CYBER TERRORISM AND CRIMINAL POLICY MEASURES TO COMBAT

ALIMORAD MORADI

MSc. Information Technology, Security Information, Abadan Branch, Islamic Azad University

Abstract— Cyber-crime, is an online crime, which includes crimes that occur in cyber space, it is true that the masses cannot be seen with the eyes, but in some cases it is possible to create numerous risks that cannot be compensated for years , to identify the types of attacks that occur in the virtual environment and learn how to deal with them and be conscious in your data protection is important. For the sake of being unknown in these attacks, By notifying others, these attacks can be fought better. On the other hand, according to the country's dependence on communications infrastructure and computer software, today and in the future, cyber warfare will be among the countries in which computer network technology is as the uncertain border between cyber warfare, cyber crime and cyber terrorism . IT and computer science form the strategic nature of all elements of vital infrastructure in modern civilization, therefore to be effective before the terrorist computer networks and communication systems for government and also to the extent of global scale, these elements are vulnerable infrastructure. The main objective of this paper is to identify and explain the phenomenon of cyber terrorism which is quite serious, so first defines cyber space that is a virtual environment, Cyber space features, that users worldwide can access any electronic information services, and the way of forming cyberspace crimes that are copy as the same, and types of the criminals, and perpetrators of cyber space as well as the flow of future cyber terrorism that is like normal terrorists who have political incentives to commit crimes. And define challenging crisis makers and so forth, and the end, will note shortly to Cyber and network and data security procedures and will submit recommendations and suggestions.

Keywords— Measures, cyber warfare, Cyber-terrorism, criminal policy.

I. INTRODUCTION

In this paper we discuss about cyber space, how this crime develops in this space, different types of criminals and how dealing with them, space security of networks, cyber terrorism and Iran criminal policy to fight against this problem. Our aim is making our networks and Internet environments safety and prevents these kinds of crimes and assassinations, which prevention of cybercrimes or other crimes depends on our consciousness. If people be aware about forms and methods of cybercrime, then decrease the number of victims. Hundreds of companies for a computer security advisor appear in the community and the entire world to resolve a weakness in computer systems and software and make more protection. Furthermore, uses of encryption on data methods, secure socket layer, data separations are effective methods to prevent hacker's access to data. Finally, the possibility of political cybercrimes increases with skill development of more people in programming and infiltrates to computer systems, but terrorism and computer espionage are not only threats for computer networks!! Cybercrimes would compromise individual's security and privacy as society security.

II. CYBER SPACE

In different cultures, cyber means virtual and intangible lexically; this is virtual and intangible environment in international network's space (these networks connected to each other through information thoroughfares like the Internet). All the information which exists on our planet physically such as relationships, cultures, nations, countries (as note, image, voice, and document) exist in the digital form in a virtual space, and they are usable and available for users through computer.

III. CYBER TERRORISM

Terrorism is violence against persons, states or groups for forceful advance of political or public goals. Cyber terrorism has the same definition of the difference that the aim focuses on available sources in virtual space. Cyber terrorism is associated with internal dimensions, or it is consisted of international's cases.

Nowadays, cyber terrorism is more dangerous to traditional terrorism, because economic and service structure of many countries is based on information and communication technologies, so cyber terrorism defined as follows:

Planned and targeted actions with political and impersonal purposes against computers, facilities and their saved programs through a global network with the aim of destruction and serious damage.

Cyber network's security and all the computer systems are very important in every country. Cyber strengthening the infrastructure has a special place in passive defense, which it has been notified by competent authorities in Iran recently. Security measures adaption in computer technologies and cybernetics is the most important step to prevent possible damages against any cyber terrorism actions.

IV. CYBER TERRORISM FEATURES

According to the mentioned notes about cyber terrorism, its features are as follows:

More people involvement, use of unknown computer groups in the international level, no geographical limit, and hidden identity, international advertise and recruitment; expand the scope of terrorism to financial, economic and municipal service's issues.

-- Tools

The internet or virtual space terrorisms, use from malicious software to advance their objectives instead of conventional weapons, bombs, missiles or other common tools. Viruses, worms, Trojans, spams, e-mail bombing, Google's bombing, hack, internet and network sabotage and manipulation are a part of virtual terrorism's tools.

-- Crimes

The internet as a digitized version of real worlds, make an environment with any kinds of crimes. Of course, real world is enclosing, so there is control process ability, but there is no boundary in virtual space, so legislators have many problems. There is no need to passport and visa to sign in the neighboring country web site, so this is a free world with the lowest possible legislative, obviously.

Although, governments try to form legal groups in order to stop criminals, but the crimes of criminals against related crimes to the international rights are negligible in terms of content and number, and this is the main problem. Virtual environment is very powerful in all the areas of human life, and it can present solutions to facilitate them, like family dentist appointment or necessary purchases for the friendly or family parties.

Nowadays, electrical technology does secretarial tasks in virtual environment or personal computers; furthermore, computers don't have any delays in the workplace, or they don't allocate hours to talk with their friends with company telephone. Computers in all the areas of human life are a real revolution at the bureaucracy level.

Computer presence in all areas doesn't have positive points only. Although, computer leads to greater success, but this ubiquity presence setting the stage for a criminal act in terms of the crime act.

Computer crimes challenge all the old legal definitions, because somebody with no output of his / her home does the biggest history robberies from accredited banks with tens of protective and warning devices, and with intelligent acts, by new technology training, withdrawal millions of dollars from bank accounts and deposits them to his / her bank account as a gentleman.

The internet has been made very different space with natural environment and crime emission from a country to other countries become very simple. As countries become more advanced, their Internet crimes increased associated with dangers with more damages.

Nowadays, international criminals use from PC games, animation, chat room and so on for penetration simply. Of course, there are a variety of viruses, worms, anti-services programs and advanced software of password discovery. The use of these methods is in serious confrontation with international rules, and international criminals broken these rules with their criminal acts.

-- Virtual terror

The lack of accurate identification is the main problem of virtual terror that makes it very dangerous. Despite legislative halls, terrorists don't know all the criminal act's aspects too. Therefore, America with the most cyber-attacks is incapable of Chinese hackers. National groups of some countries such as participate in the WSIS summit, and some other entities try for controlling and planning to inhibit this phenomenon.

Interpol is one of the mentioned organizations. Last year in Europe, Europe treaty association was formed; however, this is not European completely, but it is the first serious attempt in this content. There are several ways to fight with this problem.

The first way is vulnerability assessment. On the other words, this way is a prevention method, of course this way is not a defense method, but it eliminates weaknesses and decrease vulnerability in attack case. Second way is another form of prevention, identifies possible attacks and eliminates them. Third way is usable after attack, so that preparations for the attack and fix the created bug after this point.

V. IRAN AND CYBER TERRORISM

The internet is one of the most complex tools for terrorist's targets without a doubt. Terrorists in Internet world can spread violence and their other interests with thousands of virtual names and without any footprint. A part of these activities is explicit and with violent, terrorist and anti-democratic purposes. Opposition groups to Islamic Republic of Iran use this tool to hit the national interest naturally. The best dealing way for these terrorist's acts in cyber space strengthen security measures and instruction implementation based on passive defense.

VI. CYBER TERRORISM AND PREVENTIVE MEASURES

In order to prevent any damage infliction to country information infrastructure it is necessary to take preventive measures to prevent computer terrorism crime, which Iran needs to preventive measures in security policy and efficient technical measure's format in addition to allocation of special criminal rules.

Nowadays, cyber terrorism is one of the main challenges in legal systems and in penal systems, especially, and this problem defined in the following.

-- Computer terrorist

Terrorist crime is not traditional approaches anymore, and it is associated with novel technologies. There are no explicit and specific considerations to cyber terrorism criminalization between most legal systems in the world, and more important note is lacked of any support for cyber terrorism victims with irreparable damages due to cybercrimes. In the first step, prevention of cyber terrorism to support victims is essential. Between all kinds of prevention, situational prevention is the most suitable way to prevent this crime.

Computer terrorists have political motives for their crimes as common terrorists. However, their dangers don't limit to governmental computers only, and private companies systems and even nonprofit groups are vulnerable by them, because they would attack to any computer for desired information based on specific political goals of terrorists groups. Of course, spies attack to governmental computers too.

-- Is computer terrorism possible?

Computer viruses and other computer instrument crisis are tools for terrorist or malevolent hackers to disable important computer systems. Viruses or self-replacing programs are programs to blur other systems, and they permeate with disc, the Internet or e-mail networks. Some viruses may attack to system files and melt motherboard, delete all data from hard drive or disable the computer; however, most viruses are not very dangerous.

The possibility of political cybercrime increases with skill improvement of more persons in programming and infiltrate to computer systems. However, computer terrorism and espionage are not the only threats for computer networks. Computer crimes would compromise individual privacy and security ac society security.

-- Solutions

Computer science specialists should be aware of this phenomenon to have more protection from their control systems and prevent from this problem and its damages. In today's digital world, according to terrorist attacks, the need of investigations in prevention methods is essential more than ever.

The best way for prevention is the use of correct methods, in the first step, operating procedures and attacker sources should be identified. The main problem is that many private and even governmental sectors are unaware about their computer's vulnerability, while computer dependence is very obvious and unawareness in this field associated with irreparable consequences and damages. Which person and from where an attack against the system is another problem. This problem is more important to damages problem. As the first proposal, experts recommended using the firewall to protect and isolate systems from network communications, besides items such as password protection and other security and protection acts. Some solutions to fight with cyber terrorism are as follows:

1. Security strategy formulation for computer network's security in the country
2. Provide the necessary training to network-related forces for maintaining network security; including social engineering skills
3. Use of software, anti-viruses, firewalls in networks
4. Access level determination to the networks and cyber systems

Furthermore, some security recommendations for network users administrators include:

Determine a password so that guessing that be very difficult and its characters be unusual; in case of network defect's detection, change its configuration, install corrective and upgraded versions of existing programs, form a report files for following aggressors and their actions. Don't visit suspicious web sites and don't open e-mails from these web sites to be safe at possible damages.

CONCLUSION

Cyber terrorism becomes a main challenge for governments in recent years, especially in our country. In terms of legislation, criminal legal system of Iran is alienated with this crime, and no specific criminalization exists in this field. Furthermore, victims don't have any provisions for compensating except general rules. Therefore, it is essential to take preventive measures for prevention of any more damages to country information infrastructure.

Situational prevention is the best way to prevent this crime in terms of technical measures. Therefore, there is a need in our country to preventive measures in terms of security policy and efficient technical measures in addition to criminal special rule's allocation. So, about prevent victimization of home users and infrastructural network as the main victims of this crime proposed measures should be done, include: applying intrusion detection and prevention systems, make independent the control and enterprise networks, use from software and hardware firewall, mandatory usage of native e-mail, explicit rules adaption with certain penalties to deal with cyber terrorism and adopting a common point of view based on international criminal law in developing comprehensive convention about cyber space threats such as cyber terrorism are the ways in order to improve the current situation in our country or at the international level.

REFERENCE

[1] Bastaani, B., The internet and computer crimes, Behnami publication, 1383

[2] Stewart, J., et al., Novel challenges, novel tools for defense decision, Translation by Zangeneh, J., Gharibzadeh, K., Join chief of SepahPasdaran Islamic Revolution, first edition, Tehran, 1384

[3] Jalilifarahani, A., H., Situational prevention from cybercrimes in the light of human rights standards, Specialty journal of law and jurisprudence, No. 6, Fall of 84
[4] Hasanbeigi, E., Law and security in cyber space, Abrar international studies and research institute, Tehran, 1384
[5] Hasanbeigi, E., Web-based global information network pathology and present suitable ways to prevent the threats from the view point of national security with the emphasis on technical and legal aspects, Dissertations, The supreme national defense university, 1382
[6] Hosseini, B., Internet crimes against children and its criminology fields, MSc thesis, Azad Islamic University, science and research branch, 1382
[7] Daziani, M., H., Beginning of the cyber-computer crimes, Informatics newsletter, No. 93, 1384
[8] Daziani, M., H., Introduction to the nature and classification of theoretical computer (cyber) crimes, informatics newsletter, No. 87, 1384
[9] Safari, A., Theoretical foundations of crime prevention, Journal of legal research, No. 33 – 34, Bita
[10] Najaf Abrandabadi, A., H., Criminology course pleadings, Criminal law and criminology in graduate course, Tuning by Seyedzadeh, M., The second semester, 1381 – 82
[11] NamakdoostTehrani, H., Johannesburg principles: national security, freedom of expression and access to information, From Iran's web site and the information society, Communication research center, 1384

★★★