead or at all anonymous. Currently there are a lot of companies that offer free SIM-cards in shops and even airlines. Such SIM-cards are technically registered when inserted into the cell phone. At that time cell phone number is assigned. In cases of such SIM-cards it would be useless to trace the nominal subscriber to find out who was calling. Special means would also give very little and would allow to trace only serial number of the device (and even this is not always possible), a place of connection to the network (the base station), and also, in some cases to trace traffic from the device. Such services are often used by tourists and other frequent fliers, however criminals and terrorists also often use such services. Often criminals use stolen cellphones, however more technically advanced criminals use specially programmed cell phones that change every so often it's IMEI (International Mobile Equipment Identity) what allows to mask equipment (mobile device) from tracing by number.

Another great opportunity for criminal to get usually traceless access to the Internet are the free Wi-Fi spots. Even thou in some places providing of the first and lust name required to get access to the Internet, it is usually done be user online. So practically there are no means to make sure that information entered is accurate. Usually points of free Wi-Fi access are placed at crowded areas, so if in future law-enforcement officials would investigate and find out that access was done from such point the chances of finding any new traces of who was actually the person conducting actions would be almost impossible. The only technical trace that would be reasonable left is the MAC address of the network device, from which the connection was made. The only thing it gives is the chance to trace the buyer of this device which would be possible in only few cases.

Often persons possessing sufficient knowledge in the sphere of information and telecommunication technologies, experienced in application of such technologies can easily mask and/or falsify their identity, thus avoiding punishment for illegal actions.

In the same time legislation of many countries lags behind the speed of new information technologies development and doesn't give police and other law-enforcement officers enough legal tools for providing due level of legality, law and order. Legal instruments for the investigation of offenses are also often questionable.

Unfortunately some legislators and other citizens have a wrong opinion that there is no need in revision of legislation and adoption of new acts to appropriately regulate legal relationship on the Internet as well as many other fields of information technologies use. Such approach in some countries lead to the line when responsibility for illegal actions with the use of information technologies does not exist, exists buy is not applied in practiced or is applied but very rarely. These emphasize their misunderstanding of a situation and weak awareness in the field, however unfortunately in some ways support computer crime and terrorism development.

According to survey conducted by the author in three countries, from 1000 respondents considerable part at least once within the last five years faced offenses on the Internet, and some of respondents even suffered from illegal actions personally. Only few respondents reported that perpetrators were found and even les that perpetrators were punished for their actions. However majority of suffered respondents noted that appropriate governmental bodies weren't interested in the investigation of offenses.

Respondents noted such offences, as:

1. Unauthorized use of personal information;
2. Copyright infringement (Copyright violations);
3. Unauthorized access to information (including money theft);
4. Illegal business;
5. Slander;

and many other [2].

Meanwhile, companies, non-profit organization, international organizations and public organizations face even bigger threats. Often, even though offenders get unauthorized access to their networks, servers, sites, accounts, information (including reading, change, removal), plunder personal information, obtain information being a trade secret or other protected by law information remain unknown and/or unpunished.

Governmental and municipal authorities are sometimes even a much more interesting target to cybercriminals and cyberterrorists who organize data theft from the state information systems (or even modification of data) and/or interfere their normal work. Nowadays we can even talk about cyberwars as a form of war conduct.

It all began on the April 27, 2007 with the series of cyber-attacks on the web servers of the Estonian government. This appeared after the relocation of the Bronze Soldier of Tallinn (a Soviet Soldier grave marker). Estonia is one of the countries of the world with a good developed electronic government. In Estonia it is possible to watch parliament debates, get other official information and get governmental services, for example file applications for the governmental services online, as well as even vote online. For this reason attacks were especially painful.

Attacks on the Estonian governmental resources in the Internet was the first, however not the only one. Massive attacks on certain governmental services were faced in USA, China, Russia, Iran, Israel, Netherlands and other. From one side such actions may be seen as cyberwars, however author believes it would be more correct to say that such actions are cyberterrorism acts.

For the best understanding of the problem let’s take a look at what "cyberterrorism" is and compare it with the meaning of the term "cybercrime".

Currently many different definitions of cyberterrorism exist, for example cyberterrorism can be defined as the "intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives" [3].

Some scientists believe that intended political motivated attack on the computer, computer systems, networks that may endanger lives and/or health of people, may lead to any heavy results (including illegal access to data, damage or temporary disabling of equipment, information systems, etc.) of any kind should be considered as cyberterrorism.

Some other scientists believe that cyberterrorism does not much differ from the ordinary terrorism.

Ehen more definitions exist for Cybercrime or Computer Crime or Netcrime is. Before taking a look at some of the definitions let’s take a look at the comparison of cyberterrorism and cybercrime.

Generally the only difference of cyberterrorism from cybercrime is it's openness. "Cyberterrorism acts are conducted openly with intend of the most number of people to see the result. Cyberterrorism is a serious threat to humanity, comparable with the nuclear, bacteriological and chemical weapon, and extent of this threat is not studied in full. Cyberterrorism is especially dangerous because it is very hard to find and neutralize a cyberterrorist due to the small number of traces left. Cybercrimes are usually conducted secretly with the use of the conspiracy measures. Publicity is not usually interesting to criminals." [4].

Let’s take a look at some other definitions. For example under the Random House Dictionary computer crime is an "unauthorized use of a computer for personal gain, as in the illegal transfer of funds or to alter the data or property of others" [5].

On the web site of the Law Office of William Spade it is stated that "cyber crimes are defined by the United States Department of Justice (DOJ) as any violation of the criminal law that involves a knowledge of computer technology for its perpetration, investigation, or prosecution" [6].

"Cybercrime and Cyberterrorism as a problem arose pretty much reassembly and is studied by many different experts and scientists worldwide. However, until recently there is no one set meaning to the words Cybercrime, Cyberterrorism, as well as o many other. Different understandings to these terms exist. Author beliefs that without a good understanding of all corners of the problem are s impossible solve any problem. While there are differences in the understanding of the terms, differences in the understanding what problem areas they cover also exists. This makes it extremely hard to unify different approaches of fight against cybercrime and cyberterrorism" [7].

If we would take a look what is typically included to the list of cybercrime acts we would see:

- Web vandalism, including content of the web site change of deletion;
- Illegal use of copyrighted and/or licensed audio-visual, textual, photo materials and software;
- Illegal access to personal or classified data;
- Fraud;
- Assault.

If we would take a look what is typically included to the list of cyberterrorism acts we would see:

- Web vandalism, including content of the web site change of deletion;
- Distributed Denial-of-Service Attacks (DoS) against a specified server, a number of servers and/or datacenters, sometimes against the channel;
- Attacking equipment of the critical infrastructure, including hydro, water, etc.;
- Disruption of certain equipment to disconnect certain objects from the channels, take control over the equipment.

In general techniques of counteracting to cybercrime and cyberterrorism can be divided into three general groups.

First group is – technical, this groups is dedicated to the development of software and hardware meant to counter certain types of attack.

Second group is – legal group, which is dedicated to making and/or adopting laws to give instruments to the law-enforcement officials for considering certain actions to be crimes.

Third group is – law-enforcement group, which is dedicated to investigating illegal actions, finding of suspects and bringing offenders to justice. Their actions are based on law, developed and adopted by the second group and conducted with use of technical means developed by the first group.

Unfortunately many people believe that no law exists in the Internet space, obviously this is a mistake. If for example someone is punched in the eye on the street, no one probably would reasonably think that police should not be involved. Than why some people believe that in the Internet offences are different and no responsibility exists.

In this view it is quite interesting to point out words of Richard A. McFeely – Executive Assistant Director of the Criminal, Cyber, Response, and Services Branch of the Federal Bureau of Investigation in his Statement Before the Senate Appropriations Committee stated that the "committee is well aware, the frequency and impact of cyber attacks on our nation’s private sector and government networks have increased dramatically in the past decade, and are expected to continue to grow. Since 2002, the FBI has seen an 84 percent increase in the number of computer intrusion investigations.

Our adversaries in the cyber realm include spies from nation-states who seek our secrets and intellectual property; organized criminals who want to steal our identities and money; terrorists who aspire to attack our power grid, water supply, or other infrastructure; and hacktivist groups who are trying to make a political or social statement. It is difficult to overstate the potential impact these threats pose to our economy, our national security, and the critical infrastructure upon which our country relies. The bottom line is we are losing data, money, ideas, and innovation to a wide range of cyber adversaries and much more is at stake" [8].

4. CONCLUSION

As the Veniamin F. Yakovlev – Adviser to the President of the Russian Federation fairly noted, "we now have two important social spheres in which Law present is unfortunately poorly presented. The first is the Internet. Internet – is the greatest benefit while it didn't turn into the greatest evil" [9].

"Considering cyberspace as a unique arena through the lens of polycentrism can help reshape the way we view governance framework, and how cybersecurity should be approached to promote cyber peace. First, though, before these core concept may be examined, the current framework for Internet governance and the lesson it holds for enhancing cybersecurity must be analyzes" [10].

Development of new technologies is unstoppable. However, new information technologies should be used wisely and use should be appropriately regulated.

Unfortunately at the present time actions in the Internet are regulated in every country by own national laws. Some actions are self-regulated in the Internet community. Only very few self-regulating norms are actually working. Current practice shows that national regulation of activity in the Internet has none of very little impact on the state of law and order in the Internet. Moreover, as Internet is a global network, regulation in every separate country leads to the practical unaccountability for many cases of theoretically illegal actions in the Internet.

To make Internet a safe place for lawful activity appropriate regulations should be developed and adopted on the international level, mechanisms of appropriate control should be made standard for the international community. Probably such regulations should be made on the UN bases, however it might be more useful to create a specialized agency or organization with elected representatives from every country of the world.

While regulation of activity is important and is a core stone for any other actions, norms of criminal and administrative liability must be developed and appropriate international mechanisms of controlling it's application introduced. Almost any lay is useless if there is now instrument of bringing offender to the real punishment that would stop this offender, as well as many others from conducting an offence again.

Such mechanisms may be implemented through the specialized convention and enforcement done through the specialized international organization. Authors believe that international community should make affords in the above field on official bases and implement mandatory norms. After such norms would be implemented really effective means of counteraction to computer crime and computer terrorism may be realized.

5. REFERENCES

[1] Grudtsina, L.J., Galushkin, A.A., Questions of Modern Civil Society Development in Russian Federation, World Applied Sciences Journal, Vol., 25, No. 5, p. 790, 2013.

[2] Galushkin, A.A., To the Question of Crimes and Offenses in the National Segment of the Global Information and Telecommunication Network Internet, Pravozashitnik, No. 1, p. 71, 2014.

[3] Kim, A., Computer Crime: Psychology and Law, Journal of Criminal Justice, No. 1, pp. 72, 2014.

[4] Allabin, B.V., Information Technologies and New Forms of Terrorisms, Person. State. Law, No. 2, pp. 17, 2014.

[5] Random House Dictionary, Random House, Inc., 2014.

[6] Law Office of William Spade, URL: http://www.spadelaw.com/cyber-crimes/, 2014.

[7] Shaine, A.J., Cybercrime Characteristics, Journal of The International Institute of Informatization and Public Administration named in the honor of P.A. Stolypin, Vol., 1, No. 1, p. 22, 2014.

[8] McFeely R.A., Cyber Security: Preparing for and Responding to the Enduring Threat, Federal Bureau of Investigation, URL: http://www.fbi.gov/news/testimony/cyber-security-preparing-for-and-responding-to-the-enduring-threat, 2013.

[9] Yakovlev V.F., Public Report By the Adviser on Legal Questions of the President of the Russian Federation, Pravovaya Initsiativa, No. 2. p. 5, 2013.

[10] Shackelford, S.J., Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace, Cambridge University Press, p. 19, 2014.