PREVENIREA TERORISMULUI INFORMATIC

Ileana ŞTEFAN[1]

[1]Universitatea "Petru Maior" din Tîrgu–Mureş

Str. Nicolae Iorga, nr.1, Tîrgu – Mureş, MUREŞ, 540088, România

REZUMAT: *Lucrarea prezinta o abordare teoretică a conceptului de terorism cibernetic, apariţia şi dezvoltarea definiţiilor şi limitărilor conceptuale, precum şi dimensiunea economică a fenomenului. Cercetarea scoate în evidenţă apariţia şi dezvoltarea acestui fenomen, urmată de prezentarea definiţiilor existente ale furtului de identitate în timp ce încearcă să stabilească relaţii între ea şi frauda de identitate. Deasemenea se face o prezentare a implicaţiilor socio-economice ale infracţiunii.*

.

Cuvinte cheie**:** *infracţiuni teroriste, atacuri cibernetice, spatiul cibernetic,criminalitatea informatical*

Clasificare JEL: K OO, K23

[1] Ileana Ştefan, tel./fax/ :+40744678844, e-mail:stefan.ileana@yahoo.com

1 INTRODUCERE

Utilizarea reţelelor de calculatoare conduc la o serie de avantaje dar şi dezavantaje. Unul dintre cele mai mari dezavantaje este reprezentat de criminalitatea informatică care constă în activităţile ilegale comise cu ajutorul sistemelor informatice şi a Internet-ului .

O condiţie esenţială pentru dezvoltarea omenirii constă în identificarea unică a fiecărui membru a societăţii. Odată cu nevoia identificării diferitelor persoane, a apărut şi furtul de identitate sub diferite forme incipiente. Dezvoltarea mediului informatic şi a mijloacelor de comunicare la distanţă, au facilitat dezvoltarea furtului de identitate care a dobândit noi dimensiuni şi forme. Una dintre formele cele mai des intalnite de criminalitatea informatică este furtul de identitate, în care Internetul este utilizat de către infractori pentru a fura informaţii personale de la alţi utilizatori.

2. DEFINITIE TERORISM INFORMATIC

Terorismul cibernetic reprezintă infracţiunea informatică cea mai des întâlnită în mediul online, având o complexitate foarte mare şi ajungând să fie o infracţiune transnaţională.

Criminalitatea informatica reprezinta o activitate criminala in care obiectul delictului consta in utilizarea calculatorul si a retelei Internet.

Acest fenomen este definit diferit de catre specialistii din domeniu, neajungandu-se la o definitie unanim acceptata, din cauza complexitatii acestui act infractional, iar diferitele modalitati de reglementare a criminalitatii informatice din fiecare stat in parte au condus la imposibilitatea crearii unui tipar legal international. Cauza principala a acestor situati controversate este o definire insuficienta a termenilor de terorism si terorism cibernetic.

In ceea ce priveste terorismul cibernetic definitiile acestuia variaza de la simpla utilizare a internetului de catre teroristi, de exemplu folosirea servicilor de emali, etc., in faza de pregatire a atacurilor teroriste, pana la cazuri concrete soldate cu daune virtuale sau materiale.

Una dintre definitiile criminalitatii informatice este “orice actiune ilegala in care un calculator constituie instrumentul sau obiectul delictului, astfel spus orice infractiune al carei mijloc sau scop este influentarea functiei unui calculator.”

Grupul de experţi reuniţi în cadrul OCDE a adoptat o definiţie de lucru sub forma: „abuzul informatic este orice comportament ilegal sau contrar eticii sau neautorizat care priveşte un tratament automat de date şi/sau o transmitere de date”.

Biroul Federal de Investigaţii a oferit urmatoarea definiţie lucrativă: „ cyber- terorismul este atacul premeditat, motivat politic împotriva informaţiei, sistemelor informatice, programelor informatice şi datelor, rezultând în violenţa împotriva ţintelor noncombatante, de către grupări sub-naţionale sau agenţi clandestini"[1, 7].

Cyber-teroristul este întâlnit numai în spaţiul virtual şi nu va distruge fizic infrastructura care susţine existenţa spaţiului virtual. Spre deosebire de cyber-terorism, acţiunile teroriştilor informatici au efect asupra persoanelor reale, aceştia acţionând în lumea virtuală a cyber-spaţiului pentru a manipula persoanele alese ca ţinte.

Pentru a determina efectele terorismului cibernetic şi urmările utilizării internetului în scopuri teroriste pe lângă analiza atacurilor şi a datelor culese până în acest moment, trebuie să se determine riscurile care pot să apară în urma utilizării internetului şi modul care conduce la apariţia atacurilor cibernetice [2]. Cazurile cele mai întâlnite sunt reprezentate de atacurile teroriste care acţionează prin intermediul internetului, astfel de atacuri pot fi direcţionate către alte infrastructuri informatice, de exemplu calculatoare personale, servere, modemuri sau alte obiecte din lumea reală, de exemplu clădiri, aeronave, trenuri, sau chiar asupra vieţii umane [3].

Toate aceste atacuri teroriste informatice pot avea loc numai cu ajutorul unor programe specializate utilizate de către persoane care sunt dotate cu aptitudini şi cunoştinţe specifice domeniului informatic, şi aceste atacuri reprezintă cele mai periculase tipuri de atacuri cibernetice teroriste. Criminalitatea informatică se bazează pe informatizarea activităţilor din domenii diferite ale vietii sociale şi existenta unor reţele de calculatoare. Aceste reţele pot gestiona baze de date şi se pot realiza o serie de operaţiuni financiare folosindu-se sistemele de plată electronice. De asemenea, se măreşte numărul utilizatorilor sistemelor de calcul electronic şi a reţelei Internet în comiterea unor infracţiuni de drept comun (prostitutia, proxenestismul, pornografia infantila, falsificarea de documente, santajul etc.)

Organizaţiile teroriste utilizează ca şi mijloc de comunicare Internetul. Cu ajutorul site-urile create pe World Wide Web, aceştia îşi propagă intens ideologiile pe care le-au îmbrăţişat, utilizând Internetul ca vector principal al legitimării lor ideologice [4].

Prin folosirea reţelei Internet se poate pastra confidenţialitatea comunicărilor între membrii organizaţiilor teroriste, şi totodată se poate realiza accesul la informaţiile care sunt utilizate la pregătirea atacurilor, de exemplu: planurile de construcţie a unor clădiri sau părţi ale infrastructurii, imagini prin satelit, schiţe pentru a construii dispozitive explosive. În concluzie fenomenul terorist la nivel global se poate desfăşura direct prin intermediul internetului-terorismul cibernetic, cât şi indirect, prin folosirea sistemelor informatice în reţelele de comunicare,în operaţiile de culegere a informaţiilor necesare pregaâătiri atacurilor teroriste, terorismul "clasic".

În prezent, ciberspaţiul a devenit coloana vertebrală a ceea ce numim societatea informaţională. Societatea Informaţională - Societatea Cunoaşterii (SI-SC) este concepută ca un mediu foarte diferit, fără precedent, în care implementarea ultimelor realizări tehnice trebuie să meargă în paralel cu adoptarea de noi soluţii juridice care să monitorizeze efectele negative ale impactului utilizării TIC [5].

3. CONCEPTUL DE INFRASTRUCTURA INFORMAŢIONALA

Din punct de vedere fizic, infrastructura informaţională reprezintă într-o formă de interconectare a tuturor reţelelor de comunicaţii electronice (de diferite tipuri, pe diferite medii), calculatoarele (ca hardware şi software, inclusiv dispozitivele periferice şi terminalele), datele, informaţiile şi cunoştinţele (generate, depozitate, transferate, prelucrate) cu serviciile aferente, inclusiv oamenii, care trăiesc, muncesc, învaţă, se relaxează/odihnesc, ca utilizatori/beneficiari ai unor servicii şi produse noi [6].

Teoretic se pot executa atacuri informatice deoarece nici un sistem informatic nu este protejat în totalitate, iar majoritatea computerelor, chiar şi cele din infrastructura critică sunt conectate la o reţea sau direct la Internet. Calculatoarele care nu sunt conectate la reţea pot fi virusate prin mai multe moduri, de exemplu, prin intermediul unui stick USB virusat.

În literatura de specialitate se precizează faptul ca infrastructura critică (de exemplu: infrastructura care coordoneaza sistemele de producere şi de transport energie ,cea care coordoneaza zborurile pe un aeroport sau infrastructura care controlează parametrii critici din instalaţii industriale) nu este niciodata în totalitate protejată şi teoreticpoate fi oricând atacata cibernetic.

Unul dintre factorii care favorizează apariţia atacurilor cibernetice este tocmai factorul uman. Motivul poate fi reprezentat de o instruire nesatisfăcătoare a factorului uman sau superficialitatea cu care se rezolvă îndatoririle de servici. Alt factor care favorizează apariţia atacurilor cibernetice constă în nesecurizarea corespunzătoare a sistemelor din cadrul organizaţiilor

4. ATACURI PRIN INTERMEDIUL REŢELEI INTERNET

Internetul este la fel de accesibil teroriştilor şi organizaţiilor teroriste ca şi pentru restul populaţiei, iar infracţiunile cibernetice, infracţiunile comise prin utilizarea infrastructurii şi structurilor informatice, au fost înregistrate încă de la începuturile erei informatice [2]. Ca urmare, exista posibilitatea apariţiei atacurilor cibernetice teroriste, dar până în prezent nici o organziaţie terorista, cu excepţia organizaţiei numită Anonymus, organizaţie care a confirmat că este formată din hackeri activisti (hacktivists), nu a revendicat atacuri cibernetice. Unul dintre cel mai cunoscut atac cibernetic dat a avut ca consecinţă scăderea vitezei reţelei Internet la nivel global. Atacul a fost comis prin intermediul unor hackeri est-europeni. Conform experţilor, un conflict între un grup care luptă împotriva mesajelor de tip spam şi o companie de găzduire web a condus la atacuri cibernetice care au afectat infrastructura principală a Internetului. Atacurile au afectat servicii de web precum Netflix. Specialiştii avertizează că există riscul blocării serviciilor bancare şi a celor de e-mail. Grupul Spamhaus, cu sedii la Genova şi Londra, este specializat în furnizarea de filtre care să blocheze mesajele de tip spam. Pentru a realiza aceste filtre, firma a creat o bază electronică a serverelor care se utilizau pentru trimiterea de spam.

De la teorie la practica

Virusul Stuxnet prezintă câteva elemente specifice care au capacitatea de a ataca informatic infrastructura critică având ca rezultat o funcţionare necorespunzătoare a infrastructurii care poate duce la apariţia unor urmări grave ca de exemplu:

- explozii de instalatii industriale;
- virusul infecteaza computerele prin stick USB;
- se propagă în reţea prin metoda peer to peer;

- dacă calculatorul infectat nu coordonează procese industriale efectul virusul consta în multiplicarea acestuia având ca scop răspândirea acestuia.
- dacă virusul infectează un calculator care coordonează procese industriale acesta caută conexiunile dispozitivelor digitale de coordonare a proceselor industriale;
- monitorizeaza activitatea dispozitive de coordonare şi le reprogramează;
- operatorul nu poate descoperii infectarea şi reprogramarea dispozitivelor de coordonare decât când răul a fost produs;
- existenţa virusului a fost descoperită dupa ce a infectat computere industriale din mai multe ţări;
- pentru a se multiplica virusul utilizează 4 vulnerabilităţi necunoscute anterior ale sistemului Windows

Acest virus a fost denumit în media "prima arma informatică în adevăratul sens al cuvantului" şi nu a produs încă o explozie dar avem un precedent şi există un obiect de studiu pentru crearea de eventuale alte astfel de programe şi variante de atac cu urmări posibil grave.

5. CONCLUZII

Incriminarea acestor infracţiuni informatice este dificilă datorită extinderii şi complexităţii reţelei Internet existentă în diferite ţări şi care au legislaţii diferite. Ca urmare, apare o nesincronizare a actelor normative din ţările respective şi care conduc la o rezolvare dificilă a infracţiunilor legate de utilizarea abuzivă a spaţiului cibernetic.

Uniunea Europeană nu a ajuns la o abordare comună în acest domeniu, cadrul legislativ existent nu poate asigura rezolvări optime şi nici să asigure o protecţie perfectă a utilizatorilor produselor informatice în faţa acţiunilor informatice apărute.

Ţara noastră se numară printre ţările care au luat o serie de măsuri legislative pentru eliminarea infracţiunilor informatice.

BIBLIOGRAFIE

[1] **Imran Awan**, *Debating the term cyber-terrorism: issues and problems*, Internet Journal of Criminology © 2014, ISSN 2045 6743 (Online)
[2] **B. Foltz**, *Cyberterrorism, computercrime, and reality*, InformationManagement & Computer Security, 15.03.2004,Vol.12,No.2, pp.154-166

[3] **Sieber, Ulrich / Brunst, Phillip**, *Cyberterrorism and Other Use of the Internet for Terrorist Purposes* – Threat Analysis and Evaluation of International Conventions. En: Council of Europe (Ed.): Cyberterrorism – the use of the Internet for terrorist purposes. Strasbourg, Council of Europe Publishing, 2007, págs. 9 - 105.
[4] **Le Doran, Serge et Philippe Rosé**, *Cyber mafias*, Paris, Denoël, 1998. HV6773 L42. op. cit., p. 205.
[5] Acad. **Mihai Drăgănescu**, *Societatea informaţională şi a cunoşterii. Vectorii societăţii cunoaşterii*, Bucureşti, Editura Tehnică, 2003.
[6] http://www.mtic.gov.md/
[7] www.internetjournalofcriminology.com

PREVENTION OF CYBER TERRORISM

Ileana ŞTEFAN[1]

[1]Universitatea "Petru Maior" din Tîrgu–Mureş

Str. Nicolae Iorga, nr.1, Tîrgu – Mureş, MUREŞ, 540088, România

Abstract: *The thesis presents a theoretical approach of the concept of cyber terrorism, the way it appeared and the development of conceptual definitions and limitations, as well as the economic dimension of the phenomenon. The research highlights the appearance and development of this phenomenon, followed by the presentation of the existing definitions of identity theft, while trying to set its correlations to the identity fraud. It is also a description of the socio-economic implications of the offence.*

Keywords*: terrorist offence, Cyber attacks,* Cyberspace, *Cybercrime*

JEL Classification: K OO, K23

[1] Ileana Ştefan, tel./fax/ :+40744678844, e-mail:stefan.ileana@yahoo.com

1 INTRODUCTION

The article presents a theoretical approach to the concept of cyber terrorism, the beginning and development of conceptual definitions and limitations and economic dimension of the phenomenon. The research highlights the beginning and development of this phenomenon, followed by the presentation of the existing definitions of identity theft while trying to establish relationships between her and identity fraud. Also is a presentation of the socio-economic implications of the offence.

The use of computer networks leads to a series of advantages, as well as of disadvantages. One of the biggest disadvantages is represented by the cyber crime that consists of illegal activities committed by the help of the computer systems and of the Internet.

An essential condition for the humankind development consists in the unique identification of each member of the society. Together with the need of identifying the various people there appeared the identity theft under different incipient forms. The development of the computer system environment and of the remote means of communication has facilitated the increase of the identity theft phenomenon that undertook new forms and dimensions. One of the most often met cybercrime forms is the identity theft, where the Internet is used by offenders in order to steal personal information from other internet users.

2. THE DEFINITION OF CYBER TERRORISM

The cyber terrorism represents the most often met cybercime within the online environment, being a very complex and internationally spread offence.

The cybercrime represents a criminal activity, the object of the offense consisting in using the computer and the Internet network.

This phenomenon is differently defined by specialists in this field, not reaching a unanimously accepted definition due to the complexity of this offending act, and the various regulating manners of the cyber terrorism in each state have led to the impossibility of creating an international legal pattern. The main cause of these controverted situations is the insufficient definition of the following terms: terrorism and cyber terrorism.

As far as the cyber terrorism is concerned, its definitions vary from the simple use of Internet by the terrorists, for example the use of e-mail services, etc., during the terrorist attacks preparation stage, to concrete cases that caused virtual and material damages.

One of the cyber terrorism definition is “all the illegal actions where a computer is the offense tool or subject, that is all the offenses whose mean or purpose is to influence upon the computer function.”

The group of experts reunited within OCDE have adopted a work definition as it follows: „the cyber abuse is any illegal, unethical or unauthorized behavior concerning an automated data processing or data transmission”.

The Federal Bureau of Investigations has provided the following work definition: „the cyber-terrorism is the premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents".[1, 7]

The cyber-terrorist can be met exclusively in the virtual space and will not physically destroy the infrastructure supporting the existence of the virtual space. Unlike the cyber-terrorism, the actions of the information technology terrorists have effect upon the real persons and they act in the virtual world of the cyber space in order to manipulate the persons that were chosen as targets.

In order to determine the effects of cyber terrorism and the consequences of using the Internet for terrorist purposes, along with the attack analysis and the collected data so far, there should be determined the risks that might appear from the use of Internet and the manner that leads to the appearance of the cyber-attacks.[2] The most often met cases are represented by the terrorist attacks that act by Internet, such attacks can be directed to other cyber infrastructures, for example to personal computers, servers, modems or other objects from the real world, for example buildings, aircrafts, trains or even to human lives.[3]

All these terrorist attacks can happen only by the help of some specialized programs used by persons that have abilities and knowledge specific to the computer technology field, and these attacks represent the most dangerous types of cyber terrorist attacks. The cyber-crime is based on the cybernation of the activities from various fields of the social life and on the existence of a series of computer networks. These networks manage databases and make a series of financial operations, using the electronic payment systems. The number of electronic computing systems

and of Internet networks users in committing some offenses of common-law (prostitution, procuring, child pornography, document forgery, blackmail, etc.) is in continuous growth.

Terrorist organizations use as communication means the Internet. By the help of the sites created on World Wide Web, they intensely transmit the ideologies they embraced, using the Internet as the main factor of their ideological legitimation.[4]

By using the Internet network, there can kept the privacy of the communication among the members of the terrorist organizations and they can also have access to the information that are used for the attacks planning, as for example: construction plans of buildings or parts of infrastructure, satellite images, plans for the construction explosive devices. Thus, the terrorist phenomenon worldwide can unfold directly by internet – cyber terrorism, as well as indirectly, by using the cyber systems in the communication networks, in the operations of collecting the information necessary to the planning of terrorist attacks, "classic" terrorism.

Nowadays, the cyberspace has become the spine of what we call cyber society. Societatea Informaţională - Societatea Cunoaşterii (SI-SC) – *Cyber and Knowledge Society* is created as a very different unprecedented environment, where the application of the latest technical achievements should work simultaneously with the adoption of new legal solutions to monitor the negative effects of TIC use impact.[5]

3. CYBER INFRASTRUCTURE CONCEPT

Physically speaking, the cyber infrastructure represents in a form of interconnection of all electronic communication networks (of various types, on different environments), the computers (hardware and software, including the peripheral and terminal devices), the data and the knowledge (generated, deposited, transferred, processed) with the due services and people that work, learn, relax/rest, as users/beneficiaries of some new services and products.[6]

Theoretically there can be performed cyber-attacks, because no cyber system is completely protected, and most computers, even those belonging to the critical infrastructure are connected to a network or directly to the Internet. The computers that are not connected to the network can be infected by using various ways, for example, by using an infected USB stick.

In the specialized literature, there is mentioned that the critical infrastructure (for example: the infrastructure that coordinates the energy production and transport, the one that coordinates the flights of an airport or the infrastructure that controls the critical parameters in

the industrial equipment) is never fully protected and theoretically can be at all times cyber attacked.

One of the factors that favor the appearance of cyber-attacks is the human factor. The reason can be an unsatisfactory training of the human factor or the superficiality solving the job duties. Another factor leading to the appearance of cyber-attacks consists in the fact that the systems within the organization are not properly secured.

4. INTERNET ATTACKS

The Internet is as accessible to the terrorists and to the terrorist organizations as it is for the rest of the population, and the cyber-crimes, crimes committed by using the infrastructure and the cyber structures have been registered since the beginning of the cyber era.[2] Consequently, there is the possibility that terrorist cyber-attacks might appear, but up to the present moment no terrorist organization, except the organization called Anonymous that confirmed that is made of hacktivists, has claimed cyber-attacks. One of the most known cyber-attacks had as consequence the reduction of the Internet speed globally. According to the experts, a conflict between a group fighting against spam messages and a web hosting company has led to cyber-attacks that affected the main Internet infrastructure. The attacks affected web services as for example Netflix. The specialists warn that there is the risk of blocking the banking and e-mail services. Spamhaus Group, with the headquarters at Genoa and London is specialized in providing filters that block spam messages. In order to create these filters, the company built an electronic base of the servers that were used to send spam.

From theory to practice

Stuxnet virus presents several specific elements that have the capacity to cyber attack the critical infrastructure, having as result an improper infrastructure functioning that might lead to serious consequences, as for example:

- explosions at industrial equipment;
- the virus infects the computers by using USB stick;
- propagates in the network using peer to peer method;

- if the infected computer does not coordinate the industrial processes, the effect of the virus consists in its multiplication having as purpose its propagation.
- if the virus infects a computer that coordinates industrial processes, it searches the connections of the coordination digital devices of the industrial processes;
- monitors the activity of the coordination devices and reprograms them;
- the operator cannot discover the fact that the devices were infected and reprogrammed until the damage has been already done;
- the existence of the virus was discovered after industrial computers from several countries had been infected;
- in order to multiply itself, the virus uses 4 Windows vulnerabilities unknown before

This virus was called in the media "the first true cyber weapon" and has not produced an explosion yet, but there is a precedent and subject matter for the creation of possible other such programs and attack types with possibly serious consequences.

5. CONCLUSIONS

Incriminating these type of computer crimes is difficult due to the extention and complexity of the Internet network existing in various countries that have different legal rules and regulations. As a consequence, there appear a lack of synchronisation of these regulations from those countries that leads to a difficult resolution of the crimes related to the abusive use of the cyber space.

The European Union has not reached a commom approach in this respect, the existing legal framework cannot provide with either the best solutions or a perfect protection of the users of IT products against the computer actions that appearred.

Our country is among those countries that have taken a series of legal remedies in order to eliminate the computer crimes.

BIBLIOGRAPHY:

[1] **Imran Awan**, *Debating the term cyber-terrorism: issues and problems*, Internet Journal of Criminology © 2014, ISSN 2045 6743 (Online)
[2] **Sieber, Ulrich / Brunst, Phillip**, *Cyberterrorism and Other Use of the Internet for Terrorist Purposes* – Threat Analysis and Evaluation of International Conventions. En: Council of Europe

(Ed.): Cyberterrorism – the use of the Internet for terrorist purposes. Strasbourg, Council of Europe Publishing, 2007, págs. 9 - 105.
[3] **Le Doran, Serge et Philippe Rosé**, *Cyber mafias*, Paris, Denoël, 1998. HV6773 L42. op. cit., p. 205.
[4] Acad. **Mihai Drăgănescu**, *Societatea informaţională şi a cunoşterii. Vectorii societăţii cunoaşterii*, Bucureşti, Editura Tehnică, 2003.
[5] http://www.mtic.gov.md/
[6] www.internetjournalofcriminology.com