How Do Terrorist Organizations Use Information Technologies?

Understanding Cyber Terrorism

Fatih Tombul, Ph.D.
Turkish National Police, Turkey
Email: ftombul@yahoo.com

Huseyin Akdogan, Ph.D.
Turkish National Police, Turkey
Email: hdakdogan@gmail.com

How Do Terrorist Organizations Use Information Technologies?
Understanding Cyber Terrorism

Fatih Tombul, Ph.D. and Huseyin Akdogan, Ph.D.

Abstract

Globalization with advanced information technologies has changed the life of the people in the world. When something occurs in one part of the world, other part of the world can be informed easily within seconds. Current information technologies such as internet, social media, blogs and news channels have enabled the people to create virtual groups all over the world and to disseminate the information easily.

Most of the states, governments, public and private institutions have been using the advantage of the information technologies to serve their citizens and customers. Concurrently, criminals are also using the advantage of information technologies while committing crime. In other words, everything including crime and criminals has changed their structures to be compatible with the advanced information technologies.

Recently, lots of terrorist organizations have erupted especially in the Middle East and their networks are spreading out with the use of technology. Most of the terrorist organizations have been using the technology for military training of their militants, preparation, and recruitment processes. Especially the internet is almost a virtual training slot for terrorist groups. Recent studies (Weimann, 2006; Rothenberger, 2012) have revealed that the internet is served as the library for the terrorist groups to provide instruction manuals and videos on technical and tactical areas such as making a bomb, taking hostages, and guerilla combat. As it has an appropriate space for interaction activities, potential terrorists use the advantage of interaction face of the internet to learn how to make a bomb and send instant messages to the instructors teaching illegal issues.

Thus, security forces in the face of all these developments should take the necessary precautions to fight against the terrorist organizations by standing one step ahead on the use of technology. Standing one step ahead can only be achieved understanding the phenomena and ceaselessly updating the knowledge. Otherwise, security forces will fail if they maintain the use of old technique and tactic to fight against the terrorist groups in this technology epoch.

Based on this point of view, this study will focus on understanding the use of technology to fight against the terrorism. Furthermore, this study will also investigate some of the terrorist organizations using the technology actively to commit crime. This study will also attempt to shed light to the fact that different technologies have been used against the humanity by terrorist groups although most of the people are not aware of that reality.

Keywords: Information Technology, Terrorism, Cyber-terrorism, Content Dissemination, E-Mail Bombing.

Literature Review

Communication technologies have developed especially with recent technological advancement. The estimations by 2012 about the use of communication technology may tell us more about the importance of these technologies and how we are addicted to technology; it is estimated that 294 billion e-mails were sent daily, information that could be stored by 168 billion DVD was produced daily, and Netflix users watched 22 million hours TV and movie daily. Two thirds of the world population had an internet connection and 20 percent of them had a membership to social networks. Eighty five percent of the world population had cell phones and 15 percent of them shop via their cell phones (Klimburg, 2012).

Most of the governments had to take required safety measures to restrict or reduce the use of communication by terrorist organizations. These precautions include restricting, censoring the information coverage of the terrorist groups, finding the contents of the perpetrators of the terrorist groups and taking the immediate actions to censor their media. However, the new media technologies led the terrorist groups to communicate easily and freely; that's why it is difficult to restrict the content of their communication (Weimann, 2005a: 380). The term "cyberterrorism" goes back to the 1990's when the National Academy of Sciences declared a report relating to the computer security mentioning" We are at risk. Increasingly, America depends on computers. . . . Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." (Weimann, 2005b:131).

Attackers, formerly, were using the internet as a tool to satisfy their curiosity about technology and to explore security related issues. These attackers were mostly young and their acts were commonly called "cybercrime". However that situation has changed and nowadays attacks over the internet have been mostly used for industrial espionage and state related issues. Attacks over the internet can cause a devastating harm that under-attacked country may not use even a single conventional weapon (Brunst, 2010). For instance, Estonia faced cyber-attacks (denial-of-service attacks) in 2007 as a protest because of the removal of the Soviet war monument (Bronze Soldier monument), erected in1974 in Tallinn. Most of the websites of the Estonian government, banks, universities and newspapers were among the attacked websites lists. The government could stop attacks by blocking all international web traffic from the rest of the world (Richards, 2009). Table 1 shows examples of cyber-terrorist attacks which was prepared for a research by asking research respondents from different countries who have academic background on cyber-crimes.

Table 1. Examples of cyber-terrorist attacks offered by respondents

Attacks on Estonia	The Russian cyberattacks on Estonia in 2007
Stuxnet, Iran	Stuxnet computer warm reportedly ruined almost one-fifth of Iran's nuclear centrifuges, 2010
Attacks on Georgia	The Russian cyberattack on a Georgian government website in 2008.
India-Pakistan	In 2010 the Indian Cyber Army hacked into the website of the Pakistani Army, and the Pakistan Cyber Army hacked into the website of the Indian Central Bureau of Investigation.
Anonymous	Anonymous hacking into the websites of the Boston and Salt Lake City Police Departments and threatening to release the names and addresses of police officers

Turkey, PKK collapsed Govt. network	The Turkish Ministry of Finance's website was hacked by the Kurdistan Workers' Party (PKK) (2011).
Zapatista spamming	The Mexican Zapatista group has shut down Mexican police and other websites.
Wikileaks	
Israel-Gaza	Following its air strikes on the Gaza Strip Israel experienced more than 44 million hacking attempts on government and other finance websites (2012).
India (social networking)	During the Assam riots threatening messages and pictures were sent to migrant workers using social networking sites (2012).
Dalai Lama	A Chinese cyber espionage organization targeted the office of the Dalai Lama (2009).
Tariq bin Ziyad Brigades	The so called 'here you have' virus, (the responsibility for which was claimed by the Tariq bin Ziyad Brigades for Electronic Jihad)
Aerospace	U.S. defense firm Lockheed Martin said it came under a significant cyberattack in 2011.
Australian sewage leak	The Maroochy Shire cyberattack (2000).
Kyrgyzstan	The sustained cyberattack reported in 2009.

Source: Jarvis, L., Macdonald, S. & Nouri, L. (2014).

According to Weimann (2005b:131), the threat of the cyber-terrorism has been inflated as there is no single event that the cyberterrorism caused a person to kill, although it is called along with the weapons of mass destruction. On the contrary to Weimann's belittling of cyber-terrorism, The US secretary of Defense, Mr. Donald Rumsfeld described the phenomena as an odd war that humankind had never met before. He quoted one of Al-Zawahiri's (One of Al Qaeda's leader) speech stating that "More than half of this battle is taking place in the battlefield of the media. We are in a media battle in a race for the hearts and minds of Muslims". After this Quotation, Rumsfeld said that;

> *"Today we're engaged in the first war in history unconventional and irregular as it may be in an era of: e-mails, blogs, cell phones, blackberries, instant messaging, digital cameras, a global Internet with no inhibitions, hand-held video cameras, talk radio, 24-hour news broadcasts, satellite television. There's never been a war fought in this environment before (Ogun, 2012).*

Public opinion about the cyber-threat seems parallel to The US secretary of Defense, Mr. Donald Rumsfeld's opinion. "75% of global internet users believe 'cyber-terrorists' may, soon inflict massive casualties on innocent lives by attacking corporate and governmental computer networks" while 45 percent of users agreed completely that "computer terrorism will be a growing problem" (Conway, 2002).

However; the anxiety and the fear of the cyber-terrorism rely on three components; psychological, political, and economic. First of all psychologically the cyberterrorism creates an unknown fear with the help of misinformation, more dangerous than the effect of the terrorist bomb, among public against to computer technology. In addition mass media also helps to increase the fear among people with publishing the front news about the

cyberterrorists' activities. As the fear is a crucial factor in terrorism, the U.S. State Department expresses terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience." (NCC, 2006).

The distinction should be made before deciding whether the attack over the internet is against to IT systems to gain money, prestige, and reputation or it is against to human life. In the past attacks against computer systems were evaluated less dangerous compare to conventional attacks such as bombs. One can think that the attack against computer system can only create harm to the computer but that perception has changed as most of the public and private institution are heavily rely on the technology called supervisory control and data acquisition (SCADA) systems. SCADA systems are used to control and measure the small systems as well as the complicated systems such as controlling the electricity, military and civil structures, and pharmaceutical products. SCADA enables the system to control remotely from a central location.

Thus sensitive data follow on the ground, in the air or in the water. Since it can be controlled remotely from a central location, cyberterrorists can damage whole systems by attacking the central location (Brunst, 2010). According to Sieber and Brunst (2008) some of the SCADA systems are directly connected to the internet and some of them are connected inside internal network that is connected to the internet. Research studies revealed that %17 of the SCADA systems are working directly on the internet. This percentage shows how big threat all the countries have to be faced with cyberterrorism.

Some motivators exist behind the attackers who use the internet as a tool to commit crime. One of them is the independence of the location of the internet so that the attackers do not have to present at a certain physical place. Criminals can easily hide themselves behind the virtual world and also it is difficult to identify who carried out the attack. The connection type is not so important that a mobile, home or internet café connection is enough for committing cybercrime. In addition the speed of the internet is not a problem for attackers as they use the speed of the internet of the victim when they launch an attack such as denial-of service (DDoS) attacks.

Anonymity of the internet is also another advantage for the criminals to commit crime by hiding their identity. In fact, the actor of the attacks over the internet can be identified normally by following the IP address of the attackers' computer. However, most of the attackers use different technique such as using proxy services or anonymity networks to hide them. Thereby, the attackers throw of the track and camouflage themselves as if they are attacking from another place where they haven't been before. Cheap cost feature of the internet is another side for criminals to prefer using the internet to commit crime. They don't have to invest too much money in an advanced computer since a moderate computer with an internet connection is enough to commit cybercrime. The advantages of the internationality of the internet are also used mostly by the criminals as a tool to commit crime. Countries have their own borders however the internet does not have a border as it connects all countries. As the rules regulating the usage of internet are not the same in all countries, the criminals have been using this discrepancy and seek ways to publish their illegal contents from the countries where the laws enable too much free-speech (Brunst, 2010).

It is not rational to expect that terrorist groups do not enjoy and benefit these inevitable advantages of cyber world to communicate, propagate and recruit. The cyber space is also

rapidly changing and developing in its inner world. Internet Protocol (IP) traffic had used to pass from wired devices until recent times. This virtual traffic has shifted to wireless and mobile devices, and by 2015 this kind of traffic will likely exceed the former wired devices. It is noteworthy to point out that the largest increase in terms of wireless IP traffic will probably take place in Latin America (48 percent), the Middle East and the Africa (52 percent) where there are a lot of instable areas that terrorist groups love (Jones and Johnston, 2013).

The main aim of the terrorists using the internet is to spread the fear, create the economic turmoil, provoke the opponents and obtain the information. Understanding the attacks over the internet whether it is cybercrime or cyberterrorism is difficult to detect. That kind of cybercrime can be committed because of willingness to spread fear among the population or because of getting the information such as learning the automobile route of a political party leader for assassination to achieve the goal of terrorism.

Thus, a deeply investigation is required to understand the terrorist attacks launched over the internet (Brunst, 2010). There is no exact definition about cybercrime and cyberterrorism that is why it is difficult to make a distinction. Terrorist use of computer to make propaganda, raise money, recruit new supporters cannot be defined totally as cyberterrorism. Cyberspace attacks should include terrorist element and activities such as results of killing or large scale damage and the actions should be politically motivated in order to be called as cyberterrorism. Although politically motivated, hacktivism is different from cyber-terrorism. Hacktivists generally use four weapons to attack. One of them is generating too much traffic through a defined web site so that other user cannot reach the site as usual. In addition, the attacked website does not fulfill its normal function and with the help of the media reports politically motivated hacktivists gain the publicity. E-mail bombing, also called ping attacks, is another method for hacktivists to employ.

With that technique they bombards with thousand may be millions of messages at once to create an environment that the website or ISP cannot operate regularly. Third technique is the web and computer hacking that the hacktivists use to get the stored information such as communication and financial information on another computer. Moreover, sending viruses and worms to harm the computer and network systems is another method that hacktivists use. The interaction between hacktivism and cyberterrorism is hazy. Sometimes the action of the hacktivists such as attacking the network to damage the national infrastructure, for example electric power, can be called as cyber-terrorism (Weimann, 2005b:135).

Some of the scenarios related to cyberterrorism such as attacking Hydroelectric Dams, traffic control systems, power plants can be utilized by the terrorist organization against the countries. With these attacks, terrorist organizations aim to damage the critical infrastructures of the countries so that they can show their power to expose the fear among public and to gain support. Terrorist attacks on Hydroelectric Dams by gaining access to the control system can cause such a devastating harm that they can open the floodgates and cause damages to the areas and inhabitants behind the gates (Brunst, 2010:67). Gleick (2006) states that the accidentally damaged dams in Banqiao and Shimantan in China caused the damage of other lower dams and at least 85.000 people died. Terrorist organization can cause to trigger fear among public by attacking on traffic control systems. As in the attack of 9/11, the hijackers demonstrated how brutal effect they can cause to the airplane and airport control systems. Moreover, terrorist attacks on Power Plants such as attacking of nuclear power plants and

military missile control center may cause devastating fear and danger in the society (Brunst, 2010:67).

Justification of the Violence

Terrorist organizations use every opportunities including violence to accomplish their goals. Since the public are against to violence, they use four different strategies to justify the violence even on the net. The first argument they employ is "no choice" motive. In most of the terrorist webpages, terrorists attempt to convince the public that they are not against the peaceful solution but the violence is the last option against to the enemies. For instance, Tamil Tigers insists that their use of violence is legitimate in as much as the Sri Lankan rejects the rights of Tamil minority.

The second argument for justification is to demonization and de-legitimization of the enemy. They simulate as if they are the freedom fighters as their groups or people are in the hand of the enemy and their rights are being restricted by their enemies. In addition, they demonstrate some images showing that their people are being killed by their enemies thus the real terrorist is their enemies. The third justification of the violence is to emphasize the weakness. They use the argument that terror is the result of the weakness. The last but not least justification is to show how brutal action such as slaughter, and genocide the authorities are acting against them conversely by avoiding how they victimize other people. The aim is to show the public how brutal action their enemies maintains against them (Tzfati and Weimann, 2002:325).

Dissemination of Terrorist Content

The term the internet and the terrorism seem to be different at first glance, but when they are combined the term cyberterrorism emerges. Cyberterrorism is more dangerous than the conventional weapon as it is used by the terrorists to disseminate the information to realize the act of terror and spread their beliefs and ideas. Moreover, it is an appropriate place for terrorist groups to propagate their points of view (Giacomello, 2010). Rothenberger (2012) defines this information dissemination as Public Relations (PR). Apart from one-sided mass media such as TV, newspapers and radio stations that terrorist groups had used before internet era, they are today gaining publicity via interactive social media as a crucial part of PR efforts.

Most of the terrorist organizations realized the effect of the mass media to reach the large audiences. They have been using different strategies and tactics to influence the public and their action is called media-oriented terror. Terrorists are aware of the fact that media is an important tool to gain psychological warfare. They can spread their terrorist activities and make propaganda on defined group of people. They work hard on the appropriate time, targets and location in terms of media preferences to have more influence on people. Before any action or any attack, they make preparation to gain more support and to affect more people. They use visual aids for the media such as taped interviews and speech of the perpetrators. They use these kinds of tools on their own media such as TV, news agencies, newspapers and websites (Weimann, 2005a: 384).

Dissemination of terrorist attacks can be defined as an amplifier of terrorist attacks and the impacts of these attacks. The impact of the attacks heavily depends on when round the clock news services on mass media and internet (Duyvesteyn, 2004: 448). This has caused a paradigm shift in terrorist propaganda. The paradigm had been defined as "propaganda by

deed" (Bakunin, 1870) before the internet era and almost all of the terrorist organizations has accepted and employed this philosophy of anarchists. However, the cyber-era has been shifting this paradigm. The new paradigm is propaganda by deed over the net.

The pre-internet era terrorist organizations had to completely rely on the effect and impact of their deeds, in order to publicize their deeds via mass media such as TV's, newspapers or radio stations and reach their aim which is the carried message by the deed. Although the main aim is conveying the message to target audience by the deed, the message should have such an impact that attracts the attention of the mass media. However, in the internet era, attracting the attention of mass media is not a primary focus of the terror organizations and their deeds. Terror organizations today can post whatever they want via internet, YouTube and social media. Mackinlay (2009) argues that these developments in cyber space have brought the world including the terrorist organizations in to a "post-Mao" era.

The technology is developing very fast that, web sites which allow only viewing information is called traditional web applications after the invention of social media. "Different from traditional web applications that allow only passive information viewing, these web 2.0 sites offer a platform for users to actively participate in and contribute to the content/service provided" (Zhao et al., 2011, p.3). The study of Qin, Zhou, Reid, Lai and Chen (2007) revealed that terrorist organizations have adopted new levels of web technologies as US government agencies. Moreover their study proved that terrorists use more multimedia technologies on their web site than the US government agencies. Moreover, they heavily use web forums in order to facilitate their communication.

Websites of the Terrorist Organizations

The existence of the cyberspace of the terrorist group has recently started to be told. Only 30 terrorist organizations, declared as foreign terrorist organizations according to U.S antiterrorism and Effective Death Penalty Act of 1996 that had the web page on the net. However that number increased and approximately all terrorist organizations started to create webpages to prove their presence on the net by the end of 1999. It is the fact that the content of these webpages usually in English language and disseminate the information about terrorist organizations' political and ideological aims, leaders, founders, commanders and some admired individuals.

Most of the webpages mention about the background and history of the organization, the activities done in the past. In addition, the contents emphasize not only the information but also the direct criticism against the enemies or rivals. On the other hand, the WebPages avoid giving information about some brutal attacks that the organization carried out. Moreover, terrorist organizations emphasize two issues on the net; the importance of the freedom of expression and political prisoners. Thereby, terrorists aim to provoke the western audiences about how important the freedom of the expression and human rights to illustrate as if their action is legal in democratic societies (Weimann, 2005a: 386).

Apart from traditional web applications such as terrorists' websites, most of the terrorist groups have shifted from dealing with static websites to using interactive social networks, online forums, blogs and media (Bockstette, 2008). Almost 90 percent of the terrorist activities take place on the social media, such as yahoo e-groups, paltalk and bulletin boards. The forum sites that are prepared by the terrorists act as firewall to hide the militants' identities. They also enable users to contact the terrorist representatives to ask question or to

learn something detailed. Nowadays all terrorist groups have forums in chatrooms, e-groups, you-tube created with the latest modern online format (Weimann, 2009: 46).

Terrorist websites aim to attract not only potential supporters but also their enemies. In addition, changing the international public opinion about the organization is also another target for terrorist websites. Terrorists use their websites offering some attractive items such as flags or printed t-shirts, videos and audiocassettes to attract the supporters. Their slogans and use of local language is an important method to appeal the supporters. The activities of the organization and recent international politics are also detailed in their websites. They also give importance to the international public opinions. The terrorist groups sometimes held press conference and put into the websites to attract opinions of the international journalists. Doing so, they try to demonstrate their enemies as guilty. In addition, they want to change the international opinions against them to demoralize their enemy (Weimann, 2005a: 388). Rothenberger (2012) analyzed some of the eminent terrorist groups' use of cyber world. Based on this research, some of the results of the analysis of terrorist groups' use of internet will be discussed below:

ETA (Basque Homeland and Freedom; Spain): Rothenberger's analysis reveals that ETA is very active in cyber world. Not only ETA does broadcasts videos and use blogs, but the group switched their long run and confined newspaper GARA to Internet newspaper. ETA even provides all of these internet actions in English and French subtitles. Twitter is the last cyberspace that ETA is active recently.

IRA (Irish Republican Army, Ireland): IRA used USB sticks and email platform to exchange information at the beginning of the cyber era. Currently they are very active in almost all internet platforms such as broadcasting on YouTube, an internet magazine titled "An Phoblacht", facebook and twitter.

Shining Path (Peru): Although the Shining Path once considered the media as a demon part of feudal and bourgeois system that they want to destroy, they currently have catch on the importance of new technologies like internet to reach their target groups. They now have accounts on social networks sites.

FARC (Revolutionary Armed Forces of Colombia, Colombia): FARC has a traditional web site conveying their aims and their history. Through this website the terrorist group is directing its followers to several links which enable a network structure that recruitment and fundraising activities can easily be conducted. FARC also provides its web services with several languages.

LTTE (Liberation Tigers of Tamil Eelam, Sri Lanka): Rothenberger (2012) portrays LTTE as a true master in cyber world. They benefit numerous cyber tools such as websites, forums, social networks and blogs. These cyber activities have ensured an international awareness about the group and provided the international dissemination of their propaganda. Tamil Tigers have also used the cyber world to recruit new members and fundraising activities.
Al Qaeda (The Basis, Arab World): Al Qaeda extensively uses the cyber world for their aims. The eye-catching point in the group's web sites is the anti-western atmosphere. The terrorist organization largely uses the web for training and instructional manuals. Since the organization has a large sympathizers and members all around the Arab world, they disseminate these kinds of materials via cyber world.

Based on these aims of terror organizations using the cyber world; one can categorize the most preferred reasons for terrorists to use internet as 1-Information provision and information gathering, 2-financing, 3-networking and 4-recruitment (Conway, 2006:10).

Information Provision and Information Gathering

With information provision, terrorists can provide support by doing propaganda on the internet. It is an excellent place for them to gain psychological warfare. Over and above, they can give information related to the profile of their leaders and their ideology as propaganda. Spreading the disinformation over the internet is another option of the internet that is used by terrorists (Conway, 2006: 10).

Information gathering is another important resource for terrorists to use the internet. The information was stored in one or some locations in the past and thus it was difficult to get information comparing today. With advancement in the technology and development in the internet, one can easily reach and retrieve the information on the internet. In the same way terrorists can obtain vast amount of information on the internet as well. Data mining and information sharing are the two components that terrorist prefer to use in terms of information gathering.

Terror groups can get important information about defining and knowing the specific targets by data mining. They can not only get information from the web pages of terror groups around the world but also other institutions' official web pages such as obtaining the location and operation of nuclear reactors in any country. Furthermore, the members of the terror organizations can use the web pages to disseminate the information about how to make bombs or such other things by using information sharing channels (Conway, 2006:18; Rothenberger, 2012).

Social networking platforms are very suitable place to disseminate propaganda to the people from different age groups. Most of the internet users accept the people on different social media platforms as a friend without investigating who they are. Some of these users are terrorist seeking to obtain the information about the users. In addition users of the social networking websites do not hesitate sharing their own identity and picture of themselves and their friends.

Thereby, terrorist groups can easily obtain the detailed information about the users even their hobbies and most visited websites. They throw the hook and they decide who will be the target based on these information. For instance the twitter is an appropriate social networking tool that terrorist groups mostly use to share information. Since twitter provide real-time update information about a place or a person it is an appropriate tool to use. When terrorist groups conduct ambushes they can obtain real time information about logistics of a troop. Secondly, terrorist groups can use the twitter to activate an explosive device with the help of using twitter's real time information. Last but not least, terrorist groups can get contact the military personal as if they are his/her friend with the help of the information that may be stolen identity of a military personal over a twitter account (Weimann, 2009:48).

These advantages of the internet had been used before 9/11 attacks by Mohammed Atta who was one of the terrorists hijacked and terminated the planes. He acquired lots of information about U.S. flights by researching U.S. flight schools. He did these researches by online

traveling from Hamburg to U.S. flight Schools (National Commission on Terror Attacks, 2004, p. 88).

Financing

Financing is a vital aim for the terrorists to use the internet. They are using the internet as a tool to raise funds for their activities. Since the internet enables interactivity so it is a best place to achieve financial donations. Thomas (2003:117) states that most of the terrorist organizations claiming they have affiliation with Islam (in fact they are not) gain lots of money via credit card fraud. There has been some evidence that some of the terrorist organizations has established e-business on the internet to raise money for their activities. For example,

InfoCom, Texas based ISP company was accused of having some accounts in communication services and funds belonging to some terrorist organizations such as Hamas (Hinnen, 2004). Terrorist groups also employ the charity organizations to raise money. At first glance it seems they collect the money for humanitarian purposes such as feeding, clothing and educating the poor and illiterate but; in fact, they are using the money, collected over the charity organization, for their terrorist activities and supporting the militant groups. Raising funds from charities, chat rooms and forums through the internet, Al-Qaeda is one of the leading examples employing cyber space for financing. On the other side, sympathizers can donate to Irish Republican Army (IRA) via the organization's web site with their credit cards (Weimann, 2007).

According to Piper (2008: 265) terrorist groups have emphasized using the internet for finance related activities since the 9/11 terrorist attacks. They usually request funds by publishing the title such as "what you can do" or "how can I help". They search and monitor the visitor on the website and get contacted with the users who visited the site more than once. Additionally, terrorist groups use electronic money transfer and laundering as fundraising methods.

Moreover, terrorist groups employ online auctioneering for the money movement. That transaction takes places between two partners called smurfs on a fake item. One of the partner bids on the fake item then other partner withdraw the money from auction house to avoid being detected. Furthermore, terrorist groups can use online casinos for laundering and storing money. They open the bid system on online casinos to maintain the money activity herewith they store and hide the large amount of money. Drug trafficking is also another source for terrorist groups to gain money. They sell the fake drug and people buy them as if they are original prescribed drugs and money goes to fund Middle Eastern terrorism (Whelpton, 2009: 265).

Networking

The internet is also an appropriate tool for terrorist organizations to create networking that provide more flexible organization structure even if they have decentralized structure. Since the architect of the internet enables people to communicate more easily and with low cost, terrorist use the advantages of that feature to manage their supporter around the world. Terrorist groups find the internet as a suitable tool to coordinate internal and external groups and they can also create discussion groups with the help of the structure type of the internet from one center. Although they have different dispersed groups around the world, they can

manage to create alternate communication channels on the internet (Conway, 2006: 14; Rothenberger, 2012: 12).

Arquilla, Ronfeldt and Zanini (1999: 85) state that terrorists changed their networking designs from hierarchical to information-age networks. Terrorist networks are connected to each other rather than stand alone. They have more organized and decentralized structure. In addition, they follow and implement the latest technologies to provide perfect communication. Since there is not a single leader, command or headquarters, even if the groups are small, medium and large on the internet, it does not create a problem. Over and above, they may have multiple leaders to organize the groups. Weimann (2006: 637) posits that terrorists not only use the communication feature of the internet inside the same terrorist organizations but also build the communication within the members from different countries. For example terrorist groups in Afghanistan and Lebanon can exchange information with each other related to recent practical information, new developments and trainings such as learning how to make bombs.

Recruitment

The web enables for an organization to gain members in terms of the recruitment in different ways. First of all, the web provides people more quick and easy information. Second, the web let more people to know the recent event through the information bulletin. The last but not least, the web creates the opportunities for interactive communication so that members can have discussion in the discussion groups and participate the debates. They can even get contact with the group leader for more information (Gibson and Ward, 2000: 306). Terrorists may have been taking advantages of that feature of the web to recruit new members and may increase more support.

With the help of social networking and gaming sites, terrorist groups obtain information about user's skills, names and interests to recruit. A social networking user, for example in the field of chemistry and engineering can be easily targeted via looking the information about a user's background information. Thus, they can be recruited as persons to make bombs. Furthermore, terrorist groups, searching the information in online gaming sites, can determine persons who have strong shooting ability that is the indicator of showing violent tendencies to use them for operation missions (Veerasamy and Grobler, 2011: 263). Schauble (2008) points that internet is more than a communication tool for terror organizations, it is an "advertising platform, distance university and virtual camp." (cited by Rothenberger, 2012. p. 10).

Conclusion

Information technology has changed the way of the information flow which in turn changed the struggle with terrorism. Moreover a new term called cyber-terrorism has emerged. Recent events have showed that terrorists are so familiar with the internet that they maintain their activities over the internet to prepare attacks, to communicate and disseminate the information. Cyber-terrorism was not evaluated as a serious danger before the cyber-attacks that caused devastating harm in Estonia in 2007. But after the Estonia attack, national organizations even NATO evaluated cyber-attacks as the risk of a missile strike. Terrorist's use of the technology is so spread that former leader of Al-Qaeda stated in his speech after September 11 attack that "hundreds of Muslim scientists were with him who would use their knowledge ranging from computers to electronics against the infidels." (Weimann, 2005b:146).

Nowadays most of the public and private institutions are heavily rely on the technology called supervisory control and data acquisition (SCADA) systems. They can be controlled remotely from a central location. Thus cyber-terrorists can attack and take the control of all systems by attacking the central location (Brunst, 2010). That probability shows how important and difficult to struggle with cyber terrorists in terms of law enforcement perspective. In addition, since the internet enables user anonymity, terrorist groups can perform their attack remotely and from safe locations without any risks related to defining their physical space. Moreover, the anonymity also enables terrorist groups to participate the cyber-terrorism all over the world as independent units.

On the other hand, law enforcement officers should provide a balance between the democratic values and security. If they only focus on providing security, democratic rights of the citizens may be eroded. Conversely, if they only focus on the democratic values of the citizens with undermining the security, cyber-terrorists can abuse that rights and take the advantages of freedom.

Cyber terrorists have been heavily using the internet to disseminate the information, recruit, raise fund, and to spread their propaganda to the public. Most of the terrorist organization has their web site on the internet as it is cheap, easily established and published. Terrorist organizations have adopted new levels of web technologies and they use more multimedia technologies on their web site than government agencies. Moreover, they heavily use web forums in order to facilitate their communication.

Developments in the technology prove that future terrorists are grooving up in the digital world and they will be more dangerous than today's cyber-terrorists. In addition, they use the advantage of the mass media as it enables freedom of press and freedom of the expression. Thus, security forces in the face of all these developments should take the necessary precautions to fight against the terrorist organizations by standing one step ahead on the use of technology. If they are behind the technology and try to struggle the cyber terrorist with the traditional method used in the past, it is impossible to be successful against the fight with cyber-terrorists.

About the Authors:

Dr. Fatih Tombul is affiliated with Turkish National Police. He received his Ph.D. in Information Science from the University Of North Texas. His research interests include Information Technologies, Social Media, Organizations, Management, Research and Statistics. Email: ftombul@yahoo.com.

Dr. Hüseyin Akdoğan is also affiliated with Turkish National Police. He is also an Associate Professor of Public Administration. He received his Ph.D. in Public Administration from the University Of North Texas. His research interests include human rights, terrorism, 0rganizations, Management, research and Statistics. E-mail address: hdakdogan@gmail.com

References

Arquilla, J., Ronfeldt, D., & Zanini, M. (1999). *Networks, netwar, and information-age terrorism*.John Arquilla, and David Ronfeldt, "Emergence and Influence of the Zapatista Social Netwar," in Networkds and Netwars, ed. John Arquilla and David Ronfeldt (California:rand, 2001)

Bakunin, M. (1870). Letters to a Frenchman on the Present Crisis. Retrieved from https://www.marxists.org/reference/archive/bakunin/works/1870/letter-frenchman.htm

Bockstette, C. (2008). Jihadist Terrorist Use of Strategic Communication Management Techniques. Garmisch-Partenkirchen: George C. Marshall Center.

Brunst, P. W. (2010). Terrorism and the internet: New threats posed by cyberterrorism and terrorist use of the internet. In *A War on Terror?* (pp. 51-78). Springer New York.

Conway, M. (2006). "Terrorist Use of the Internet and Fighting Back." *Information and Security* 19(9).

Conway, M. (2002). Reality bytes: Cyberterrorism and terrorist 'use' of the Internet. First Monday 7(11) Retrieved 15. 05. 2015 from http://firstmonday.org/ojs/index.php/fm/article/view/1001/922

Duyvesteyn, I. (2004) How New Is the New Terrorism?, Studies in Conflict & Terrorism, 27:5, 439-454, DOI: 10.1080/10576100490483750

Giacomello, G. (2004). Bangs for the buck: A cost-benefit analysis of cyberterrorism. *Studies in conflict & terrorism*, *27*(5), 387-408.

Gleick, P. H. (2006). Water and Terrorism. *Water Policy*, *8*, 481–503.

Gibson, R., & Ward, S. (2000). A proposed methodology for studying the function and effectiveness of party and candidate web sites. *Social Science Computer Review*, *18*(3), 301-319.

Hinnen, Todd M. "The cyber-front in the war on terrorism: Curbing terrorist use of the Internet." *The Columbia Science and Technology Law Review* 5.5 (2004): 1-42.

Jarvis, L., Macdonald, S. & Nouri, L. (2014). The Cyberterrorism Threat: Findings from a Survey of Researchers. *Studies in Conflict & Terrorism, 37.* 68–90

Johnson, B. (2008). NATO says cyber warfare poses as great a threat as a missile attack. *The Guardian*, http://www.guardian.co.uk/technology/2008/mar/06/hitechcrime.uksecurity

Jones, S. G. & Johnston, P. B. (2013). The Future of Insurgency, *Studies in Conflict & Terrorism*, *36*(1), 1-25, DOI: 10.1080/1057610X.2013.739077

Klimburg, A. (2012). National cyber security framework manual. NATO CCD COE Publication, Tallinn. Retrieved: 03.04.2013, http://www.ccdcoe.org/369.html

Mackinlay, J. (2009) The Insurgent Archipelago. London: C Hurst & Co Publishers Ltd.
National Counterterrorism Center (2006). Country Report on Terrorism 2005, Statistical Annex.

National Commission on Terror Attacks. (2004). The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States. New York, NY: W. W. Norton.

Ogun, M. N. (2012) Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes, *Journal of Applied Security Research, 7(*2). 203- 217, DOI:10.1080/19361610.2012.656252

Piper, P. (2008). Nets of terror: Terrorist activity on the internet. *Searcher, 16(10),* 260-266.

Qin, J., Zhou, Y., Reid, E., Lai, G., & Chen, H. (2007). Analyzing terror campaigns on the internet: Technical sophistication, content richness, and Web interactivity. *International Journal of Human-Computer Studies, 65(1),* 71-84.

Richards, J. (2009). Denial-of-service: The Estonian cyberwar and its implications for US national security. *International Affairs Review, 18*(2).

Rothenberger, L. (2012). Terrorist Groups: Using Internet and Social Media for Disseminating Ideas. New Tools for Promoting Political Change. *Romanian Journal of Communication and Public Relations. 14*(3).

Thomas, T. L. (2003). Al Qaeda and the Internet: The Danger of Cyberplanning'. *Parameters, 33(1),* 112-123.

Tsfati, Y., & Weimann, G. (2002). www. terrorism. com: Terror on the Internet.*Studies in Conflict and Terrorism, 25*(5), 317-332.

Weimann, G. (2005a). The theater of terror: The psychology of terrorism and the mass media. *Journal of aggression, maltreatment & trauma, 9(3-4),* 379-390.

Weimann, G. (2005b). Cyberterrorism: The sum of all fears?. *Studies in Conflict & Terrorism, 28(2),* 129-149.

Weimann, G. (2006). Virtual disputes: The use of the Internet for terrorist debates. *Studies in conflict & terrorism, 29*(7), 623-639.

Weimann, G. (2007). How modern terrorism uses the Internet. *Asian Tribune, World Institute for Asian Studies, 9(342)*. Retrieved from http://asiantribune.com/index.php?q+node/4627

Whelpton, J. (2009). Psychology of cyber terrorism. In *Cyberterrorism 2009 Seminar, South Africa: Ekwinox*.

Weimann, G. (2009). Terror on facebook, twitter, and youtube. *Spring 16(2),* 45-54.

Veerasamy, N., & Grobler, M. (2011, March). Terrorist Use of the Internet: Exploitation and Support through ICT infrastructure. *In The Proceedings of the 6th International Conference on Information Warfare and Security,* 260.

Zhao, V. H., Lin, W. S., & Liu, K. J. R. (2011). Behavior Dynamics in Media-Sharing Social Networks. Cambridge: Cambridge University Press.