2011 3rd International Conference on Cyber Conflict
C. Czosseck, E. Tyugu, T. Wingfield (Eds.)
Tallinn, Estonia, 2011 © CCD COE Publications

Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism

Murat Dogrul, Adil Aslan, Eyyup Celik
Turkish Air War College
Istanbul, Turkey

***Abstract*- Information Technology (IT) security is a growing concern for governments around the world. Cyber terrorism poses a direct threat to the security of the nations' critical infrastructures and ITs as a low-cost asymmetric warfare element. Most of these nations are aware of the vulnerability of the information technologies and the significance of protecting critical infrastructures. To counteract the threat of potentially disastrous cyber attacks, nations' policy makers are increasingly pondering on the use of deterrence strategies to supplement cyber defense. Nations create their own national policies and strategies which cover cyber security countermeasures including cyber defense and deterrence against cyber threats. But it is rather hard to cope with the threat by means of merely 'national' cyber defense policies and strategies, since the cyberspace spans worldwide and attack's origin can even be overseas. The term "cyber terrorism" is another source of controversy. An agreement on a common definition of cyber terrorism among the nations is needed. However, the international community has not been able to succeed in developing a commonly accepted comprehensive definition of "terrorism" itself.**

This paper evaluates the importance of building international cooperation on cyber defense and deterrence against cyber terrorism. It aims to improve and further existing contents and definitions of cyber terrorism; discusses the attractiveness of cyber attacks for terrorists and past experiences on cyber terrorism. It emphasizes establishing international legal measures and cooperation between nations against cyber terrorism in order to maintain the international stability and prosperity. In accordance with NATO's new strategic concept, it focuses on developing the member nations' ability to prevent, detect, defend against and recover from cyber attacks to enhance and coordinate national cyber defense capabilities. It provides necessary steps that have to be taken globally in order to counter cyber terrorism.

Keywords: cyber terrorism, terrorism, cyber defence, cyber deterrence

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the Turkish Air Force, Turkish Ministry of Defense, or the Turkish Government.

I. INTRODUCTION

The rapid evolution of information and communication technologies, and widespread services provided by the cyberspace bring up the question, "How can security of cyberspace be ensured?". IT and critical infrastructure networks are interconnected with each other, and can be accessed from anywhere in the world. In today's cyber world, a wide range of critical infrastructures from water supplies to transportation, from energy to communication technologies are vulnerable to cyber attacks. These infrastructures have little to none cyber protection, and rely on outdated conventional security solutions. A terrorist cyber attack on these industries could give rise to environmental disasters, economic casualties, and loss of property and/or loss of life. In this context, it is urgent that nations prepare for a possible cyber attack on critical infrastructure.

Plenty of investments have been made to prevent classical terrorist violence but the developed countries remain highly vulnerable to cyber attacks against the computer networks that are critical to national and economic security. The growing complexity and interconnectedness of these infrastructure systems, and their reliance on computers, not only make them more vulnerable to attack but also increase the potential scope of an attack's effects. This fear has prompted the governments to pump significant resources into protecting the critical national infrastructures [1].

In order to protect their vital interests, many technology dependent countries concentrate on organizing their cyber security policies. Most of these nations have taken some sort of national legal and military measures. But without international cooperation, these national measures are inadequate against cyber terrorism. Regional partnerships also do not provide adequate cyber security, since the cyber attacks can originate from off-region or off-partnership countries. In order to provide a worldwide international cooperation; the term "cyber terrorism" should be defined precisely and activities, considered as terrorist activity, should be determined as a first step. After that, developing both legislative and military collaborations should be discussed.

This paper first introduces the existing definitions and different aspects of cyber terrorism and relevant terms. It clarifies the extent of the cyber terrorism. Then it investigates how the terrorist organizations exploit cyberspace and why cyber domain is an attractive choice for terrorists. Next, it examines both legislative and military international cooperation attempts against cyber terrorism up to this day. Lastly, it offers an international game plan in order to set up defense and deterrence against cyber terrorism globally.

II. THE TERM "CYBER-TERRORISM"

While some authorities claim that there hasn't been any true cyber terrorism attack yet, others assert that terrorists already take advantage of the Internet. The source of this disagreement is inability to exactly define both "terrorism" and "cyber terrorism".

There is no universally accepted definition of terrorism and cyber terrorism; even when people agree on the rough definitions, they sometimes disagree about whether or not the definitions fit particular incidents. In order to understand terrorism, different views on what exactly constitutes terrorism must be assessed. Up to the present, no single international definition seems to satisfy the wide interpretation of terrorism or cyber terrorism.

However some authors were able to produce quite general definitions. In terms of its etymology, the word "terror" comes from the Latin word "terrere", meaning "to frighten, to terrorize, to intimidate"[2]. Usually, a series of terror incidents that are interconnected and directed at a certain political target is required in order to arrive a definition of terrorism. According to Bozdemir "Terrorism is a strategic approach which, for political purposes, identifies itself with a method which includes the use of organized, systematic and continuous terror."[3].

Denning defines terrorism as "The unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons" [4].

Denning also defines cyber terrorism as; the convergence of terrorism and cyberspace. "It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear" [4].

The term cyber terrorism may be mixed up with "information warfare" and "cyber crime". But there is a major difference between cyber terrorism and information warfare. Cyber terrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets. But older term known as information warfare is defined as "a planned attack by nations or their agents against information and computer systems, computer programs, and data that result in enemy losses." [5].

Information warfare also encloses the term "cyber warfare". But cyber warfare's interest is limited to cyberspace. Information warfare and cyber warfare have "certain targets" in a war but cyber terrorism causes fear and harm to anyone in the targeted vicinity.

Along with these terms there is a phenomenon of cyber crime used frequently by law enforcement agencies. Although physical forms of cyber terrorism, information warfare, and cyber crime often sound very much alike, cyber crime is a crime committed through the use of information technology.

For instance; if a person hacks someone's banking account and/or steals credit card information, then it is called as cyber crime, because the attacker's intention is neither political nor social. If the same attack is directed to substantial number of banking accounts and the attacker declares that he is going to continue attacks until the government accepts his demands; moreover as a consequence of this attack people begin to fear and withdraw their money from the banks then it is labeled as

cyber terrorism. If the activities are carried out by the agents of a foreign power, and if all the banking system of a nation is targeted, then it could be labeled as cyber warfare. If the attacks to the banking system are not limited to cyberspace then it is called as information warfare.
Terrorist organization websites and the use of the Internet by the terrorists are other concerns. Most of the terrorists have not mastered the technology necessary for launching large scale attacks. However, some websites offer technologies for hire on the internet and provide information to reach bot-nets to execute "Distributed Denial of Service Attacks". Since the cyber terrorism is the convergence of terrorism and cyberspace, not only the devastating terrorist cyber attacks but also terrorist actions such as propaganda and recruiting carried out on the Internet should be considered as "cyber terrorism". Terrorist organization websites agitate public opinion, educate and motivate the members, command and control the organization, make propaganda to the target population and provide information to carry out cyber attack. Therefore, both the terrorist cyber attacks and the use of internet websites by the terrorists should be treated together and evaluated under the definition of the cyber terrorism.
After defining the extent of the term cyber terrorism, the exploitation of cyberspace by terrorists will be discussed.

III. WHY AND HOW THE TERRORIST ORGANIZATIONS EXPLOIT CYBERSPACE

There are many reasons that why cyberspace is an attractive choice for the terrorist purposes. Cyber attacks offer the capabilities for terrorist activities with wider-reaching impacts. Using cyber attacks, terrorists can inflict much wider damage to a country than they could by resorting to physical violence. With traditional terrorist activities, such as bombings, the impacts are isolated within specific physical locations and communities. Large part of the population acts only as observers and they are not directly affected by terrorist acts. The media and public attention is more likely to focus on the destruction of property and/or loss of life than whatever "cause" the activity was intended to promote. The ability of cyber terrorism activities to effect wider part of the population may give the groups involved greater leverage in terms of achieving their political and social objectives [6].
The motivation of the cyber terrorists comes from their political agenda. Their attacks are politically motivated and directed to specific critical system and infrastructures. This common agenda gathers all the hackers in the terrorist organization on the same goal. This collective action would do more harm than the action of individual hackers.
There are various reasons why cyber attacks are an attractive choice for terrorists such as;

- As terrorists have a limited amount of funds, cyber attacks are more tempting as they would require less people and less resources (meaning less funds). On the other hand, they can target and affect large numbers of

people with same amount of funds. In other words benefit to cost ratio is extremely high.

- It enables terrorists to remain unknown, as they could be far away from the physical location where the terrorism is being carried out. As terrorists normally set up camp in a country with a weak government, the cyber terrorist could set up anywhere and remain anonymous [7].
- Mostly, attacks are easy to carry out because many targets are poorly protected. Therefore attackers can choose from a wide variety of targets [8].
- When the attack is set up, it can be launched quickly without any need for further preparation [8].
- There are no physical barriers or check points that they have to cross [9].
- The speed and form of attacks are not dependent on the connection speed of the attacker. The connection speed of captured victim computers can be fully exploited [8].
- A combination of both physical terrorism and cyber terrorism is thought to be the most effective use of cyber terrorism [10].

In this regard, how the terrorist organization websites encourage the terrorist attacks should be revealed as well. Terrorist groups are increasingly using new information technology (IT) and Internet to

- formulate plans,
- raise and launder funds,
- spread propaganda,
- communicate securely with the members (internal comm.) [10],
- share information and knowledge with similar groups (external comm.) [11],
- command and control [9],
- make research and development,
- recruit new members,
- generate international support,
- gather intelligence [12],
- make information warfare on behalf of the nations.

In addition to above, Internet offers;

- little or no regulation,
- potentially huge audiences,
- anonymity of communication,
- fast flow of information [10].

One of the striking examples that can be given on the use of websites by terrorists is PKK/KONGRA-GEL terrorist organization websites. There are 37 determined websites that are related with this organization. These websites generally include: the history of the organization, biographies of the influential people and its killed terrorists, and information on the political aims of the terrorist network. Content of these websites aims to create and enforce identity based separatism. One of the websites named “pajkonline.com” aims women who were mostly used in suicide bombings in the past. Another one is dedicated to cyber attacks and encourages the members to learn hacking techniques and provides information about the

vulnerabilities of computer operating systems [13]. This multidimensional example reveals the disrupting aspect of the issue.

IV. Cyber Terrorism Attempts and Further Expectations

Cyber attacks come in two forms; those that target data, those that target control systems [14]. Theft and corruption of data are the most common forms of Internet and computer attacks, and aim to sabotage services. On the other hand, attacks which focus on control systems are used to disable or manipulate physical infrastructure. For example, the provision of electrical networks, railroads, or water supplies could be infiltrated to have wide negative impacts on particular geographical areas. This can be done by using the Internet to send malicious programs or by penetrating security systems.

Weak spots of such an infrastructure were exploited in an incident in Australia in March 2000 where a disgruntled employee (who failed to secure full-time employment) used the Internet to release 1 million liters of raw sewage into the river and coastal waters in Queensland [14].

In 1998, a terrorist guerrilla organization flooded Sri Lankan embassies with 800 e-mails a day for a two-week period. The messages simply read “We are the Internet Black Tigers and we’re doing this to interrupt your communications.” Intelligence departments characterized it as the first known attack by terrorists against a country’s computer systems [4].

In July 1997, the leader of a Chinese hacker group claimed to have temporarily disabled a Chinese satellite and announced he was forming a new global “cracker” organization to protest and disrupt Western investment in China [10]. Internet saboteurs defaced the Home Page of, and stole e-mail from, India’s Bhabha Atomic Research Center in the summer of 1998. The three anonymous saboteurs claimed in an Internet interview to have been protesting recent Indian nuclear blasts [10].

Cyber terrorism may be used not only to inflict damage in itself, but in combination with conventional or nonconventional terrorism. Had Shoko Asahara and Aum Shinrikyo group been able to hack into the Tokyo power system and stop the subways, trapping passengers on the trains, the number of casualties caused by their 1995 Sarin gas attack might have been significantly larger [15].

Recently, Keith Lourdeau, deputy assistant director of the FBI’s Cyber Division, said the FBI’s assessment indicates that the cyber terrorist threat to the U.S. is “rapidly expanding,” and predicted that “terrorist groups will either develop or hire hackers, particularly for the purpose of complementing large physical attacks with cyber attacks” [16].

A survey of 600 IT security executives from critical infrastructure enterprises worldwide showed that more than half (54%) of them have already suffered large scale attacks or stealthy infiltrations from organized crime gangs, terrorists or nation-states. The average estimated cost of downtime associated with a major incident is $6.3 million per day [17].

The survey also introduced that the risk of cyber attack is rising. Despite a growing body of legislation and regulation, more than a third of IT executives (37%) said the vulnerability of their sector has increased over the previous 12 months and two-fifths expect a major security incident in their sector within the following year. Only 20% think their sector is safe from serious cyber attack over the following five years. 60% of those surveyed believe representatives of foreign governments have been involved in past infrastructure infiltrations. In terms of countries that posed the biggest threat to critical infrastructure security, the United States (36%) and China (33%) topped the list. More than half (55%) believe that the laws in their country are inadequate in deterring potential cyber attacks. Among the interviewees those based in Russia, Mexico and Brazil are the most sceptical. Among them 45% don't believe that the authorities are capable of preventing or deterring attacks.

Governance issues are at the centre of any discussion of security for critical infrastructure. Both the governments and private sector organizations need to gain cyber security capabilities. Although the security industry seems to stay one step ahead, governmental regulations has a vital role in defending critical infrastructures around the world. Moreover, a global cyber defense capability can only be obtained by means of international cooperation among the governments.

V. DEVELOPING INTERNATIONAL COOPERATION AGAINST CYBER TERRORISM

Starting with the basic "cooperation" thoughts, following part of the paper evaluates the international cooperation opinions from two aspects: Legislative cooperation and military cooperation.

A. The Legislative Cooperation against Cyber Terrorism

Up to today a number of both governmental and international steps have been taken. Governments are organizing themselves to confront the new threat. Some countries have established Computer Emergency Response Teams (CERTs) to handle incident response. USA and UK are the leading model nations for other countries that compose their cyber security policies. Many governments continue to struggle with the organization chart question, but some countries have been able to successfully form a national organization against cyber threats. For instance; in Brazil, the federal government established the Critical Infrastructure Protection Information Security Working Group, under its Department of Information and Communications Security in August 2009. This group works on information security and incident response plans. In Australia, a 2009 defense government report announced the establishment of a national Cyber Security Operations Centre, within the military's Defense Signals Directorate [17]. In Turkey, "The Scientific and Technological Research Council of Turkey" is tasked as a coordinator organization on cyber security. They have been able to form the national cyberspace security policy in 2009.

But the main problem is to establish a universal consensus on cyber threat. In recent years, a number of international communities have drawn the main frame and discussed the initial steps that need to be taken against cyber threat. However, global measures against cyber terrorism has not been addressed specifically yet.
European Commission Reports reveal the incoming threat as:
"The new information and communication technologies are having a revolutionary and fundamental impact on our economies and societies. In fact, the success of the information society is important for growth, competitiveness, and employment opportunities and has far-reaching economic, social, and legal implications. However, in the hands of persons acting in bad faith, malice, or grave negligence, information society technologies (ISTs) may become tools for activities that endanger or injure, the life, property, or dignity of individuals or even damage the public interest." [18]
"Despite the many and obvious benefits of the modern electronic communications development, it has also brought with it the worrying threat of intentional attacks against information systems and network platforms/infrastructures. As cyberspace gets more and more complex and its components more and more sophisticated, especially due to the fast development and evolution of (broadband) Internet-based platforms, new and unforeseen vulnerabilities may emerge." [19].
The European Union has therefore taken a number of steps to fight harmful and illegal content on the Internet, protect intellectual property and personal data, promote electronic commerce and tighten up the security of transactions. However, in spite of the EU initiatives, many observers believe that cybercrime requires an international response that should include countries that are havens for cybercriminals [20].
Council of Europe (CoE) Convention on Cybercrime released the first international declaration on crimes committed via the Internet and other computer networks. Four categories of criminal offenses are defined in the CoE Cybercrime Convention:

1) Offenses against the confidentiality, integrity, and availability of computer data and systems;
2) Computer-related offenses;
3) Content-related offenses;
4) Offenses related to infringements of copyright and related rights.

The purpose of this convention was "to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective, and to enable the collection of electronic evidence of a criminal offence" [21]. In this regard, international legal measures play a critical role in countering cyber terrorism. Since the nature of the cyber terrorism issue is global then the response should be global as well. Globalization of crime demands globalized law enforcement [22].
The four criminal offenses defined above, confirm the ideas presented in the second part of this paper "The Term Cyber Terrorism". International common definition of the cyber terrorism should not only include destruction, degrading and denial with or through cyber- or IT-related means, but should also include the use of internet website contents for terrorist purposes.

In order to establish a global cooperation, a concerted strategy and policy should be constituted. There is a need to continuously watch, examine, observe and review terrorist organization websites. In order to maintain a common understanding and cooperation among international community, a consistent intelligence sharing and assembling process should be carried out. It is vital in our era, since terrorist organization websites and vulnerabilities of the ITs offer terrorists lots of opportunities for their activities.

Collecting intelligence is the starting point and the key part of building an international cooperation. Afterwards defensive and offensive (deterrence) collaborative actions should be set out. Counter information and cautions to the related public opinion and parties must be provided by the international organizations as defense strategies. The collection of electronic evidence whenever it relates to terrorism is crucial for the nations who desire to cooperate. An "Intelligence pool" should be created in order to collect and share the intelligence simultaneously among the nations. This intelligence pool should not only monitor and gather information from terrorist websites, but should also collect electronic evidence for the potential cyber attacks.

Knop, offers an "open source intelligent system" on this issue. Instead of a hierarchical organization, there should be a network, and knowledge should be pooled. There should be committee management, and a credit point system. Governments should be allowed to use the resource only to the extent that they contribute good quality information and analysis [1]. The collective open source idea is a well thought-out response to the challenge of organizing international cooperation regarding terrorist contents on the Internet.

"M.U.D." (Monitoring, Using, Disrupting) approach is also a well-organized applicable approach. According to MUD approach; "monitoring" forums, blogs and frequently updated terrorist websites gives information about terrorist organizations' motives, mindsets, audiences, operational plans and potential target population and potential targets for attack. In the "using" step, retrieved data can be achieved to identify the propagandists, members, connections between people and organizations. This approach also helps to identify the countries those support terrorists by means of funding and politics. Disrupting step can be applied by infecting the terrorist websites by viruses, worms and by destroying or changing the contents of the website [1].

MUD approach has many advantages. But disrupting step has the challenge of gathering all the participating nations on the same denominator. While one country wants to disrupt the content on a website, another country could still want to monitor and use that website in order to get more intelligence.

Monitoring and using steps could be organized to understand the radicalization process of the terrorist organizations. De-radicalization opportunities can be obtained after understanding the reasons of the radicalization. The target population of the terrorist organization could be reached and educated with a comprehensive human focused education program campaign on the web and media. This campaign should be developed and prosecuted for the various types of regional cultures.

According to Janczewski, building company defenses will not always be enough to reduce threats. Quite often a wider cooperation is required. This cooperation may be split into two streams. Stream one would group organizations using similar systems or facing similar threats. The best example would be the cooperation between Internet service providers (ISP). The handling of distributed denial of service attacks is much simpler if ISPs are working together on this issue. Stream two is to coordinate national and international law. Common sense dictates that if hacking would be made strictly forbidden in each and every country, then the number of hacking attacks would definitely drop across the globe [5].

Laws and conventions such as Council of Europe Convention on Cybercrime should be utilized to facilitate worldwide cooperation. Unless these conventions are expanded to include all the nations in the world, efforts will remain relatively inconclusive. But in order to respond to this kind of global threat, the key factor is to agree on a common definition of the threat. However implausible it may seem to reach a global consensus, there are many examples where such worldwide cooperations are already in effect. Air traffic control is an example of such global security arrangements.

Since the provisions of international agreements supersede the provisions for international cooperation, not only bilateral agreements but also multilateral agreements among nations must be signed. UN Security Council should also focus on cyber terrorism threat. Most of the permanent members of the Council are also the most vulnerable and targeted countries in the world. These countries also host most of the international cyber attacks. According to the charter of the UN, all members of the United Nations agree to accept and carry out the decisions of the Security Council. While other organs of the United Nations make recommendations to governments, the Council alone has the power to take decisions which member states are obligated under the charter to carry out. Therefore, worldwide cooperative law enforcement decisions against cyber terrorism could be taken under UN. Only under UN common definitions of "terrorism" and "cyber terrorism" could be generated and also "intelligence pool" against cyber terrorism could be formed. Since the nature of the cyber threat is global and spans throughout the world, the organization to respond this threat should be comprehensive and global.

A robust, international legal framework under UN that addresses cyber aggression is the most critical component of a comprehensive approach to deter cyber attack, much more critical than national offensive and defensive cyber capabilities. International law and norms are fundamental to deterrence because states "share an interest in adopting or codifying common standards for the conduct of international transactions…or in promoting or banning specific kinds of behavior by" states [23]. In this way, international law builds the framework that guides how and when states employ offensive and defensive cyber capabilities and forms the foundation of cyber deterrence. International law adds certainty to punitive actions and amplifies the costs of cyber attack by engendering a negative response from the international community, not just from the attacked state [24].

Unfortunately legislative measures are not adequate to fight against cyber terrorism. Military deterrence measures should be established in order to make

terrorists hesitate exploiting internet for their own destructive purposes. Proactive actions are required to disrupt the information on these websites and to locate and neutralize the attack's origin. In order to take offensive deterrence measures, NATO and other international organizations should establish deterrence strategies and keep agile and quick response teams always at their finger tips.

B. Military Cooperation against Cyber Terrorism (Cyber Deterrence and NATO)

The term "cyber deterrence" is the proactive measures that are taken to counter cyber terrorism activities. The mission of cyber deterrence is to prevent an enemy from conducting future attacks by changing their minds, by attacking their technology, or by more palpable means (such as confiscation, termination, incarceration, casualty or destruction) [25]. In response to a cyber attack, retaliation is possible, but is not limited to the cyber domain. For example, in the late 90's the Russian government declared that it could respond to a cyber attack with any of its strategic weapons, including nuclear [26].

NATO is the unique international military organization in the world that has cyber-defense and deterrence capability against cyber terrorism. The cyber terrorism against critical infrastructures and ITs is a growing threat for the member countries as well. Since the origin of an attack can be oversees, then it should be treated like an intercontinental ballistic missile attack. Moreover, the possibility of a large-scale cyber attack that comprises military force components is much more than the possibility of a ballistic missile attack. And also missile defense system will be able find adequate time to detect and engage the missile in seconds. But in the response to cyber attacks, there may not be sufficient amount of time to react. Therefore, NATO's next concept should cover cyber-attack defense shield, following the missile defense shield.

NATO's new Strategic Concept focuses on importance of terrorism and cyber-terrorism. According to Strategic Concept; cyber attacks are becoming more frequent, more organized and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organized criminals, terrorist and/or extremist groups can each be the source of such attacks [27].

NATO aims to combine the cyber-deterrence abilities under centralized defense system. Strategic concept intends to develop further NATO's ability to prevent, detect, defend against and recover from cyber-attacks, by using the NATO planning process to enhance and coordinate national cyber-defense capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations [27]. This is the first time that an international organization seriously declares its members are going to coordinate and cooperate their national cyber-defense capabilities.

Experts report on the new concept emphasizes that it is vital for NATO to respond to the rising danger of cyber attacks. Report reveals that NATO must accelerate efforts to respond to the danger of cyber attacks by protecting its own communications and command systems, helping allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defense capabilities aimed at effective detection and deterrence [28].

According to report the most probable threats to NATO in the coming decade are unconventional. Three in particular stand out:

- An attack by ballistic missile,
- Strikes by international terrorist groups,
- Cyber assaults of varying degrees of severity.

Since the next significant attack in the near future might be expected from cyberspace, NATO has taken some steps to develop these capabilities through creation of a Cyber Defense Management Authority, a Cooperative Cyber Defense Centre of Excellence, and a Computer Incident Response Capability. Nonetheless, serious gaps still exist in NATO's cyber defense capabilities.

Already, cyber attacks against NATO systems occur frequently, but most often below the threshold of political concern. However, the risk of a large-scale attack on NATO's command and control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defense measures under Article 5. Effective cyber defense requires the means to prevent, detect, respond to, and recover from attacks.

Utilizing NATO's Strategic Concept and the Experts Report on the Concept, a series of recommendations can be deducted.

- All NATO members should recognize that cyber attack is a growing threat to the security of the Alliance and its members.
- A major effort should be undertaken to increase the monitoring of NATO's critical network and to assess and furnish remedies to any vulnerabilities that are identified.
- The Centre of Excellence should help members improve their cyber defense programs through training.
- Allies should expand early warning capabilities in the form of a NATO-wide network of monitoring nodes and sensors.
- The Alliance should be prepared to send an expert team to any member country experiencing or threatened by a major cyber attack [28].
- Over time, NATO should plan to mount a fully adequate array of cyber defense capabilities, including passive and active elements.
- The Alliance should consider giving NATO military leaders certain pre-delegated authorities, based on agreed rules-of engagement, to respond in an emergency situation of a cyber attack [28].
- Member countries should establish their own cyber response teams, as well. Cyber defense and deterrence exercises that include different member and PfP nations should be held more frequently to train these quick response teams and share experiences on the issue. (e.g. Baltic Cyber Shield (BCS), as a highly useful international technical cyber defense exercise, was executed in May 2010. The exercise was organized

in collaboration with several organizations coordinated by Cooperative Cyber Defense Centre of Excellence (CCDCOE) and Swedish National Defense College (SNDC). An overall objective of the exercise was to gather lessons identified for the future cyber shield exercises planning [29].)

VI. RECOMMENDATIONS AND CONCLUSION

For all the reasons discussed above, it is an obligation to develop an international game plan in order to fight against cyber terrorism. Therefore, an 8-step global counter cyber-terrorism game plan is offered:

Step 1. Reaching to a common definition of terrorism and cyber terrorism is the starting point. Which activities on the internet (e.g. hacking, propaganda, attacking to infrastructures etc.) should be counted as cyber terrorism must be defined exactly. Speaking the same language or creating a common technical language could be a commencing point.

Step 2. Essential national and international legal measures have to be taken. International legal arrangements should be realized. Then national legislation has to be harmonized with the international legislation.

Step 3. Both bilateral and multilateral agreements on cyber security cooperation should be signed among nations.

Step 4. An intelligence pool should be created in order to collect and share the intelligence simultaneously among the nations. Collecting intelligence should include not only monitoring terrorist websites but also collecting electronic evidence for the potential incoming cyber attacks.

Step 5. Cyber defense expert teams should be created and charged internationally whenever a country encounters with a cyber attack. The number of quick response teams that countries own could be raised by the help of NATO's Computer Incident Response Capability and Cooperative Cyber Defense Centre of Excellence. An international counter cyber attack response training programme should be established.

Step 6. International counter-cyber attack exercises should be planned and executed in order to help the nations share their proficiency and experience.

Step 7. A well-organized international decision-making process that spans from detection to destruction (or disruption) of the cyber attack should be formed. Internationally authorized executives should respond to any attack concerning international security, based on agreed rules-of engagement.

Step 8. After-reaction analysis should be accomplished in order to identify and improve the weak points of the system. A feedback should be carried out for examining of the necessary innovations.

In consequence, cyber terrorism is a growing concern for the whole international community. The current regime of international laws, norms, and definitions not only insufficiently addresses cyber terrorism; it actually intensifies the dangers of the threat by creating a gray area or gap that can be exploited by cyber terrorists. Response to this global threat should be global as well. National efforts should be coordinated internationally to be successful against cyber terrorism. Countering

this threat requires not only legislative but also military cooperation including deterrence strategies. United Nations and NATO are two key international organizations. Due to UN's unique international character, and the powers vested in its founding charter, the organization can take action on a wide range of issues. Common definitions, international legal amendments and multilateral agreements might be considered and discussed under UN. And the steps concerning international military deterrence could be discussed under NATO and shaped under the guidance of Strategic Concept of NATO. It should be kept in mind that, international cooperation against global cyber terrorism threat is crucial and developing further proactive strategies for UN, NATO and other international organizations (e.g. European Union, Council of Europe, G-8, OECD) is essential.

REFERENCES

[1] K. Knop, "Institutionalization of a web-focused, multinational counter-terrorism campaign – Building a collective open source intelligent system, A discussion paper," Responses to Cyber Terrorism, Centre of Excellence Defence Against Terrorism, Ankara, Turkey (Ed.) IOS Press, 2008, pp.8-23.

[2] P. Wilkinson, Political Terrorism, London, 1974.

[3] M. Bozdemir, "What Is Terror and Terrorism?," School of Political Sciences Press and Publication College, 1981, v, vi. See also Wilkinson, P., (op. cit.), p. 17, and Crenshaw, M., 'The Concept of Revolutionary Terrorism', Journal of Conflict Resolution, September 1972, pp. 384.

[4] D. Denning, "Cyber terrorism. Testimony before the Special Oversight Panel on Terrorism," Committee on Armed Services U.S. House of Representatives, Georgetown University, May 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[5] L. J. Janczewski and A. M. Colarik, Cyber Warfare And Cyber Terrorism, Information Science Reference, 2008.

[6] M. J. Warren, "Terrorism and the Internet," Cyber Warfare And Cyber Terrorism, Information Science Reference, 2008, pp.42-49.

[7] T. Oba, "Cyberterrorism seen as future threat," Computer Crime Research Centre Tech. Report, April 2004, http://www.crime-research.org/news/2003/04/Mess0103.html

[8] P.W. Brunst, "Use of the Internet by terrorists, A threat analysis," Responses to Cyber Terrorism, Centre of Excellence Defence Against Terrorism, Ankara, Turkey (Ed.) IOS Press, 2008, pp.34-60.

[9] Z. Sütalan, "Current and future trends in terrorism," COE-DAT Newsletter vol.3 issue.16 p.37-49, July-September 2010.

[10] K. Curran, K. Concannon and S. McKeever, "Cyber terrorism attacks cyber warfare and cyber terrorism," Information Science Reference, 2008, p.1-6

[11] M. Rogers, "The psychology of cyber-terrorism," Terrorists, Victims and Society, In A. Silke (ed.), Chichester:Wiley, 2003, pp.77-92.

[12] A. Silke, "The Internet & terrorist radicalisation: the psychological dimension," Terrorism and the Internet, IOS Press, H.-L.Dienel et al.(Eds.), 2010, p.27-39.

[13] E. Çelebi, "Analysis of pkk/kongra-gel websites to identify points of vulnerability," Responses to Cyber Terrorism, Centre of Excellence Defence Against Terrorism, Ankara, Turkey (Ed.) IOS Press, 2008, p.127-141.

[14] R. Lemos, "What are the real risks of cyber terrorism?," ZDNet, 26 August 2002.

[15] J. J. I. Noble, "Cyber terrorism hype," Jane's Intelligence Review, 1999.

[16] D. Verton, “CIA to publish cyberterror intelligence estimate,” ComputerWeekly.com. 2004. http://www.computerweekly.com/Articles/2004/02/25/200518/CIA-to-publish-cyberterror-intelligence-estimate.htm

[17] “In the Crossfire: Critical Infrastructure in the Age of Cyberwar”, A global report on the threats facing key industries, commissioned by McAfee and authored by the Center for Strategic and International Studies (CSIS), 2010.

[18] European Commission. (2001c). Communication on creating a safer information society by improving the security of information infrastructures and combating computer-related crime (eEurope 2002) [COM(2000) 890 final, 26.01.2001]. Brussels, Belgium: European Commission.

[19] European Commission. (2001b). Proposal for a council framework decision on combating terrorism [COM(2001) 521 final, 19.09.2001]. Brussels, Belgium: European Commission.

[20] S. M. Kierkegaard, “EU tackles cybercrime, cyber warfare and cyber terrorism,” Information Science Reference, 2008, p.431-438.

[21] International Working Group (2002). “Common position on data protection aspects in the draft convention on cyber-crime of the Council of Europe,” Retrieved December 15, 2004 from http://www.datenschutz- berlin.de/doc/int/iwgdpt/cy_en.htm

[22] S. Özeren, “Cyberterrorism and international cooperation: General overview of the available mechanisms to facilitate an overwhelming task,” Responses to Cyber Terrorism, Centre of Excellence Defence Against Terrorism, Ankara, Turkey (Ed.) IOS Press, 2008, p.70-88.

[23] C. W. Freeman, Jr., “Diplomatic Strategy and Tactics,” US Institute of Peace, 1997, p.84.

[24] S. W. Beidleman, “Defining and Deterring Cyber War,” Strategy Research Project, U.S. Army War College, 2009.

[25] T. J. Mowbray, “Solution architecture for cyber deterrence,” 2010, Retrieved January 11, 2011, from http://www.sans.org/reading_room/whitepapers/warfare/

[26] M. Libicki, “Cyberdeterrence and cyberwar”, 2009, Retrieved January 27, 2010, from http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf

[27] Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. Adopted by Heads of State and Government in Lisbon, 2010. Retrieved January 9, 2011 from http://www.nato.int/strategic-concept/index.html

[28] “NATO 2020: Assured security; dynamic engagement analysis and recommendations of the group of experts on a new strategic concept for NATO,” Experts Report on New Concept. 17 May 2010.

[29] Baltic Cyber Shield Cyber Defence Exercise 2010, After Action Report, 2010.Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references)