CYBERTERRORISM - WHEN TECHNOLOGY BECAME A WEAPON

Achiko Kontselidze, PhD Student
Grigol Robakidze University, Georgia

Abstract

Everyone is well aware that the technological revolution of the 21st century is considered to be the time when the highest level was reached by the magnitude of computerization. If we look at the process of computerization, we can have the feeling that soon there will be no need for the phenomenon of human society, "everyone" and "would" be replaced by a computer. It is impossible not to note the positive changes that computerization has brought to mankind. Nowadays, e-mail can do it in one big case that a group of people spent months. It can be said that "streamlined" Modern Human Life. Every day a person can take an unlimited amount of information through a computer which makes it a much more rational and progressive thinking makes. Entering a useful discussion of the results will take us far; the author has set a goal to review the work of the negative aspects of the phenomenon of cyberspace. At the present stage of human development, when properly prepared, include the creation of a virtual network to create a global base, the human consciousness of the real world to the virtual society. And a broad range of the protected person “solves" the virtual world, as well as by the nature of the crime and the transfer of real transformation from the virtual world, where the offender and the offense has faced more solid leverage to protect oneself. Noone disputes the matter, the present reality is so increased offender "knowledge" that is difficult to fight against crime, the virtual world, around the processes being developed so rapidly that the virtual world of the crime committed against one of the two is difficult. In this study, the author aims to review the virtual cyber crime is one of the most severe form (phenomenon) – cyber terrorism, which in many cases involves a much wider range of recipients, and in many cases the effect is much more "devastating" than the force of an ordinary computer crime. Due to increased danger of cyber terrorism has long been a subject of debate has become the leading national governments.

Keywords: Cyberterrorism, Terrorism, Cyberattack, Computer Attack, Cybersecurity

Introduction

Modern reality, the more time goes by entrepreneurship, industry and governments work becomes more and more confined to information technology, all of it in the hands of the criminal activities of the terrorist groups makes it easier. If the street stops any person who has had access to the Internet at least once and wonder how they imagine a world without the Internet? In almost all cases we will have some kind of answer. As time goes by, more and more people "get involved" in the name of good news in the virtual world of the Internet. You will do well to try to analyze the terrorist groups and their attachment to the benefit of the people in the virtual world.

Cyber terrorism is on the computer, network and information on the attack or threat of attack, the state or its people are scared politically, socially, religiously or ideologically. The scale of the Internet made it clear that cyberspace is used by individuals and groups as well as international governments and citizens fear scare. Cyber terrorism is a kind of crime which is directed against the state.

In today's reality of e-business in the financial capital of no less than the actual business relations spin. In many cases the traditional business relationships are based on at least an electronic communications. We can also say that as time goes, business and technology become the closer to each other what leads to the modern form of e-commerce. Every day millions of people in the modern world of global spatial barriers of prejudice are given the opportunity to buy and sell: capital and values. By observing e-business scientists came to the conclusion that if one day the world is about to exit the Internet, 10.5 billion worth of transaction will hamper. This follows from the fact that e-business is mainly performed by Internet, e-mail, voice communication, banking machines, credit cards and other authorization. Entrepreneurship is a driving force and it can be said that the information at the same time is a social status. Information or access increased to such an extent that it became unmeasured. With the increase in e-infrastructure, there is the growing threat of its destruction, one of the factors in the value of the damage caused by the virtual network, and the second as a result of physical damage inflicted psychological harm which carries far more serious and difficult to be forgotten - as a rule.

As time goes on, it becomes more difficult to grow and develop into a phenomenon of crime in cyberspace; cyber security professionals clearly expressed their concern about the increase in attacks against not only the Internet, but these attacks increased awareness regarding the timestamp. With the increase in the complexity of attacks globally, the level of mastery decreased. This is quite a shocking figure. Terrorists learn their attack; they learn what works and what does not, how we respond to them and what types of methods we use for the detection of attacks which increases their chances of success in doing so, they will receive knowledge.

So rapidly unfolding events in the fight against crime in cyberspace that is conventionally found in the method of tomorrow "obsolete" may also exist. This will require the full mobilization of law enforcement.

There is one problem how they manage law enforcement to follow in cyber crime phenomenon of variation, and the second issue of the regulation of the level of Justice will be able to keep pace with cyber crime phenomenon volatility trends; things may be blocking the judiciary which had a place even in the legal system; in practice it is expressed in the following way: There is action, but so altered his "criminal grounds" that in fact it is impossible to regulate the action of the legislative implementation.

One of the main factors which affects the phenomenon of crime in cyberspace is the easiest time. The difficulty lies in the fact that it is impossible to reach the virtual world of illegal behavior rinsing prediction. Society has fear, cyber security specialists during the development of methods of combating crime talk about when it would be the best time in the world for electronic attack on the network infrastructure. They give you all the possible crime forecast methods. If we look from the perspective of the subjects of a criminal offense cyberterorism is the best time; example - the war, elections, inauguration, revolution or other large-scale resonant phenomenon, which has far-reaching and devastating effect on cyberterrorism. A clear example has experienced firsthand the threat from Russia in 2008. Russia was active cyber attacks to create a vacuum of information society that usually comes as a result of the introduction of fear. The event coincided with the actions of the Russian side of cyberterrorism and cybersabotage stereotypes.

Modernity of cyberterrorism is a great popular phenomenon in the society. Unlimited possibilities of the computer are free to control the masses of society; moreover - in today's world, in many cases more devastating effect on the keyboard and properly to the agitation of the carrier, than grenade in terrorist’s hand. For the first time the term cyberterrorism was used in 1980 by American Barry Collin (Collin, 1997). Cyberspace and the definition of terrorism in the context of the safeguarded and the first definition of the concept of cyberterrorism were made by the FBI agent Mark M Pollitt. He said the secret agents or sub-national cyber terrorism is intentional, politically motivated violence against a target which is reflected in the information, computer systems, programs and data bases and in their distraction. US expert Dorothy Denning's cyberterrorism is one of the leading explanations of cyberspace and cyber terrorism mixture which consists of politically motivated hackers operations aiming at devastating effect.

In practice, it is easy to confuse the notions cyberterrorism and computer crimes; moreover, American experts also say that if all the threats of attacks against the United States through cyberspace represent a simple computer crime and the threat against the United States have not been done, it could get into the definition of the scope of cyberterrorism. It all takes place in the September 11 terrorist attacks in the background through which the scrapers of explosion, explosion-mails are more people in the society introduced by terrorists.

The main distinguishing factor between a simple computer crime and cyber crime is committed target. Although computer crime, like information technologies during the commission of the crime of cyberterrorism, or arming means, but if such a crime organization and implementation of public safety violations, spreading fear among the society or by the government in order to influence decision-making, we are faced with the composition of cyberterrorism.

Professor Lawrence V. Brown conducted interesting studies and computer comparison of cyberterrorism. He explained cyber territorial group or an individual's use of information technology and the future plans of agitation. It may involve the use of information technology: network, computer system or television infrastructure for the purpose of the attack as well as the electronic exchange of information or ideas for the broad masses to the idea. Increased due to the danger of cyber terrorism has been highlighted by various Government attentions. Many facts have prompted the government to consider the recently implemented cyberterrorism detailed legislative regulation and control of the new mechanism. I want to give the latest issues in relation to cyberterrorism illustrate an example of Georgian practice; it was as if the Islamist group's jihad against their spread fake videos. So far, the investigation into the allegations has not been completed but the fact is that the video distributor is designed to install fear in the society that the Georgian units from the NATO - led peacekeeping mission. We can say that this fully meets the terms of the notion of cyberterrorism.

Review of the highlights of cyberterrorism specialists achieved outcome scales. The computer attacks which can lead to the destruction, deaths, massive power outages, aircraft disaster, massive water pollution, loss of confidence in the overall economy of the sector can also be qualified as cyberterrorism.

Cyberterrorism and computer crimes are common phenomenon in both risk groups important to be observed in practice. The effective use of the Internet can be seen as a clear example of the negative purposes "hizballah" action which has carried out a psychological attack against the Jewish people. In particular, this organization through the Internet in the summer of 2006, Israel’s anti-terrorist campaign in Lebanon, the Jewish soldiers who died in the photos released. As a result, Israeli citizens demanded from their government to stop the anti-terrorist operation. Similar was attempt by the US anti-terrorist operations in Iraq, but in this case there was such a great impact on the September 11 tragedy in the US population, currently threatening messages that terrorists could not have been realized fully addicted.

Due to the danger of increased concern of the world in the fight against cyber terrorism, NATO Prague Summit in 2002, leaders of the member states have recognized the significant threat of cyber terrorism and considered it necessary to create a "NATO cyber defense program", which consisted of three phases of the Programme of Action - During the first phase "of the NATO Computer Incident Response capacity" (NCIRC), which is the second phase into full working mode. As for the third phase, it covers the first two phases of the experience gained during the practice and the fight against terrorism as well as cyberterrorism modern means of defense.

NATO's important role in the fight against cyber terrorism is "the NATO Communications and Information Systems Services Agency", which is "the NATO Defense Technical Information Center" (NITC). It has duty to protect NATO’s wide communication and information systems from cyber attacks. NITC - holds "NATO defense operations center of information" and "NATO Computer Incident Response Center technical capacity" which allows the organization to provide a high level of cyber defense. On June 14, 2007, a massive cyber attack on Estonia was carried out. The NATO member state's defense ministers agreed that a more active fight against cyber terrorism was required.

Cyber-terrorism, defense activities and events controlled by the North Atlantic Council also shared responsibility, "the NATO Consultation, Command and Control Agency" (NC3A) and "NATO military authorities" (NMA).

Today, the most successful country in the fight against cyber terrorism can be seen as Estonia, which is located in the center of cyber defense - the Cooperative Cyber Defence Centre of Excellence (CCD COE). It was founded on May 14 2008, in order to enhance NATO's cyber defense capabilities.

In this section I would like the reader to focus on Georgia and Georgian legislation with current trends in crime in the legislation of cyberterrorism. As I have mentioned above, cyberterrorism attacks have been repeatedly exposed to the epicenter of Georgia, according to those in the country as well as all of the concerns raised in the Government of our country's resources to improve cyber security. Cyber security plan developed several years’ figures, as for the action of the legislative regulation: December 28, 2002 has been included in the Article 324(1) of the Criminal Code -"Cyberterrorism" title, placed under the Criminal Code Chapter XXXVIII, which deals with terrorism and the door to the XI - "crimes against the state". Cyberterrorism is severely punishable under the Criminal Code, namely, computer information protected by law and unlawful appropriation, use or threat of use, which creates a risk of serious consequences, committed to intimidate the population and /or authority in order to influence is punishable by imprisonment of ten to fifteen years. The same action that led to the loss of human life or other grave consequences is punishable by imprisonment for a term of twelve to twenty years or a lifetime. According to this Article, the legal person of a crime is punished by a fine, deprivation of the activity right or liquidation.

Regulatory and legislative steps taken towards encouraging only cyberterrorism are regarded as a positive development. It is reasonable to draw the reader's attention from the authorities of the new international standards of the University of Technology and Research Center for the meetings of the government level. All of the above is encouraging the Georgian society that our country will be able to confront the challenge of technology and a good answer which can be expressed against the global threat of cases - such as cyber terrorism.

Conclusion

As time goes by, the more complex and multi-point cyberterrorism phenomenon takes the form of crime. We can say that the future of cyber terrorism is the real face of the broad masses and the virtual conflict between terrorist groups. For a long time, the technology has already lost its harmless virtual mask function and become an instrument to commit the crime.

In order to avoid the confusion of a cybercrime and cyberterrorism, I would like readers to pay attention to the modern period expressed by the arbitrary acts of cyber criminals who are more or less contained cyberterrorism/or elements of the phenomenon of cyber crime :

- ✓ Yugoslavia - US (NATO) military operations during the summer of 1999, NATO computer network was blocked in Italy, as well as for political reasons, NATO headquarters and the US Defense Ministry portals of entry into the apartments;
- ✓ Russian Federation - Chechnya since 1999 was carried out systematic attacks on Russian portals. Only one week in May 2000, there were 140 attacks on the portal of the "Caucasus";
- ✓ Armenia-Azerbaijan in February 2000 Armenian hackers groups Liazor (authorized), Apache Group, Russian Apache Team carried out a computer attack to the Azerbaijan governmental organizations and to the 20 mass website through the Internet. These actions are carried out in Armenia, Russia and the US territory. Los Angeles police detained three members of the group;
- ✓ Afghanistan - US GForce Pakistan infiltrated the group in November 2001 the US administration server and placed threats against the US and UK armed forces and demanded to cease hostilities in Afghanistan and the withdrawal of troops from Saudi Arabia;
- ✓ 2000 - 2002 (during exacerbation of the Palestinian problem) were 548 computer attacks on «il» (Israel) domain zone, In Israel it has repeatedly violated Parliament and Defense Ministry servers working;
- ✓ Russia - Georgia 2008, hired by the Russian government and the Russian citizens' programmers group of coordinated action at the expense of important disabling Georgian Web page. Among them: the President, the Ministry of Defense, the National Bank and other important information on web pages. Web pages were turned off, on some of the pages there was a deliberate change of information and disinformation determined to panic society. The influential American newspaper "New York Times" Russian aggression against Georgia was estimated as "the first fact in history, when the armed conflict between the two countries was preceded by intense cyber training;"
- ✓ Russia - Ukraine 2014-2015 from the cyber-terrorist propaganda on a daily basis, in particular television, and the Internet is going to spread the heavy staff, also received threatening calls from the separatist distribute the Ukrainian Armed Forces. All of this is part of the information war against Russia to Ukraine.

Computer crime

- ✓ 2001 - the US , UK, Australia portals neutralization was followed by destruction of some web sites of China, Kuwait, Romania, Georgia and Vietnam (accomplished by the group Pentaguard);
- ✓ 2002 May - it was carried out access to the US Space Intelligence Center network and the confidential information (by a British hacker individually);
- ✓ 2002 June - it was carried out access to the US Strategic Research Centre and to the confidential information (by Austrian hacker individually).

Finally, it can be said that cyber crime, terrorism has emerged as a result of the transformation of the real world to the virtual cyberspace; this type of cybercrime develops and transforms day after day. In the future that could turn into cyber terrorists' effective weapon is the Web wars.

Thus, the fight against cyberterrorism concerns the society in general, methods of combating cyberterrorism gradually improves. I hope that the 21st century rational minded people finally will come to the conclusion that violence is not the only way to resolve the conflict!

References:

Brown Lawrence V. Cyberterrorism And Computer Attack. New York: Novinka Books, 2006.

Collin, B. The Future of Cyberterrorism, Crime and Justice International, March 1997.

E.B Awan I. And Blakemore B., Policing Cyber Hate, Cyber threats and Cyber Terrorism. USA: Ashgate Publishing Limited, 2012.

Denning, D. “Cyberterrorism”, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000.

FBI, 2002. Code of Federal.Regulations. 28 CFR. Section 0.85 on Judicial Administration. July 2001.