Cyber terrorism on the Internet, the specific realities and challenges of combat it.

Dr. Saddam Faisal Kokez Al-Mohammadi
Assistant professor of private law
Faculty of Law / University of Fallujah - Iraq

د. صدّام فيصل كوكز المحمدي
استاذ القانون الخاص المساعد
كلية القانون / جامعة الفلوجة – العراق

Abstract

The phenomenon of terrorism is traditionally a global phenomenon, has grown and evolved and increased in influence when coupled with this phenomenon environment electronic, providing internet users and them terrorists Field welcoming the "legal" for the exercise of their actions and their activities freely away from the authority of the control and spread of wider and low cost, and which increased the danger of this phenomenon is the premise of the traditional coupling terrorism with electronic terrorism, when terrorists used electronic means and techniques that are linked to the Internet, it is true that the impact so far did not exceed the limits of the effects of terrorism, electronic criminal operations that fall within the framework of cyber crimes, but the studies specialized propositions and the current focus on the issue of the possibility of terrorists exploit the Internet as it can target the sites infrastructure and technical and technological and even military, and that can cause a complete standstill if there were facilities for all life in the target country.

Keywords: Cyber-terrorism, terrorist groups, the challenges, and the means of electronic terrorism, combating- electronic terrorism .

الملخص

تعد ظاهرة الارهاب تقليديا ظاهرة عالمية، وقد نمت و تطورت وزادت في تأثيرها عندما اقترنت هذه الظاهرة بالبيئة الالكترونية، حيث وفّرت شبكة الانترنت لمستخدميها و منهم الارهابيون الميدان الرحب "المشروع" لممارسة انشطتهم و فعالياتهم بحرية بعيدا عن سلطة الرقابة و بانتشار اوسع و بكلفة قليلة،
و مما زاد في خطورة هذه الظاهرة هو فرضية اقتران الارهاب التقليدي بالارهاب الالكتروني،عندما يستخدم الارهابيون الوسائل الالكترونية والتقنيات التي ترتبط بشبكة الانترنت، صحيح ان تأثيره لحد الان لم يتجاوز تأثيرات الارهاب الالكتروني حدود العمليات الاجرامية التي تدخل ضمن اطار الجرائم السيبرانية،الا ان الدراسات المتخصصة و الطروحات الحالية تركز على مسألة امكانية استغلال الارهابيين للانترنت على النحو الذي يمكن ان يستهدفون به مواقع البنى التحتية و التقنية و التكنولوجية و حتى العسكرية، والتي يمكن ان تتسبب لو حدثت بالشلل التام لكل مرافق الحياة في الدولة المستهدفة .

الكلمات المفتاحية: الارهاب السيبراني، الجماعات الارهابية، التحديات، وسائل الارهاب الالكتروني، مكافحة الارهاب الالكتروني.

Introduction

The phenomenon of terrorism and of which E-terrorism is a global security issue and the national most pressing faced by all countries around the world, and this became dramatically clear to the shock in the September 11, 2001, and the problem is that terrorism-mail has become a long-term threat requires a full commitment by the United States and the international community to eliminate on terrorism, whether individuals or terrorist organizations wherever they exist.

And here it is necessary to grasp the fact that the increasing presence of modern terrorism on the Internet is actually normal for the blending of two major trends as a result of:

- The spread of democracy and the ease of communication that facilitates the delivery of content presented to users on the Internet.

- Growing awareness of the terrorists and the growing potential of the Internet that achieve their purposes.

But this was and the Internet is still the scene optimal choice for terrorists and will remain so for a long time, Decentralization and the provision of non-disclosure of the user's identity represent the most important ,The advantage can be nearly this network for terrorists ideal environment to work, as it can not be that the Internet is subject to control or restrict because of it's subject allows access to anyone who wants it.

The problem in the fact that large and small terrorist groups as well as individuals, each has its own positions on the internet they can through the use of this network both for the dissemination of propaganda, or to raise funds, money laundering, or to recruit and train new members, or to secure means of communication or a communication and facilitate coordination and conspiracy and planning attacks, and other risks that could fall within the framework of terrorist acts.

And now operates hundreds of sites on the Internet, and arise, and many others each year show, as well as sites on the Internet, and is constantly increasing, and the terrorists at the moment also rely on e-mail, chat rooms and groups of e-mail, forums, The boards of default messages, as well as resources such as YouTube, Facebook, Google Earth and others in achieving their goals, both to spread its ideas and narratives in or carry out terrorist acts.

And raise the fight against terrorism online issue of countermeasures by states or targeted institutions and cost, since the advent of the Internet to this moment and methods of combating terrorism is renewed and resort the states to develop specialized in all parts of the world and the security agencies operating on the Internet, especially since the warnings in succession from here and there, both at the level of official statements and unofficial growing ability of terrorists at this time to use the Internet, both global communications, as well as to launch an electronic vital installations and infrastructure attacks in the flag States Collect, not least because they face the developed world including the United States and the European Union countries of terrorist threats to launch cyberattacks over the network daily and increasingly.

Recently, it many security services and the specialized agencies began to focus on Internet control, and track terrorists who use them, as well as monitoring the Internet messages incoming and outgoing from the terrorists, has this many attempts security devices, each series and others, including public, for the application of various systems and defense mechanisms against terrorists on the Internet.

1- The Legal regulation of the Internet:

The spread of the Internet is limited and seclusion heavily marketed by the world as a whole, reason not the need for the organization to deal with it through its own legal system legislation, as it was seen that the last he had interfered unnecessary.

However, the information revolution unleashed by the internet marketing and the spread of use and diversity of the areas to take advantage of them in the whole world and ways and methods were not known in advance, something that would lead to the explosive growth of the countries connected to the Internet, not states not realize that the use of growing computers would rely on the growing computer systems lead to computerize all daily activities and for various services in the country and that such services may expose the country to some weaknesses, such as a potential Launched from different directions against Systems that working across the network attacks.

Internet has brought around the physical challenges of the world and that existed before the Internet marketing, and what was Internet depends network in existence on the electronic media, the risks they are exposed to these many ways and variety, which was born in the belief among many that he can not meet these challenges the risk that deviate electronic media and software related without the involvement of law and in many cases, not only at the national level, but that the international character of the network showed there is a need for cooperation between different countries to address legal issues such as copyright infringement and cyber crime on an international scale. [1]

Whereas the fact that there is no central entity that governs the Internet, the many countries at the beginning of it now issue and implement the various laws to address issues arising from electronic media applications and as part of its sovereignty, and is ordered to pay other countries because the show a little attention to the legal regulation Similar to the issues on its territory, and at this stage carried nations legal regulation of the Internet at the local level without giving any consideration to the enforcement of laws regulating network Internet on the international level.[2]

However, soon they realized that refer to the characteristics of the Internet self and universality, as well as skip risk limits of a single state, which was favored when many countries in the need to consolidate the trends and the general principles approved by the local laws to be consistent with the laws of other countries and in order to combat cross-border crimes and terrorism.

Moreover, what was it (controls) under which Internet service providers liable working on Internet service (ISP) parts of the network within the national borders of a country controls what, the legal regulation on the Internet can not be implemented effectively and successfully without the help of the ISP. In addition to that there are some "powers" that dominate the development of laws governing the use of the Internet, in terms of status and the nature and content of the legal regulation of the issues related to the Internet, and this means that you must decide to what extent can extend the influence of these "powers" on laws governing the use of the Internet in countries that fall outside the scope of the "great powers" Home in the world.

2- The problems of crime and terrorism on the Internet :

In fact we not surprising that opposes the interests of different players lead to conflict, it can be asked whether the expectations of the human rights of Internet users are reasonable, taking into account the spread of Internet use in the commission of serious crimes, as well as the threat posed by terrorism. Commit cyber crime and terrorism is undeniably harmful to the Internet community as a whole, and adversely affect the growth of confidence in the use of the Internet. In addition, you must decide whether the State used control methods, constitutes a violation of human rights in a reasonable Internet user ?

Is it possible, for example, to monitor and / or retention of communications all Internet users, regardless of whether the user is a suspect or not? In many cases today, and ISP bears the legal burden to ensure the technical enforcement to monitor the state.[3]

In this regard, one should look at the involvement of ISPs when drafting legislation and not only at the stage of implementation of laws. Should be asked whether the obligations imposed on reasonable ISPs within the evolution of the Internet from the informal to the medium regulator.

3-1/ The reality of the Internet in light of e-crime and cyber terrorism:

Terrorism is a national security issue most pressing facing the United States and its allies around the world. This became clear in the shocking September 11, 2001 and promises to be a long-term threat requires a full commitment by the United States to eliminate the terrorist organizations wherever they are.

Has identified the former vice president of the Center for the fight against terrorism, the four elements of the CIA that are common to all acts of terrorism, where in spite of the diversity of images of such attacks in cyberspace, they still appear on the four elements common to all acts of terrorism:[4]

1- premeditated and not abstract acts as breed of terrorist attacks to carry out an attack.

2- political aims to influence the political structure cyberterrorism is an act that aims to completely destroy the computer system. Cyber-terrorists are hackers

with political motives, their attacks can affect the political structure of this corruption and destruction.[5]

3- that target civilians and civilian facilities terrorist attacks Cyber civil institutions, Qualifies as terrorism, cyber attack that leads to violence against persons or property[6], or at least cause enough harm to generate fear.

4- Cyber terrorism has become a substitute for conventional armies that fight conventional wars, and in some cases exclusive of electronic warfare, information warfare, which are attacks on the computer network connected to the Internet.

Electronic warfare is the last term is of several terms used to describe various aspects of defense and attack information and computer networks in cyberspace, as well as the denial of an opponent's ability to do the same[7]. Electronic warfare and information warfare employs information technology as a tool of war to attack the enemy's sensitive computer systems.[8]

3-2/ How to use the Internet by the terrorists

All terrorist organizations in the world today, have their own sites on the Internet,[9] which is using this medium for advertising, and to raise funds, or money laundering, or even to recruit and train terrorists, and the modern use of the Internet is also a key element in the concept of terrorism and psychological warfare, and in fact the case today could be a terror computational reality because of what to attack your computer from the possibility to do the actions can only be described a disastrous, such as dropping aircraft, and destroy the infrastructure of biotechnology, and the destruction of the stock market, and reveal state secrets, etc.

as well as the lack of expected effects of what will happen after that the effects of the tent can infect all aspects of public life and private. . .

It is clear that the Internet enables small groups of work force and makes it look more capable than they might be in fact, even the threat of turning into a kind of virtual fear, because the network allows terrorists to amplify the consequences of their activities with messages for follow-up and threats directly to the general population, although that terrorist groups may be completely unable to act in the physical world.

And the fact that the Internet allows a person or group to appear to be larger or more important or threatening than it is already.[10]

3-2-1/ The Advantages of the Internet that exploited modern terrorism:

great virtues of the Internet Was converted for ease of access, and the lack of regulation, the vast potential of the masses, and fast flow of information, and multimedia applications and so forth to take advantage of groups committed to terrorize communities to achieve teir goals.

Internet takes very little skill to use, has a small number of systems and provides the public all over the world who can send information quickly and at low cost, and allows the user anonymity.[11]

It allows terrorists to engage in activities which with minimal risk, and is in fact the Internet is very attractive to terrorists, to provide them with the non-disclosure of the name, as well as easy accessible from everywhere, as it gives them the option to post messages, and e-mail, upload or download information and hide in the dark again. [12]

And the most prominent example of this is that the Internet has become a valuable tool for al-Qaeda, not only to coordinate operations and launch attacks, but also like virtual camps training and indoctrination, and employment. [13]

In fact, the web of al-Qaeda has become what he calls the Online University of terrorism experts, as they are published more than 300 new pages of codes and manuals and instructions, and rhetoric on the Internet per month, search is no longer necessary for the supporters of al-Qaeda and its supporters to join in the training camp military, or travel to another country because a person can learn alone, or with other brothers, in the Internet and pass setup.

Ironically, the decentralization of the Internet was necessary for the liberalization of the telecommunications and secured between the security agencies of the United States in its work in the face of the fear of the Soviet Union days of the Cold War, and is now working in the interests of the greatest enemy of the security services since the end of the Cold War and it is only international terrorism, as the modern terrorist groups working to make full use of the Internet for communication between the group itself or the work of the Special Group's internal networks.[14]

Al-Qaeda, for example, has shown itself to be remarkably intelligent entity, he can cope with the difficulties and risks and challenges, mainly due to its decentralized structure based on the decentralized online course.[15]

And the Internet by its very nature, is in many yard perfect for the activities of terrorist organizations, ways, and in particular, the largest field of terrorism, provides many advantages, including:

1- Ease of access.

2- lack or weakness of any regulation or control, or other forms of government control.

3- The possibility of deployment on the level of potentially huge audiences all over the world;

4- anonymity while communication;

5- Fast flow of information confidentiality;

6- react quickly and accurately.

7- possibility is charged with the development and maintenance of the existence of the Internet.

8- The presence of a variety of multimedia environment to express their opinion, the ability to combine text, graphics, audio and video.

9- allow users to upload and download movies, songs, books, posters, etc.

10- The ability to shape coverage in the traditional media, which are increasingly used the Internet as a source of stories.

The problem is that all of these benefits did not go unnoticed by terrorist organizations, regardless of their political or ideological tendencies so today we find that almost all terrorist organizations active through its Web sites, but many of them are working to be have more than web sites and become one of them used several different languages to promote her ideas and beliefs. [16]

Often shed reports issued by specializing in US institutions that light on the uses of the Internet by al-Qaeda before the implementation of 11/9 attacks, which include search the Web for information about flight schools in the United States, using the online processing kidnappers contacts with e-mail accounts, and coordinate the actions of the attackers using e-mail, Web pages and download anti-American, and the collection of flight information.[17]

3-2-2/ The Cyber terrorism in the internet:

The threat posed by cyber-terrorism has held the attention of the media in most spaces, and started at the present time is to address this phenomenon as a form of threat to the security of society, and the information technology industry.

And had assumed the journalists, politicians and experts in a variety of areas and a popular scenario in which in which terrorism, cyber talk infiltration electronically to computers that control the dams or air traffic and to generate electricity and control traffic and railways and ports and other vital interests in the stations control systems the lives of the people in the state, and thus wreak havoc and threaten not only millions of lives, and this means that the National Security itself will be vulnerable to sabotage, because the most important in Western societies network infrastructure is managed through computers, and the potential threat of terrorism, cyber thus be a cause for concern dramatically, and experience has proven that hackers - but were not their motives are the same goals that inspire terrorists - have proven that they have access to sensitive information and disrupt operation of essential services.

At least in theory, could follow the example of terrorists pirates, and thus penetrate the government and your own central server computer systems, paralyzing or disrupt military and financial sectors, and service economies in the developed countries, and the reason for all this risk is due to the increasing reliance in communities developed countries information and communication technology, which peppered a new form of security weaknesses by giving terrorists the opportunity to approach the targets that would be otherwise can not be compensated and fully confront, such as national defense systems and air traffic and other control, and is This means that whenever the country was more advanced in terms of technology were more susceptible to electronic attacks may encounter technical infrastructure.

So,What should be considered cyber-terrorism?

Dorothy Denning provided a clear definition of unambiguous cyber terrorism in many of her articles :

When she said that " … cyber terrorism is cyberspace and terrorism affinity, and here refers to the attacks and illegal threats against computers, networks, and information stored in them carried out to intimidate or coerce the government or citizens of the country in furtherance of political or social objectives.

Moreover, and as described, it should be that terrorism leads cybersecurity as an attack on violence against persons or property, or at least cause enough harm to generate fear, and that the attacks that lead to death or bodily injury, explosions, or significant economic loss to be examples, attacks serious against vital infrastructure can rely on acts of cyber terrorism, depending on the impact, and attacks by non-essential services or that are mainly would inconvenience expensive does not crash …" .[18]

It is important to distinguish between cyber terrorism, piracy, and the extent to which can limit their terms coined by scientists to describe the Interdependence of piracy and political activity.

Programmatic struggle, although politically motivated, does not constitute a cyber-terrorism or piracy, because the objective is to protest not disruption, and they do not want the murder or mutilation or terrorism, however, the struggle script does highlight the risk of cyber-terrorism.

Individuals with lack of moral discipline likely to be used methods similar to those developed by hackers to wreak havoc as they are terrorists.

Moreover, the line between cyber-terrorism and piracy or struggle compiler may mixing the fairly effacement sometimes, especially if terrorist groups are able to recruit or hire computer hackers who have the savvy or if the pirates decided to step up their work by attacking the systems that run the basic elements the infrastructure of the target country.[19]

Cyber-terrorism, and the emergence of "computer age" has produced a boom and there are already well-known threat of fear and a lot of this kind of terrorism, and unfortunately, this new danger has not completely gain the attention of the public more aware and educated and even official institutions.

Also there should be a distinction between the terrorists who take advantage of the technology available, and they are terrorists, cyber and terrorists traditional, and who may increase their arsenal of more conservative methods, such as bombings, kidnappings, and murder, and new methods such as computer viruses, and Penetration radio frequencies, and attacks "denial of service."

However, it can also be the presence of the terrorist cyber pure, this diversity of images and the sources of terrorism may do so without the traditional terrorism approach, rather than the exploitation of computer technology to put them into the demands of the impact, and the ransom, or the destruction caused to the world's population in general, in addition, cyber terrorist can achieve these goals without exposing himself to the actual harm.

4/ The Internet field fertile environment for the production of cyber terrorism.

4-1/ Production terrorism traditional manner

Directed media emergence of terrorism, which led many experts in the field of communications and terrorism to re-modern concept of terrorism in the actual production of communication framework, and a perfect act of cyber terrorism can be analyzed like a lot of other means of communication, and consists of four basic elements:

1. transmitter (terrorist),
2. intended recipient (target),
3. The message (of the bombing, ambush), and
4. Feedback (Reply target audience reaction).[20]

In fact, Ralph Dowling suggested applying a new concept of confrontation talk of a new kind of terrorism, and argued that the terrorists have the ability to engage in frequent rhetorical forms that force the media to provide access without which terrorism can not meet its objectives.[21]

Moreover, some terrorist events have become short of terrorism,[22] and that could be better analyzed by the media, which depicts the event.[23]

4-2/ The production of modern cyber terrorism on the Internet

Terrorists today in the world of postmodern enabled to take advantage of the benefits of globalization, especially the most advanced modern technologies technology and including communications planning and coordination and implementation of campaigns deadly, so that these attacks are no longer restricted geographically within a given region, politically or financially dependent on a particular country, they rely advanced communications such as the Internet, and related to terrorism and the Internet in two ways:

First, the Internet represents a very large forum for each of the terrorist groups and individual terrorists to spread their messages of hate and violence, to communicate with each other and with their supporters and sympathizers, and even to launch a psychological war against their enemies.

Second, individuals and groups to attack computer networks, including the Internet, in what became known as - or cyber terrorism - electronic warfare. Currently, the terrorists use and misuse of the internet for their own benefit rather than attack it.

4-3/ The Cyber terrorism in the new environment:

It is known that the extent of the impact of the new terrorism in the present day is cross-border and changing forms and types of terrorism today than it was last time through the change key trends related to these trans-national groups are:

1. Development / ad hoc groups as preferred method of work of loose networks.
2. a new attitude toward violence, including suicide bombings.

3. religious groups rather than on the basis of nationality.

4. operations facilitated communications and information technology (ICT) and mobile technologies;

5. ideas and worldviews connect to each other, rather than just political ambitions.

6. they have less need to take care of the direct state;

7. groups appeal to the Diaspora and not just local audiences; and

8. They have the ability to use chemical, biological, radiological and nuclear weapons materials.[24]

5/ The Practical applications to take advantage of the Internet by terrorists

In addition to the terrorists' use of communication services and communication over the Internet, they were able to use the Internet applications as a means to achieve a useful purpose for them, as the Internet serves the terrorists as an excellent source of useful information, because it is the World Wide Web, which contains the largest data storage file free information and and that can link to it easily and pleased. [25]

Many of tools are available on the internet, which means to facilitate the collection of data of deferent kinds of informations, the so-called search engines, including the database, and lists of e-mail distribution and chat rooms, discussion groups, and many web sites who provide search tools to their own information extraction databases on their sites, and that the search by title or word from newspapers and magazines can also generate useful information and is free to the terrorists on the Internet, some of this information may also be available in the traditional media, but the search capabilities on the Internet allow terrorists to get them with complete anonymity and with very little effort or cost.

According to a statement made by USA Defense Secretary Donald Rumsfeld, the readers of training to al Qaeda guide the growing number of insiders after the war in Afghanistan, and began to use public sources openly and without resorting to illegal means, it is possible to easily collect 80 per cent at least of all required information about the enemy, and so the terror without employing these features can not prevail or survive, and even been Evolves, and then provides recruiting killers and bombers, kidnappers, torturers, and engineers, and soldiers of the armies of terrorism in the future, the Internet has become a useful tool Talk to recruit terrorists. "[26]

And so, the Internet combines many advantages for recruits, for example:

1. it makes it easier to gather information to potential recruits through access to more information, more quickly, and multimedia format.

2. The global spread of the Internet allows groups to publish events for more people.

3. increase the possibilities for interactive communication, the Internet along with more opportunities to connect the group directly.

4 and also the possibility of online recruitment by terrorist organizations on a large scale, although the Internet is used more for the initial attraction, recruitment and ideological, and social support for direct employment.

5. Moreover, the process of creating blogs and sites on the Internet are more than activate the reward recruits and the suicide terrorists, and thus serves as an additional indirect employment initiative.

6. Recruits terrorists may use Internet technology to roam interactive chat rooms on the Internet to search for receptive members of the general public (especially young people) using sophisticated persuasion procedures.

7. The terrorists use the Internet to create and activate virtual training camps, also they use online communication to provide information to his fellow terrorists, including maps, and photographs, and trends, and symbols, and technical details of how to use explosives.[27]

8. Internet is home to dozens of sites that provide information on how to build explosives and chemical weapons .

9. Finally, like many other political organizations, terrorist groups are using the Internet to provide the funds, for example, al-Qaeda, has always depended heavily on donations, and is building its global network to collect donations on the basis of charities and non-governmental organizations, and institutions Other financial used Web sites and chat rooms and online forums to the poll and fundraising.[28]

5-1/ The practice of terrorism informational across cyberspace:

The concept of terrorism information rooted in the ideas that surround the information war. Description for the first time information warfare elements to be seven sub-types of the war:

1. Leadership
2. Control,
3. intelligence building,
4. E-piracy,
5. Psychology,
6. existing economic war on cyber attacks on economic interests.
7. information warfare.

Information warfare has focused in its early stages so much to exploit new technologies to gain an edge, while there was an element of psychological warfare, and it was mostly about the command and control systems and disrupt the enemy. As the potential of these techniques to influence and realized both friend and foe, and there was a concentration of new to this side.

5-2/ The Electronic attack & defence in cyberwar

1- Attack technology by using, Logic bombs, viruses, worms, spy-ware, flooding, DOS attacks, Web defacement.[29]

2- Defend technology by using:

Virus checkers, network tools, network forensics, standards, backups, intrusion detection systems, honeypots, training.

5-3/ The Exercise leadership and control of the leaders and organizers

1- Coordinating activities:

Network centric organisations using such elements as the Web, SMS, coordinated sensors, and streaming video.

2- Bind supporters and spread message:

Use the Web and the mass media to promote cause to a global audience. Use the Web to collect monies.

In another side, the Online Network Communications (CMC) is ideal for communication between terrorists, We have provided in the past that the decentralization enjoyed by the Internet, has made this network as a network can not be made subject to control or restrictions, and can not be provisions undergoing controlled completely, and it allows free access to any person anywhere in the world, and thus the structure of terrorist organizations Modern computing makes communications more relevant and useful to them.

In fact, the web sites are just one of the Internet used by terrorists now services, there are many other facilities on the Internet, e-mail, chat rooms, e-groups, forums, virtual panels that terrorists use more and more message. And use many of the sites on the Internet for terrorist psychological campaigns against hostile states and military forces, and send messages of verbal and graphic attempt to demoralize and intimidate the enemy or create a sense of guilt and doubt and division.

Terrorists use the Internet to disseminate scary footage of executions and beheadings, and deadly sniper attacks and deadly bombings to intimidate the enemy forces or the public, as they use the Internet to make threats and letters to the governments of the enemy and the population as well.[30]

5-4: The Exercise of Lobbying and influence.

1- Contemporary audience

Globalized reach of communications has given the ability to reach anyone and in anywhere.

2- Strategic communications

Influence campaigns are now an integral part of national and terrorist strategy. Each has its own targeted constituency in the globalized information environment.

3- Terrorism is psychological warfare

A. Violence as communication.

B. Goals cannot be obtained by violence alone.

C. Victims must be enlisted to gain objectives.

D. Persistent campaign with the target population increasingly perceiving (irrationally?) risk.

E. Boost its supporters, frighten it opponents.

F. Seek to undermine beliefs in the collective values of society.

Terrorists uses the victims' imagination against themselves

4- Technology of the despised West is used against it

A. Even the Taliban, who are averse to technology, had a Web site.

B. Web and other technologies such as SMS are more difficult to censor.

C. Terrorists' Web sites are better suited to their target audiences than 'of ficial' sites.

D. Effective use of video imagery on Web and, subsequently, the mass media.

5- Technology has decreased the West's dominance of mass communication.[31]

A. The terrorists' strategy is recognises the importance of having information/influence practices.

B. The importance of the media is shown by the increase in violent targeting of broadcasters by Western militaries and governments.

C. Censorship of the Web is increasing although terrorists seem to be able to combat this. It is the Mind/Influence functions that will be further discussed below Operations.

In the other side ,the influence and terrorist groups often be regarded as terrorist groups it is fighting the war asymmetric mostly psychological warfare.

Psychological warfare is a term used to describe a set of procedures, which consists of violence or the threat of violence as well as some form of psychological warfare operations, and psychological operations consist of actions such as disinformation and deception and propaganda, and show false strength, in the forms of the most successful, it can Create a victory without the need to use traditional power, has been considered as another way to make the surrender of the enemy.

However, their methods can be used to destroy the morale of the enemy, and to promote pro position, in the contemporary terrorist acts actors are the terrorists themselves, and their supporters, and to try to attract neutral groups to its side, in addition to confuse governments and world public opinion, the terrorists know they can not win using violence alone because they are in a weak position militarily, so the violent components terrorist acts are symbolic and designed to send political messages, any sense, if there is no message to be understood by the target audience and then things like bombings and shootings will not have any goal, but the violence itself.

Although some religious terrorist groups based on what seems to be interested in maximizing body counts, there is still the basic political message, mentions that symbolic acts of violence should be analyzed using the following factors:

1. The purpose of the communication,
2. In the context of communication,
3. Relative in a symbolic message.

Since each of these acts of violence have goals or public elementary and secondary schools, and universities.[32]

conclusion

clearly recognizes that cyber terrorism is a serious problem ("Threats and protection).

There are many forms of terrorism on the Internet. Some are not dangerous enough to be deemed a simple spread of information instead of terrorism. They are simple show of skill and are harmless.

Acts of cyber-crimes may involve stealing of money, company secrets, or attacking country's infrastructure and causing real damage.

Cyber terrorism is an impending threat to the United States, or any other technologically advanced country. Even nations with more primitive technology can be negatively affected by the "ripple effect".

With the excess of technology increasing at a tremendous rate, the threat of cyber terrorism will only get worse .

Cyber-terrorism is a complex issue that is vital for information security specialists and to some extent the society to recognize. One must be conscious of all of its characteristics in order to better evaluate how and where the "terrorists" are likely to attack our approach.

What makes this subject significant is that a cyber terrorist attack is comparatively very easy and economical to instigate. For that reason, it can from any where in the world, at anytime, and, more importantly, the stakes of this cat and mouse game are can be quite high. In view of the fact that it is only a matter of time before a system is attacked, one must stay alert and share the knowledge obtained so that we can help protect ourselves at a personal, business, and national level.

Notes

[1] - M. Watney: State surveillance of the internet: human rights infringement or e-security mechanism? South Africa, University of Johannesburg, 42 Int. J. Electronic Security and Digital Forensics, Vol. 1, No. 1, 2007 , Copyright © 2007 Inderscience Enterprises Ltd.. pp.42-54

[2] - ibid ; p p – 45.46.

[3] - ibid: p – 47.

[4] - Denning, D. (1999). Activism, hacktivism, and cyber terrorism: The Internet as a tool for influencing foreign policy. Retrieved October 10, 2003, from http://www.nautilus.org/....html

[5] - Galley, P. (1996, May 30). Computer terrorism: What are the risks? [English translation July 1, 1998 by Arif M. Janmohamed]. Retrieved November 2, 2003, from http://www.genevalink.ch/pgalley/infosec/sts_en/terrinfo.html

[6]- Denning, D. (2000a, May 23). Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives Retrieved October 10, 2003, from, http://www.cs.georgetown.edu.....html

[7] - Hildreth, S. (2001, June). Cyberwarfare. [CRS Report for Congress]. Retrieved November 10, 2003, from http://www.fas.org/irp/crs/RL30735.pdf

[8] - Hirsch, E. Jr., Kett, J. & Trefil, J. (2002). The new dictionary of cultural literacy (3rd ed.). Boston: Houghton Mifflin.

[9] - See generally G. WEIMANN, TERROR ON THE INTERNET: THE NEW ARENA, THE NEW CHALLENGES (2006) see also Hof fman, at. 4; WEIMANN, WWW.TERROR.NET, at 2.

[10]- L. Thomas, Al Qaeda and the Internet: The Danger of "Cyberplanning," 33 PARAMETERS (2003); at 112, 112–123.

[11] - G. Weimann, Virtual Training Camps: Terrorist Use of the Internet, in TEACHING TERROR: STRATEGIC AND TACTICAL LEARNING IN THE TERRORIST WORLD 110, 111 (James J.F. Forest ed., 2006); WEIMANN, TERROR ON THE INTERNET, at 30; Irving Lachow & Courtney Richardson, Terrorist Use of the Internet: The Real Story, 45 JOINT FORCE Q. 100, 100–02 (2007) at 100; WEIMANN, WWW.TERROR.NET, at 2–11.

[12] - See generally Weimann , TERROR ON THE INTERNET, &; Weimann, Virtual Training Camps .

[13] - Marc Rogers, The Psychology of Cyber-Terrorism, in TERRORISTS, VICTIMS AND SOCIETY 77 (Andrew Silke ed., 2003).

[14] - WEIMANN, TERROR ON THE INTERNET, at 25.

[15] - Bruce Hof fman, Al Qaeda, Trends in Terrorism, and Future Potentialities: An Assessment, 26 STUD.CONFLICT & TERRORISM 427, 435 (2003).

[16] - Global network of terrorists appearance has given way much easier access to information and the exercise of command and control of operations, and continued operational charge of the attacks of 9/11, Mohamed Atta, a web of Hamburg, Germany, to discuss US flight schools, has become a target for intelligence gathering more sophisticated, these changes have made the threat warning and control more difficult… see NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 88 (2004).

[17] - Ibid. at 157, 529 n.140, 530 nn.152, 221–222.

[18] - Dorothy E. Denning, Cyberterrorism: The Logic Bomb Versus the Truck Bomb, GLOBAL DIALOGUE (Autumn 2000) http://www.worlddialogue.org/content.php?id=111; Dorothy E. Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, in NETWORKS AND NETWARS 239,281 (John Arquilla & David Ronfeldt eds., 2001).

[19] - G. Weimann: Terror in Cyberspace, & His recent book, Terror on the Internet: The New Arena, the New Challenges, was published in Washington, D.C., in 2006.p- 26.

[20] - Phillip A. Karber, Urban Terrorism: Baseline Data and a Conceptual Framework, 52 SOC. SCI. Q. 521, 527–33 (1971).

[21] - Ralph E. Dowling, Terrorism and the Media: A Rhetorical Genre, 36 J. COMM. 12, 14 (1986).

[22] - J. Bowyer Bell, Terrorist Scripts and Live-Action Spectaculars, 17 COLUM. JOURNALISM REV. 47, 50. (1978).

[23] - G. Weimann, Media Events: The Case of International Terrorism, 31 J. BROADCASTING & ELECTRONIC MEDIA 21, 31 (1987) (analyzing media events and terrorist spectaculars).

[24] - Arquilla, J., Ronfeldt, D., Zanini, M. (1999 the New Terrorism, RAND, Santa Monica, pp.3984. , Medhurst, P. (2002) Global Terrorism, UNITAR, New York., Hof fman, B, (1998) Inside Terrorism, Columbia University Press, New York.

[25] - for example, alone contain from retired US federal employees system about a billion pages of information, much of which is free and is noted here is that many of these sites can provide interest to terrorist organizations and terrorists and more free, as well as, for example, that the terrorists can learn from the online tables and locations targets such as transportation facilities, nuclear power stations, public buildings, airports and ports so that they can know the counter-terrorism measures taken in these places…fore more see Dan Verton: "Black Ice: The Invisible Threat of Cyber-Terrorism" , McGraw-Hill Osborne Media; 1st edition 2003, ISBN: 0072227877.

[26] - G. Weimann, Terrorist Dot Com: Using the Internet for Terrorist Recruitment and Mobilization, in THE MAKING OF A TERRORIST 53–65 (James J.F. Forest ed., 2006).
[27] - Weimann, Virtual Training Camps, at 119. & Weimann, G. (2006) Terror on the Internet: The New Arena, the New Challenges, United States Institute of Peace press, Washington, D.C.
[28] - Thomas, Al Qaeda and the Internet, at 112–123.
[29] - Goldberg L. : "Cyber risks confronting airlines: a practical approach to manage the risks and pursue the wrongdoer" Air & Space Law, http://www.kluwerlawonline.com . (2003), p p – 294. 310.
[30] - G. WEIMANN, TERROR ON THE INTERNET: THE NEW ARENA, THE NEW CHALLENGES (2006); Maura Conway, Terrorism and the Internet: New Media—New Threat?, 59 PARLIAMENTARY AFF. 283, 283–92 (2006).
[31] - W. Hutchinson : Information terrorism: networked influence , Edith Cowan University Research Online Australian Information Warfare and Security Conference Security Research Institute Conferences, W Hutchinson Edith Cowan University Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006. This Conference Proceeding is posted at Research Online. http://ro.ecu.edu.au/isw/10, p-4-5.
[32] - For example, the attacks on September 11, 2001 on New York and Washington immediate goal for the victims of violence, and secondary objectives such as the US government and the public of the World Islamic population, and higher masses in Europe and other countries. The symbolism of the attacks and the many objectives.
The attacks on the US military (Pentagon) and government (a failed Whitehouse / Capitol), economic / capitalist trading systems and attempts (World Trade Center). Also, it can be considered an attack on the immunity of America "home", and modernity (represented by the Architecture World Trade Center)…see Weimann, G. (2004) How Modern Terrorism Uses the Internet, United States Institute of Pease, URL:WWW.USIP.ORG, Accessed 19 Sep 2006.& Weimann, G. (2006) .