TESAM Akademi Dergisi - Turkish Journal of TESAM Academy
Ocak - January 2019. 6(1). 213 - 247
ISSN: 2148 – 2462

E-GOVERNMENT AND CYBER TERRORISM: CONCEPTUAL FRAMEWORK, THEORETICAL DISCUSSIONS AND POSSIBLE SOLUTIONS[1]

Mahir TERZİ[2]

Abstract

Technology generates a new kind of terrorism which is called as cyber terrorism. Cyber terrorism is not only a tool for propaganda of traditional terrorism, but also a logic embedded in the cyber space. Cyber terrorism needs more attention for the security of "e-government" in terms of not only at national level, but also at international level. So the main purpose of this article is to study the interaction between "e-government" and cyber terrorism in the context of Actor Network Theory which provides a model and general frame for participatory democracy. For this reason, it is firstly explained what "e-government actually is. Afterwards, cyber terrorism is defined by generating a new one. Methodologically speaking, descriptive analysis has been made in defining and understanding "e-government", and a new definition for cyber terrorism has been generated by the method of induction. Finally, the interaction between "e-government" and cyber terrorism has been debated in the context of Actor Network Theory through the method of deduction in addition to the conclusions related to some prevention and advices. These measures and recommendations include the recruitment of qualified personnel, institutional capacity development, government support for brand antivirus software, cyber risk insurance, global cooperation and the creation of ethical codes.

Keywords: E-Government, Cyber terrorism, Actor network theory, ICTs, Cyber risk insurance, Ethical codes, Purple brain, International collaboration

1 Makalenin Geliş Tarihi: 23.02.2018 Makalenin Kabul Tarihi: 31.01.2019
2 Dr., mahirterzi@yahoo.com

Atıf: TERZİ, M. (2019). E-government and cyber terrorism: conceptual framework, theoretical discussions and possible solutions. *Tesam Akademi Dergisi* 6(1). 213-247. http: //dx.doi.org/10.30626/tesamakademi.528011 ORCID: 0000-0003-1308-2060.

E-Devlet ve Siber Terörizm: Kavramsal Çerçeve, Teorik Tartışmalar ve Olası Çözümler

Öz

Teknoloji, siber terörizm olarak nitelenen yeni bir tür terörizm ortaya çıkarıyor. Geleneksel manada terörizm için sadece bir propaganda aracı değil, ama aynı zamanda siber alana gömülü bir mantığı ifade eden siber terörizm, hem ulusal hem de uluslararası düzeyde, e-devletin güvenliği için daha fazla dikkat gerektiriyor. Bu nedenle, bu çalışmanın amacı, katılımcı demokrasi için bir model ve genel çerçeve sunan Aktör Ağ kuramı çerçevesinde, e-devlet ve siber terörizm arasındaki ilişkiyi incelemektir. Bu amaçla öncelikle e-devletin ne olduğu açıklanmış, ardından yeni bir tanım üretilerek siber terörizm tanımlanmıştır. Metodolojik açıdan konuşmak gerekirse, e-devleti tanımlamada ve anlamada betimsel bir analiz yapılmış olup, siber terörizm açısından da ilgili değişkenler dikkate alındığında tümevarım yöntemiyle yeni bir siber terörizm tanımı üretilmiştir. Son olarak Aktör Ağ Kuramı bağlamında, e-devlet ve siber terörizm arasındaki etkileşim, tümdengelim aracılığıyla tartışılmış ve nihayet bazı tespit, önlem ve tavsiyelere ilişkin düşüncelere yer verilmiştir. Bu önlem ve tavsiyeler; uzman personel istihdamı, kurumsal kapasitenin geliştirilmesi, marka antivirüs yazılımları için devlet desteği, siber risk sigortası, küresel işbirliği ve etik kodların oluşturulmasını içermektedir.

Anahtar Kelimeler:E-Devlet, Siber terörizm, Aktör ağ kuramı, BİT, Siber risk sigortası, Etik kodlar, Mor beyin, Uluslararası işbirliği

Introduction[3]

Unfortunately, there is no agreement on the definition of cyber terrorism. In other words, like terrorism, there is no universally accepted definition about cyber terrorism (Terzi, 2018, s. 107). Cyber terrorism which is also an international threat in accordance with its nature deserves international notice. Security deficient in the cyber space could bring about unrecoverable huge damages. Therefore, engineers and other technical specialists have to be included to the process of decision-making in combating cyber terrorism.

Another issue is to be able to determine the differences between cyber crime and cyber terrorism. Except being politically motivated, cyber crime and cyber terrorism overlaps. Such problem makes the struggle hard in terms of international law in particular. This means that collaboration at international level is much more important today than was it past.

The deprivation of universally accepted definition on cyber terrorism also triggers to contemplate the other danger like cyber warfare that will be able to be defined as operations in military attribute conducted by nation states through ICTs.

Solutions towards technological threats including cyber-crime, cyber terrorism and cyber warfare can be developed by better policies. Collaboration at international level also facilitates to produce better policies (Terzi, 2018, s. 107).

For future studies on cyber terrorism, intellectual performances can be revealed for legal remedies, technical arrangements and type of collaboration at international level in combating threats.

By proposing prospective solutions, the main purpose of this article is to study the interaction between "e-government" and cyber terrorism in the context of Actor Network Theory which provides a model and general frame for participatory democracy by pointing prospective and/or present threats via such intellectual performances.

3 This article is an updated and developed version of a previously published section of a book written as Turkish in 2015 by the author. A small part of this work was also presented in *Turkish* as a statement at the symposium in Ankara in 2017. The arguments and explanations about e-government and actor-network theory take part essentially in the master thesis, namely Information-Based Economy and E-Government: Transformation in the Public Administration, written in 2006 as English by the author of this article. The issues that provide the originality for this article are the discussion of cyber terrorism and the related opinions.

E-government

E-government" is not simply a technical innovation, but also is a necessary organizing model for economic, political and cultural transformation (Terzi, 2006, s. 33). So, in this part, it is tried to be clarify what "e-government" essentially is by categorizing the concept "e-government" in terms of some parameters including description, purpose, history, element, and vision as various countries absorb it in terms of their own cases, preferences and formularizations.

The Description of "e-Government"

To be able to define "e-government", it is needed to use some reference concepts such as "Internet", "Information and Communication Technologies (ICTs)", Effectiveness, etc. Because of different priorities specified by various governments, the term itself is not universally employed in the same meaning. However, upon minding to different definitions, one can notice some of the same references such as "Internet" and "ICTs". In the narrow sense, "e-government" is defined as internet service delivery and other internet-based activities like consultation. In the broader sense, e-government is equated with the use of ICTs in government services. That is, ICTs replace the concept of internet (Terzi, 2006, s. 34).

Nonetheless, as mentioned above, owing to the different primacies of the varied governments, the description of "e-government" can be commented as a capacity to transform public administration via ICTs. That is, "a new form of government which is built around ICTs" (OECD, 2003, s. 23).

İnce points out that "e-government" are a state of information and technique which benefits from the savings of paper (İnce, 2001, 22-6). According to Yücetürk, "e-government" is defined as the realization of relations and transactions between citizens or business world and government in electronic media (Yücetürk, 2004).

In the much broader sense, United Nations General Assembly states that "e-government is defined as strengthening democratic accountability, control and collective decision-making" while Organization for Economic Co-Operation and Development (OECD) uses the concept in the narrow sense by stating that "e-government is the use of Information and Communication Technologies, and particularly the Internet, as a tool to achieve better government" (OECD, 2003, s. 23).

Moreover, some organizations standardize the priorities and applications of "e-government" by taking especially the developing and under-developed countries into consideration. For example, the most prominent organization is the International Telecommunications Unity (ITU) which operates under the United Nations Organization. International Telecommunications Unity (ITU) declared in the Action Plan that "e-government" should be supported by all levels of government to enhance transparency, accountability and efficiency (ITU, 2003a: 8). That is, the concepts of transparency, accountability and efficiency are regarded to be connected with ICTs in the World Summit on Information Society which was held in Geneva in 2003.

On the outside of the references to Internet, ICTs, efficiency, transparency, accountability, democracy, etc. in some countries, "e-government" is seen as integration to the world beyond these concepts (Terzi, 2006, s. 35). For example, the Turkish Prime Ministry states that;

> *"The rapid developments in ICTs in a world where the globalization advances speedily and the boundaries disappear in economic sense enhance the distance between our country and contemporary countries. It is necessary to actualize re-organization which gives priority to the service towards citizens and provide the use of advanced technology with modern administration techniques by eliminating this distance to integrate with the world and to become "Information Society"* (Türkiye Bilişim Şurası, 2002, s. 211).

Thanks to these descriptions and accounts, it is explicit that because of the different priorities determined by various sources, there is no consensus upon the meaning of the term. Still, Internet and/or ICTs are the same basic means to be utilized in the organizing model of "e-government" (Terzi, 2006, s. 35).

The Purposes of "e-Government"

The different descriptions of "e-government" indicate that there is no single and same purpose about e-government. Any individual country keeps its own ends in accordance with its own economic and social conditions, and with its own priorities. While the purposes of "e-government" in the broad sense are stressed as efficiency and higher quality services, etc., those terms, on the other hand, are underlined as the integration with the globalizing world.

OECD Project's priorities, for example, are "to analyse e-government within

the framework of public governance" (OECD 2003, p. 24). "E-government" can help administrations do their duty better by strengthening good governance objectives and necessary administrative reforms. In addition, for OECD, the issues such as higher quality services, efficiency and greater engagement with citizens, better policy outcomes, etc. are accepted the subjects of "e-government". OECD also takes the public management reform into account in accordance with good governance purposes by asking for legitimacy, rule of law, transparency, accountability, integrity, effectiveness, coherence, adaptability, participation, and consultation. That is, public reform agenda focuses on using ICT "to transform the structures, operations and, most importantly, the culture of government" (OECD, 2003, p. 41).

In a broader sense, in the World Summit on the Information Society which was held in Geneva in 2003, in the Article 15 of the Action Plan, the purposes of "e-government" are charecterized as transparency in public administration, democratic process, efficiency, efficient allocation of resources and public goods, and international cooperation initiatives in order to increase transparency. Plan of Action counts the purposes of "e-government" in the same Article, as 1) Perform e-government strategies concentrated on applications that target to innovate and promote transparency in public administrations and democratic processes by developing efficiency and strengthening relations with citizens, 2) Improve national e-government attempts and services, at all levels, which are tailored to the demands of citizens and business, so as to obtain a more efficient disposition of resources and public goods, 3) Promote international cooperation attempts in the field of e-government, in order to enhance transparency, accountability and efficiency at all government levels (ITU, 2003a, p. 8).

Furthermore, the Action Plan takes account of e-business outside of the other topics such as e-employment and e-science. In the Article 16 it is mentioned that;

> *"Government policies should favour assistance to, and growth of Small, Medium-sized and Micro Enterprises in the ICT industry, as well as their entry into e-business, to stimulate economic growth and job creation as an element of a strategy for poverty reduction through wealth creation" (ITU, 2003a, p. 8).*

The European Information Society defines ICTs broader than OECD describes. Besides, one can see the much broader definition in the United

Nations Millennium Declaration assembled in September 2000. United Nations emit to guarantee the right of public to have access to information in Article 5, titled Human Rights, Democracy and Good Governance (United Nations, 2000).

In the Action Plan European Information Society proclaims to conform to internationally agreed development goals which include those declared in the Millennium Declaration in 2000 (Terzi, 2006, p. 37).

Bertucci recounts the utilities of "e-government" as:

- Solve the complexity of bureaucracy.
- Help the public and business to connect to government information and services online.
- Augment efficiency, transparency and accountability in the use of public resources.
- Participate in the digital economy.
- Accomplish greater openness and transparency of the policy-making process.
- Test the new media within the process of democracy.
- Make strong the democratic control over the accountability of service delivery through enhanced documentation, tracking and feedback mechanism (Bertucci, 2003: 1-14).

Özcivelek remarks the purposes of "e-government" as;

- *efficiency,* which will project to economical effectiveness,
- *governance*, which emerges with "e-government" that encourages the actors as media, various interest groups, political parties, decision-maker, public opinion, etc.
- *participatory democracy,* which is concluded as political equality and freedom of expression,
- *participation,* which bring about changing the concept of citizenship (Özcivelek, 2003, pp. 1-12).

Briefly, apart from the organizations which specify standard purposes

on "e-government", every individual country detects the objectives of "e-government" with respect to its own social and economic conditions.

The History of "e-Government"

Historical account of "e-government" demonstrates not only the purposes of the governments, but also why various countries give priority to different "e-government" applications[4].

To exemplify, "e-government" studies in UK and Canada started in mid-1990s. British government administered the project of "United Kingdom Gateway" along with Microsoft Company. The aim of the project was to unify 200 central and 482 local state institutions for 60 million citizens and 3 million place of employment. In Argentina, the government provided a service that involves transforming driver's license into smart card in 1995. Hence, the process has progressed well, providing a considerable input increase against free and other legal payment. In El Salvador, the government put a similar application into practice in 1999. By this application, driver's license, vehicle license and taxes related to these documents were entered in the system of smart card. In Finland, citizens in this country have started to use smart ID card since December 1999. E-Code given by Finland Public Registration Office takes place on the card. The card gives individuals an opportunity of digital signature on the internet. In addition, Finland Government established structures for youth to be able to monitor the parliament and the municipality assembles via Internet. In Spain, the government has established tax portal with the support of IBM Company. This application has provided public information on tax via internet. Therefore, the citizens and companies fill out the written forms of tax in the electronic media and pay the tax debts via internet. Singapore is one of the leaders of "e-government" applications in the world. Singapore Government put its national Plan of Information Technology into practice in 1981. This plan is the basis of "e-citizen" gateway, which is known as the most advanced gateway today. "E-citizen that provides services in more than 150 fields such as education, accommodation, health, job, transportation and travel, was put into practice in 1997. In Portugal, the government put the INFOCID Project into practice in 1991 and improved this project in 1993. One of the aims of INFOCID is to facilitate tax process for taxpayers and to reduce the amount of the written transactions based on the paper. Therefore,

4 The examples including UK, Argentina, El Salvador, Finland, Spain, Singapore, Portugal and USA have been summarized from e-Devlet Raporu (e-Government Report) (2002) published by Türkiye Bilişim Şurası (2002, 253-57).

taxpayers can get the information related to tax paying which interests them. Payments can be made through the smart card. In USA, the concrete studies about "e-government" were primarily put into practice at level of local authorities. While California State Portal, for example, provides online services about traffic tax, renewal of license, etc., North Carolina State Portal started to provide special content and online services for employment and public staff in 2000. The US Government has provided an "e-learning" system for government employees via online virtual campus with a wide range of courses since 2002 (Türkiye Bilişim Şurası, 2002, pp. 253-257).

Thanks to the examples of "e-government" applications in the world, it is explicit that most of these applications are engaged in using Internet than using ICT for the moment. As a matter of course, it is possible to say that governments perceive "e-government" as a tool of communication with citizens, stakeholders, and other government institutions by giving and obtaining information. Another highlighted point is that "e-government" applications have come out as a result of search for comfort such as tax-paying, renewal of license, acquisition of knowledge, smart card, etc. which citizens and stakeholders demand. Nonetheless, in examining the declarations of international organizations such as OECD and ITU, and noticing the performances of these organizations, it is possible to understand explicitly or implicitly that the purpose of "e-government" and the objective of using ICTs, particularly Internet, are greater than an individual country's objectives which an individual government gives priority in accordance with their social and economic circumstances (Terzi, 2006, pp. 40).

Those greater intents put forward by international organizations will be explained under the sub-subheading of "vision of e-government". Another important matter is now the elements of "e-government". It is significant to describe the elements of "e-government" as they help to grasp the general purpose of "e-government".

The Elements of "e-Government"

Even though there is a series of different priorities for the nations, it is likely to collect the elements of "e-government" into three categories. These are citizens, business world and public institutions. These are called as e-citizen, e-business and e-institution in accordance with "e-government" respectively. Turkish Prime Ministry, for example, determines the elements of "e-government" as e-citizen, e-business and

e-institution. E-business includes e-worker whilst e-institution contains e-staff (Türkiye Bilişim Şurası, 2002, p. 206).

"E-government" covers all the society with its elements which include citizens and foundations such as business enterprises and public institutions. As "e-government" is an innovative means of practicing the duties and services that the state has to offer to her citizens and that the citizens are to perform for the state in the electronic media as interactive, uninterrupted and safe; then, it expresses a new form of government. Each element will try to actualize the fact of "e" in itself and "e-government" will come into being with time. However, in spite of various projects and priorities announced by different nations, with the declarations of intergovernmental organizations and in accordance with the structure of ICTs, especially Internet, it is possible to assert another component. This is the state itself. That is, apart from the relation between government itself and its elements such as citizens *(e-citizen)*, business world *(e-business)* and institutions *(e-institution)*, there is an *e-relation* between one state and another or between one government and another (Terzi, 2006, p. 41).

The Vision of "e-Government"

Under this sub-subheading it is helpful to analyze the vision of "e-government" identified by intergovernmental and international organizations to understand what the future of "e-government" is by reviewing the arguments of intergovernmental and international organizations. Despite different priorities of various governments and nations, these regional, especially international and intergovernmental organizations aim at standardizing the objects of "e-government" all over the world by taking aim at the developing and underdeveloped countries in particular. Through the United Nations' "Principle Declarations" and "Action Plan" stated and published internationally, it is obvious that "e-government" via ICTs is not the aim but a means. E-government is merely a part of the whole like other transformations such as e-democracy, e-transformation, e-business, e-governance, etc. (Terzi, 2006, p. 42).

The General Assembly of United Nations gathered in New York from 6 to 8 September 2000 declared its purposes in the United Nations Millennium Declaration. In the Article 6 the United Nations mentioned about democratic and participatory governance by stating that;

> *"Democratic and participatory governance based on the will of the people best assures these rights [Men and women have the right to live their lives and raise their children in dignity, free from hunger*

> *and from the fear of violence, oppression or injustice]" (United Nations, 2000)*

In the Article 13 the United Nations General Assembly emphasized the importance of good governance and transparency in the financial, monetary and trading systems, stating that "...It also depends on transparency in the financial, monetary and trading systems. We are committed to an open, equitable, rule-based, predictable and non-discriminatory multilateral trading and financial system" (United Nations, 2000).

In addition, the United Nations General Assembly remarked some subjects including human rights, democracy and good governance. In the Article 25 the United Nations General Assembly aimed at strengthening the principles and practices of democracy, attributing to Article 24 by stating that "We resolve therefore to strengthen the capacity of all our countries to implement the principles and practices of democracy and respect for human rights, including minority rights" (United Nations, 2000).

Nevertheless, the United Nations Organization which offers unity with its agencies dependent on itself takes these agencies into account to put its aims into practice (Terzi, 2006, p. 43). In the Article 30, for instance, the United Nations General Assembly states that;

> *"We resolve therefore to strengthen further cooperation between the United Nations and national parliaments through their world organization, the Inter-Parliamentary Union, in various fields, including peace and security, economic and social development, international law and human rights and democracy and gender issues" (United Nations, 2000).*

General Assembly of the United Nations gathered in another session, in Monterrey, Mexico, on 21-22 March 2002 informed the draft outcomes of the International Conference on Financing for Development, attributing frequently to the United Nations Millennium Declaration. General Assembly of the United Nations specified its purposes in the framework of development by attributing to some of the key concepts and expressions such as globalization, good governance, development for all, and an effective, efficient, transparent and accountable system for mobilizing public resources and managing their use (Terzi, 2006, p. 43).

The General Assembly stressed many subjects in Monterrey Consensus. Some of these are:

- Domestic economies which are interwoven with the global economic system.
- The opportunities and challenges of globalization.
- A holistic approach to the interconnected national, international and systematic challenges of financing development.
- Promotion of national and global economic systems based on the principles of justice, equity, democracy, participation, transparency, accountability and inclusion (United Nations, 2002, pp. 1-16).

In this Consensus, the General Assembly intended to eliminate the challenges in front of globalization and of financing development through its financial organizations such as IMF and World Bank oriented to economic development by stipulating good governance, investments in basic economic and social infrastructure including education, health, etc. (Terzi, 2006, p. 44).

The points summarized up here under the title of the "vision of e-government" cannot be admitted to involve directly "e-government" via ICTs. Yet, International Telecommunication Unity, which is in charge under the Specialized Agencies and which is dependent on the United Nations Organization, clarifies what the vision of e-government is and the importance of declarations stated by the General Assembly of United Nations and the relation among the purposes in general. While Monterrey Consensus emphasizes the development, sustainable development and sustainable economic growth by financing development, ITU (International Telecommunication Unity) emphasizes the development through ICTs. At the same time, the Declaration of Principles and Action Plan of ITU in particular that was assembled in Geneva in 2003 stressed the vision of e-government. ITU that was gathered for building Information Society announced its aims through Declaration of Principles and Action Plan with the last corrections in December 2003 (Terzi, 2006, p. 44).

The representatives of the people of the world stated some of their goals in Article 1 of Declaration of Principles in the World Summit on Information Society by declaring that;

> *"...our common desire and commitment to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and*

> *knowledge, enabling individuals, communities and people to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights" (ITU, 2003b, p. 1).*

ITU that assumes "to pay special attention to the needs of people of developing countries, countries with economies in transition, Least Developed Countries, Small Island Developing States, Landlocked Developing Countries, Highly Indebted Poor Countries, counties and territories under occupation, countries recovering from conflict and countries and regions with special needs as well as to conditions that pose severe threats to development, such as natural disasters" (Article 16) views ICT as not aim but solution to the following in Declaration of Principles (Terzi, 2006, p. 45):

- To provide new forms of solidarity, partnership and cooperation among governments and other stakeholders (Article17).
- To foster and respect cultural diversity, to encourage international and regional cooperation (Article 19).
- To achieve a sustainable development (Article 33).
- To contribute rule of law accompanied by a supportive, transparent, pro-competitive, technologically neutral and predictable policy and regulatory framework reflecting national realities (Article 39).
- To support foreign direct investment, transfer of technology, and international cooperation, particularly in the areas of finance, debt and trade, as well as full and effective participation of developing countries in global decision-making (Article 40).
- To create benefits in all aspects of our daily life such as government services, health care, education, employment, agriculture, transport, protection of environment and management of natural resources, and culture (Article 51).
- To encourage eradication of poverty, to contribute to sustainable production and consumption patterns and reduce traditional barriers by providing an opportunity for all to access local and global markets in a more equitable manner (Article 51).

- To stimulate respect for cultural identity, cultural and linguistic diversity, traditions and religions and to foster dialogue among culture and civilizations (Article 52).
- To preserve cultural heritage (Article 54).
- To uphold basic values of freedom, equality, solidarity, tolerance, shared responsibility and respect for nature (Article 56).
- To build global Information Society (Article 61).
- To realize regional integration with the development of global Information Society (Article 62), etc. (ITU, 2003b, pp. 1-9).

The purposes, some of which were accounted in Declaration of Principles, it can be said that international organizations remark purposes, comparatively more meaningful, according to individual countries. In other words, International Organizations like ITU does not perceive ICTs to be just a simple application, but perceives it as a project for seeking strategy for globalization.

In addition to these objectives offered in Principle of Declaration, ITU explained the necessary steps for these ends in its Action Plan which was come to an agreement in the World Summit on "Information Society" in Geneva in 2003 (Terzi, 2006, p. 46).

To sum up, it seems enough to accent the concepts of efficiency, transparency, and accountability in accordance with Action Plan which has been mentioned about under the sub-subheading of "purposes of e-government".

Nonetheless, in spite of United Nations' emphasis on the importance of development for all people, it is not wrong to say that there is a contest between globalization and nationalization since European Union declares its purposes for "Information Society" and its tools like "e-government" by aiming at its member countries and citizens while the United Nations Organization informs the objectives for globalization and its tools oriented towards all world people (Terzi, 2006, p. 46).

Commission of the European Communities, assembled in Brussels in 2002 for eEurope 2005, for instance, presented its goals towards "Information Society" by documenting its action plan. The Commission set priorities as having modern online public services, "e-government",

e-learning services, e-health services, a dynamic e-business environment for "stimulating secure services, applications and content that create new markets and reduce costs and eventually increase productivity throughout the economy" and for contributing e-inclusion, cohesion and cultural diversity (Commission of the European Communities, 2002, pp. 6-8).

As a result "e-government" is an organizing model not only for articulation to globalization, but also for establishment of "Information Society" at national level for participating information-based economy and building global Information Society.

Cyber Terrorism

In the narrow sense cyber terrorism that is defined as "terrorism that involves computers, networks, and the information they contain" (Coffman, 2006) is expressed in different types by different mental formulations.

The Federal Emergency Management Agency (FEMA) defines cyber terrorism as "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" (Wilson, 2007, p. 7). Nonetheless, this definition of cyber terrorism does not give information enough to understand destructive results of cyber-terrorism such as economical damage and death.

FBI defines cyber terrorism as "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents" (Elmusharaf, 2004). This definition is also problematic since it reduces cyber terrorism to only violence.

Brenner says "cyber terrorism consists of using computer technology to engage in terrorist activity" (Brenner, 2007, p. 386). Although this definition is very wide, it does not point out that cyber terrorism is also international terrorism including international threat as opposed to any other kind of terrorism such as domestic or non-state terrorism.

As the present definitions of cyber-terrorism are not accepted as satisfactory in measuring the effects of cyber terrorism in detail, *a new one has produced in this article to grasp cyber terrorism in compliance with e-government*. For this purpose it has been used the components of

Criminal Law in defining terrorism by being inspired by Başeren[5]. These components are cause, instrument, aim and intent.

Cause is politically motivated. Instrument is motion. Aim is prevention of performance. Intent is to influence.

Cyber terrorism, which is politically motivated, is to influence the behaviour of millions of people and to break the run of everyday life as a result of prevention of performance resulted from a motion that harbours to realize or to make threat for the corruption, inclusion or violation against cyber systems including people in cyber space with reference to global infrastructure based on ICTs.

In this definition, the reason why people are accepted as a segment of cyber systems will be explained under the title of "Actor Network Theory".

The Development Process of Cyber Terrorism

Cyber terrorism develops its scope and content as to the goals that it defines in time along with flourishing and diseminating of Internet technology.

While some people use the term "cyber-terrorism" to refer to any major computer-based attack on the U.S. government or economy in 1980s (Coffman 2006), it has been distinguished that the content of cyber terrorism is enriched. For example, according to the Bureau of Alcohol, Tobacco, and Firearms, Federal agents investigating at least 30 bombings and four attempted bombings between 1985 and June 1996 recovered bomb-making literature that the suspects had obtained from the Internet (Anti-Defamation League, 1998).

Some examples of cyber terrorism could be given as follows.

Tupac Amaru sympathizers in the U.S. and Canada established several solidarity Internet sites, one of which included detailed drawings of the terrorists' plan of assault on the Japanese Ambassador's residence after the terrorist group Tupac Amaru in Peru attacked the Japanese Ambassador's residence in Lima and held scores of diplomatic, political and military officials' hostage in December 1996 (Wikipedia, 2009a).

5 In defining terrorism, Başeren (2006) uses the components of cause, instrument, and aim and of intent. Cause is politically motivated. Instrument is motion. Aim is a result like death. Intent is to influence. According to Başeren (2006), terrorism, politically motivated, is to influence and to conduct the behaviour of the millions of people via motion including violence with a result like death by horrifying.

Among the most electronically sophisticated extremist groups of Latin America, Mexico's Zapatista guerrillas are prominent. They have been rallying support online since their 1994 uprising (Wikipedia, 2009b).

Islamic militant organizations also use the Internet to disseminate their anti-Western, anti-Israel propaganda. Several Internet sites created by Hamas supporters, for example, carry the organization's charter and its political and military communiqués. Others, like the Hizb ut-Tahrir, a radical Islamic organization based in Britain, uses its web site to provide details to the public about its regular meetings around the United Kingdom. Others use the Internet to raise funds; Hezbollah, for example, the pro-Iranian Shiite terrorist organization based in south Lebanon, sells books and publications through its Web site (Anti-Defamation League, 1998).

The examples, mentioned above, are related to propaganda tools of traditional terrorism. Cyber terrorism is much more than that as it brings about the examples in compliance with its own ontology. In other words, cyber terrorism comes on the scene as a new kind of terrorism. The logic embedded in the cyber space uses its method in cyber space. But its destructive results are real and physical.

Some examples cited from Brochure on the Countering Cyber Terrorism Course held by the Centre of Excellence Defence against Terrorism in Turkey in 2006 have been listed below.

- A hacker disabled the computer system of the airport control tower at Worcester, Mass, in 1997.

- A hacker from Sweden jammed the 991 emergency telephone system in the west-central Florida in 1997.

- Someone hacked into Maroochy Shire that is Australia waste management control system and released millions of gallons of raw sewage on the town in 2000.

- A hacker was able to control the computer system that governs the flow of natural gas through the pipelines (Centre of Excellence Defence against Terrorism, 2006, p. 35).

In addition these examples, mentioned above, it is possible to take some probable scenarios into consideration as follows.

- Blocking emergency communications or cut off electricity or water in the wake of a conventional bombing or a biological, chemical, or radiation attack.

- Destroying the actual machinery of the information infrastructure.

- Disrupting the information technology underlying the Internet, government computer networks, or critical civilian systems such as financial networks or mass media.

- Using computer networks to take over machines that control traffic lights, power plants, or dams in order to bring about huge damage.

- Stealing classified files, altering the content of Web pages, disseminating false information, sabotaging operations, erasing data etc. in cyber milieu.

- Disrupt financial markets or media broadcasts, an attack could undermine confidence or show panic. Breaching dams, colliding airplanes, shutting down the power grid etc., via remote control systems (Coffman, 2006).

The Infrastructure of Cyber Terrorism

The infrastructure of cyber terrorism necessitates an appropriate structure for its own ontology. This structure comes on the scene as cyber space. What determines the cyber space is network infrastructure. Those such as, network, file server, local area network (LAN), wide area network (WAN), file transfer protocol (FTP), backbone, modem, TCP/IP protocols, internet servers, router, internet, world wide web (www), domain name system (DNS) etc., are elements of network infrastructure (Şenel, 2003, pp. 241-261).

In the cyber space, some vulnerabilities that will be able to be exploited by cyber terrorism have been defined for giving an opinion *thanks to the glossary of Trend Micro House Call* on web. These vulnerabilities are malware such as backdoor, phishing, Trojan horse, virus and worms, and grayware such as adware, hacking tools, remote access and spyware (Trend Micro House Call, 2014).

In addition, it is important to stress that cyber-crime also uses the same infrastructure and vulnerabilities like cyber terrorism. In that sense, except being politically motivated, it is difficult to determine the

differences between cyber-crime and cyber terrorism. Hence, it could be concluded that cyber-crime and cyber terrorism go arm in arm.

Illegal Formation against E-Government: Cyber Terrorism

In the network, authority, making-decision and control do not disappear; instead they are embedded in the network. Nodes and hubs will constitute this process. (Castells, 1998, pp. 410-28). In other words, it can be said that the state shows her existence in the cyber space.

Under the title of "E-government" it has been said that "e-government" is an innovative means of practicing the duties and services that the state has to offer to her citizens and that the citizens are to perform for the state in the electronic media as interactive, uninterrupted and safe (Türkiye Bilişim Şurası, 2002, p. 206) and that each element including citizen, business world and public institutions will try to actualize the fact of "e" in itself and "e-government" will come into being with time (Türkiye Bilişim Şurası, 2002, p. 206)

Since any state moves her reason of existence into network as ontological and potential threats will be able to be happened in the process of the development of cyber terrorism, it has to be considered that cyber terrorism will try to be power as opposed to e-government.

Nonetheless, the interaction between "e-government" and cyber terrorism will be scrutinized for a better comprehension in the following pages under the subtitle of "Actor Network Theory".

Actor Network Theory

Evaluating the interaction between "e-government" and cyber terrorism in the context of "Actor-Network Theory" is not easy task in essence as "Actor Network Theory", inspired by grounded theory and semiotics (Garrety, 2014, p. 15) is still in the process of development. Thus, many contributions come from different scholars in defining "Actor-Network Theory". Therefore, it is necessary to give some definitions of it, which takes the characteristics of "Actor-Network Theory" into consideration below.

"Actor-Network Theory (ANT)" is interested in the processes by which scientific disputes become off, ideas are accepted, and tools and methods are adopted. The work of science is involved in the enrolment and juxtaposition of heterogeneous elements including rats,

test tubes, colleagues, articles, grants, papers, and so on in this model. Methodologically, ANT has two major approaches including "follow the actor" through interviews and ethnographic research, and "examine inscriptions" which can travel across space and time, and be merged other works (van House, 2001).

ANT is the product of ongoing performances in the area of social studies of science and technology. For instance, when driving your car, there are lots of things like traffic regulations that influence how to drive a car. In a similar way, all acts that you execute and all of the factors that influence your realizing the acts should be considered together. This is absolutely what the term of actor network integrates. An actor network is the act that is linked together with all of its influencing factors that again are linked by producing a network. An actor network consists of links embracing both technical and non-technical elements. In the example of driving a car, not only the car's motor capacity, but also your driving training influences your driving. As a result, ANT mentions about the heterogeneous nature of actor networks (Hanseth and Monteiro, 1998, pp. 96-97).

The thing which is called as "Network Theory[6]" has developed a vocabulary that takes the distinction between subjects and objects, the subjective and objective into consideration. "Actant" replaces "Actor". "Actant" is more than human actor is. Both humans and non-humans could be actants (Couldry, 2008: 96; Tatnall, 2005, pp. 42-43). An "actant" could be "enrolled" as "allied" to give power to a position. When a biologist discusses the existence of molecule, the data that prove this existence are enrolled actants. An "actant" could be an automatic door opener. "In networks of humans, machines, animals and matter in general, humans are not the only beings with agency, not the only ones to act; matter matters" (Risan, 1997).

ANT has its roots in the studies of networks of interdependent social applications that establish work in science and technology. Both human and non-human participants are equally actants. They are defined as arguments or elements in the network. This brings about a relational epistemology that rejects the naive positivist view of objects or actors (Lemke, 2001).

ANT is a set of negotiations which define the progressive constitution of a network in which both human and non-human actors count identities

6 Network Theory is also called Graph Theory. A Graph consists of a set of nodes and of edges. Whilst nodes represent the processing units, edges represent the communication links between the units (Scheideler, 2004: 1-11).

according to prevailing strategies of interaction. Actor's identities and qualities are defined throughout the deliberations between representatives of human and non-human actants. "Representation" as a process of delegation is seen in its political dimension. "Translation" which is a multi-faceted interaction where actors construct common definitions and meanings, define representatives, and co-opt each other in the pursuit of individual and collective purposes is the most important of these deliberations. In the ANT, both actors and actants share the scene in the reconstruction of the network of interactions resulting in the stabilization of the system. Yet, the critical difference between them is that merely actors can put actants in circulation in the system (Bardini, 1997).

The concepts in the ANT comprise "regimes of delegation", "the centrality of mediation" and "the position" in which nature and society are not the reasons but the results of human scientific and technical work (University of Colorado, 2003).

ANT is based on no stable theory of the actor. In other words, it counts up the radical indeterminacy of the actor. For example, neither the actor's size and its psychological make-up nor the motivations behind his/her actions are predetermined. ANT is a break from the more orthodox currents of social science from this perspective. This hypothesis has opened the social sciences to non-humans-what is called as political ultra-liberalism- (University of Colorado, 2003).

ANT's prosperous methodology covers scientific realism, social constructivism, and discourse analysis in its central concepts of hybrids or "quasi-objects" which are real, social and discursive simultaneously. Its theoretical richness stems from its refusal to reduce explanations to natural, social, or discursive categories while recognizing the significance of each one. ANT stresses that 'the stability and form of artefacts should be seen as a function of the interaction of heterogeneous elements as these are shaped and assimilated into a network' (See J. Law, cited in Frohmann, 1995).

Network is consisted of actors, which all of them are not normally considered by the academically oriented sociologists. The network includes not only people and social groups, but also devices, entities and artefacts. For instance, engineers who design a new technology as well as those who participate in its design, development in any time continuously establish hypothesis and forms of argument that put the participants in

the field of sociological analysis. Thus, the participants are transformed into sociologists who are called as engineer-sociologists (Callon, 1983).

ANT is the infrastructure which is usually left out of the heroic accounts of scientific and technological achievements. For instance, Newton was not alone in creating the theory of gravitation. He was in need of the geometry of Euclid, the astronomy of Kepler, the mechanics of Galileo, the rooms, lab, etc. at Trinity College, and so on. In a similar way, any scientific or technological project can be asserted in the ANT (Goguen, 1998).

The modern worldview employs one-dimensional language running in the framework of opposite poles of nature and culture. Knowledge and artefacts are explained either by social constructionism (society) or by realism (nature). In order to pass over this dualism, a second dimension is necessary since society (subject, mind or brain) cannot be seen as the practice of science since both science and society are the consequences of the science and technology making. Accordingly, the second dimension is the process of nature/society construction that results in the stabilization of a strong network. There is a single focus of the analysis by merging these poles, instead of two poles one by one, now on (Miettinen, 1997).

As seen thanks to these definitions above, every definition more or less enlightens the matter. In essence, every explanation stresses some dimensions of ANT by emphasizing the characteristics of ANT. ANT is a set of deliberations that define the progressive constitution of a network in which both human and non-human actors assume identities according to prevailing strategies of interaction based on "regimes of delegation", "the centrality of mediation" and "the position" in which nature and society are not the reasons but the consequences of human scientific and technical work by opening the doors of social science to actants including human and non-human elements, and by rejecting positivist view of world (Terzi, 2006, p. 76).

With reference to the concept of Rousseau's "general will", the definition can be clearer.

> "There is often a great deal of difference between the will of *all and the general will; the latter considers only the common interest, while the former takes private interest into account, and is no more than a sum of particular wills…As long as several men in assembly regard themselves as a single body, they have only a single will which is concerned with their common preservation and general*

> *well-being…there are no embroilments or conflicts of interests; the common good is everywhere clearly apparent, and only good sense is needed to perceive it" (Rousseau, 1762/1989, p. 36).*

Actor Network Theory makes contribution to the approach of "general will" by implying that the will is realized with non-human actors in the cyber space. In other words, it can be said that Actor Network Theory provides a model for participative democracy by locating also non-human actors into the system.

In the context of terrorism, one of the autonomic conclusions of Actor Network Theory is that people constituting society are represented in the very large political spectrum and hence general will is acquired. Nonetheless, the theory is in the need of querying. Moreover, the only reason of terrorism is not to be lack of very large political spectrum[7].

Theoretically speaking, so long as the parameters and components of the theory are compatible with each other, there is no problem in defining "Actor Network Theory". Yet, the variant of culture creates the blank between theory and reality (Terzi, 2006, p. 76). So, some objections against Actor Network Theory are put forward as follows.

— By excluding interpretivism and hermeneutics[8], such efforts of defining "Actor Network Theory" give rise to reductionism, accepting "Actor Network" as heterogeneous network of aligned interests, and societies absorb the concepts and applications according to their needs, demands and circumstances in accordance with their interpretivism (Terzi, 2006, p. 77).

— From the perspective of anti-foundational approach that Rhodes

7 According to Crenshaw, one of the causes of terrorism is that "some groups are weak because weakness is imposed on them by the political system they operate in…" (Crenshaw, 1981: 388). In addition, for the argument that all experiences related to participatory democracy flourish in the environment of political insecurity, see Vera-Zavala (2006). Furthermore, it seems that Actor-Network Theory; for example, do not take the importance of confidence in voting via internet into account as silent vote is a principle in any parliamentary democracy.

8 For interpretivism, social reality is the outcome of its inhabitants. It is a world that is already interpreted by the meanings which participants produce and reproduce as a necessary unit of their everyday activities together. As for hermeneutics, social reality is interested in the understanding of human activities than can be acquired from the interpretation of the meanings which underlie these activities (See M. Terzi, cited from Blakie, 2006). In addition, for overall and comprehensive explanations about interpretivism and hermeneutics, see the book of Blaikie (1993: 36-48), titled Approaches to Social Enquiry.

asserts, it is significant to take whose story within which tradition into consideration. For example, in network management, there are a few participants in managing networks such as politicians, employees, and users. Each might talk about different stories about network management and its challenges (Rhodes, 2000, p. 73). Hence, anti-foundational approach concludes "practitioners learn by telling, listening to, and comparing stories; policy advice becomes the telling of relevant stories" (Rhodes, 2000, p. 76).

—E-institution, e-business and e-citizen are the elements of e-government in the case of e-government. In other words, they are the "actants". Yet, firstly, government institutions have privilege in actualizing network infrastructure by planning activities based on network and coordinating projects including portals which are put into practice. So, government is still in a strong position in terms of universal functions of administration/ management such as planning, organizing, co-ordination and control (Terzi, 2006, p. 80).

— Network system is also determining factor in satisfying the demands of the other "actants" such as individuals and ordinary people as the wants of these "actants" will be gratified in the limits circumscribed by the network. In other words, as long as the needs will be defined in the network, responses are given to those needs. There will be no equilibrium between non-human actor and human actor. Naturally, it could be said that non-human actor such as software, hardware, protocols and server capacity, so on, will have privilege as opposed to human actors, ordinary people in particular as a result of techno-determinism. This leads us, for example, to thinking about the possible threats of artificial intelligence. Google's chief engineer, Ray Kurzweil, notes that "it can be very difficult to write moral codes that would put a strain on the super-intelligence software." (BBC Türkçe Haber, 2014).

— There will be a difference of skill in dominating and using devices of ICTs even among not only ordinary people, but also staffs and employees. The more competence is the more power for participating in the process of decision-making. Naturally, those who have high competence for using the devices of ICTs could transform into close group as opposed to those who have less competence for using the devices of ICTs. Furthermore, they can occur as a new form of elitist who excludes those that are unskilled. So, in network management, with anti-foundational approach, it can be concluded that those, who are skilled, learn and act together by merely telling, listening to, and comparing their own stories that do

not probably reflect the stories of majority.[9] In addition, e-bureaucracy as an administration tool of not only governmental institutions, but also private organizations[10] could try to make the demands of other "actants" harmonious with its own demands to protect itself in the context of autopoietic and self-referential systems (Terzi, 2006, p. 81).[11]

As a conclusion, Actor Network Theory taking aim at participative democracy could not be an absolute solution for preventing terrorism and eradicating the causes of terrorism. Moreover, new technology means new kind of terrorism like cyber terrorism. In that sense, cyber terrorism needs more attention for the security of e-government in terms of not only at national level, but also at international level.

Nonetheless, in the context of cyber terrorism, it could be concluded that cyber terrorism will recruit candidates that are skilled and clever, and that cyber terrorism will be a weapon for elitists[12].

Potential Solutions

At the national level, e-government components need to create specialized staff teams to combat cyber threats and to increase the capacity of institutions to improve their infrastructures on information and communication technologies. The National Judicial Network Project (UYAP) in Turkey is a good example of this.[13]

At the individual level, it is unlikely that everyone will become a computer expert, but the individual states have important tasks in order to ensure

9 Conversely, for the argument that "e-government" provides high participation of people to the process of decision-making and results in a transparent management, see Koyun (2003: 76-112).

10 According to Weber, "the bureau" is often called "the office" in private organization. That is, the characteristics of "bureau" in public institutions are current for "office" in private organizations. Weber states that it does not matter for the property of bureaucracy whether its authority is called as "private" or as "public" and that the principle of hierarchical office authority is found in all bureaucratic structures including state, private enterprises and ecclesiastical structures (Weber, 1973: 24).

11 Self-referentiality means that some systems in the nature determine mostly their directions of entity by realizing their own organizing and by not reacting directly to the pressures coming from outside. So, all feedbacks are internal to themselves providing that those feedbacks are expressive for keeping the system alive as autopoietic (Üstüner, 2003: 54-57).

12 Gouldner describes technical scientist as those who have theoretical knowledge. For Gouldner, there will be two elitist classes in the futurity. While one is technical intelligentsia, the other is political intellectuals (Dura and Atik, 2002: 39).

13 Details for National Judicial Network Project, see Uysal (2016).

the security of the national cyber border. In Turkey, for example, the country needs brand anti virus software company or companies such as Kaspersky, AVG, and McAfee. In this sense, the financial support and encouragement of the state is important.

Studies should be carried out on how to improve ethical codes in order to prevent the ways in which information and communication technologies can harm humanity. Ethical codes are very important since, on the one hand, there are robots that operates like a surgeon, there is, on the other side, a process that can be evolved to create killer robot as in the film "Terminator". Cooperation with universities is important in creating those ethical codes because it is not yet known by the institutions (private or official) how to create these ethical codes. Otherwise, the abilities of information technology can be used for corruption purposes, associating innocent people with terrorist organizations via special software as in the case of Purple Brain.[14]

There should be a global cooperation in the fight against cyber crime, especially in cyber terrorism; because the world must at least be aware of the global cost of cyber crime[15].

Taking the "cyber risk insurance" approach into the consideration to remedy the losses that cyber crime/cyber terrorism gives rise to is also one of the solutions for post-loss financial compensation.

Conclusion

"E-government" is seen as equivalent for keeping up with the times today in terms of not only technical aspect, but also especially social, economic, political and cultural transformation. "E-government" is an organizing model not only for articulation to globalization, but also for establishment of "Information Society" at international and national level where Information-Based Economy will bloom (Terzi, 2006, pp. 32-129).

Technology generates a new kind of terrorism. This new kind of terrorism is cyber terrorism. Cyber terrorism is not only a tool for propaganda of traditional terrorism, but also a logic embedded in the cyber space.

Cyber terrorism, which is politically motivated, is to influence the behaviour of millions of people and to break the run of everyday life as a

14Seehttp://www.posta.com.tr/mor-beyin-nedir-nasil-bylock-tuzagina-dustuler-haberi-1366539 for Purple Brain software developed by Fettullahist Terrorist Organization (FETÖ) to pollute innocent people.

15 The cost of cyber crime in the world in 2016 was about $ 450 billion (Graham, 2017).

result of prevention of performance resulted from a motion that harbours to realize or to make threat for the corruption, inclusion or violation against cyber systems including people in cyber space with reference to global infrastructure based on ICTs.

The infrastructure of cyber terrorism necessitates an appropriate structure for its own ontology. This structure comes on the scene as cyber space. Thing that is defines cyber space is network infrastructure. Those such as, network, file server, LAN, WAN, backbone, modem, TCP/IP protocols, internet servers, router, internet, WWW, DNS etc., are elements of network infrastructure.

In the cyber space, cyber terrorism has competence to exploit some vulnerabilities such as malware and grayware to reach its end as well as cyber crime.

Since any state moves her reason of existence into network as ontological and potential threats will be able to be happened in the process of the development of cyber terrorism, it has to be considered that cyber terrorism will try to be superior power as opposed to "e-government".

When the results are evaluated, it can be said that any service of the e-government issue may be the target of cyber terrorism. This service can be seen in a wide range of area and at risk levels, from preventing to access the website of any official institution to opening up dam covers to cause floods, and from sabotaging applications in cyber space to closing power grids. In that sense the scope of the threat of cyber terrorism is large.

At the same time, it is also a logical implication that developed and developing countries, which are predecessors of investments based on ICTs, are the primary targets for cyber terrorism when the effects of ICTs on gross domestic product are considered; because e-government is not a concept that is far from knowledge-based economy and information society. On the contrary, for Terzi (2006, pp. 6-19), there is an organic relationship between them. Knowledge-based economy refers to the economy based on information and communication technologies, whereas information society refers to the post-industrial society built on this technology.

However, an implicit conclusion emerging within the framework of the Actor-Network Theory is the conclusion that cyber terrorism will require the skilful and intelligent, and will become a weapon of those in the elitist

position. This suggests that there is a need for professional staff to combat all cyber threats, especially cyber terrorism, and that institutions must carry anxiety about capacity building. Another consequence is that the Actor-Network Theory, which is concerned with presenting a model for participatory democracy, is not perfect. Especially as a result of techno-determinism, according to Terzi (2006, p. 80), it is one of these flaws that non-human actors (actors), such as software, hardware, protocols and server capacity, have superiority to the citizen in the street.

There is also a difference in talent among individuals in using and gaining control over the tools of ICT. It is likely to say that the more capability the participant has, the more skill it will be in the decision-making process. Over time, the use of Information and Communication Technology tools is likely to result in that those who have high ability can turn into closed groups against those with less ability to use these devices. This means that a new class of experts has begun to be born (Terzi, 2006, p. 81).

At the national level, e-government components need more specialized staff than basic computer users to combat cyber threats. In addition, institutions need to increase their capacity to improve their infrastructures for information and communication technologies. In Turkey, for example, the country needs brand anti virus software company or companies. In this sense, it is important for the state to provide financial support and platform.

It is also one of the solutions to evaluate the approach of "cyber risk insurance" in order to minimize the losses or to make them tolerable in some cases.

When the cost of global crime is taken into consideration in the world, ways of global cooperation in the fight against cyber crime, especially cyber terrorism, should be sought[16]. In addition, there are also important tasks for any individual state to provide cyber border security in her national cyber space.

Studies on how ethical codes can be developed to prevent potential threats of information and communication technologies against humanity, such

16 It should also be noted that one of the elements that make cooperation difficult is that the states perform some kind of Proxy battles against each other through cyber terrorism. In this sense, the struggle against cyber terrorism shares the same negative fate like the struggle with classical terrorism (Terzi, 2018: 107). Striking example is the Stuxnet attack on Iran in 2010. A group of volunteer cyber warlords attacked Iran nuclear plant thanks to Siemens know-how and with the support of the US Department of Defense, and with the logistics of Israel (Ceylan, 2010).

as those in artificial intelligence discussions, should be researched in cooperation with universities. What are these ethical codes? Is it what traditionally known as morality? Or is there a special form of these codes in the world of codes? Or is an eclectic thing which is the synthesis of both? We do not know these yet.

References

Anti-Defamation League. (1998). Terrorist activities on the internet. Retrieved December 18,

2007, from http://www.adl.org/Terror/focus/16_focus_a.asp.

Bardini, T. (1997). Bridging the Gulfs: from hypertext to cyberspace.

The Journal of Computer-Mediated Communication. Retrieved July 02, 2017, from

http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.1997.tb00069.x/full.

Başeren, S. (2006). Uluslararası şiddet ve terörizm ders notları (International violence and terrorism lesson notes). Ankara, Kara Harp Okulu, Savunma Bilimleri Enstitüsü.

BBC Türkçe Haber. (2014, 05 December).Yapay zeka insanlığın sonu olacak korkusu gerçekçimi? (Is it realistic that the fear of artificial intelligence will be the end of mankind?) Retrieved from (21 Ocak 2018): http://www.bbc.com/ turkce/haberler/ 2014/12/141204_yapay_zeka_ insanligin_sonu.

Bertucci, G. (2003). E-government for development. Retrieved April 25, 2004, from

http://usembassy.state.gov/Seoul/wwwh6033.html.

Blaikie, N. (1993). Approaches to social enquiry. Cambridge: Polity Press.

Brenner, S. (2007). At light speed: Attribution and response to cybercrime/ terrorism/

warfare. Journal of Criminal Law and Criminology, 97(2):379-475. Retrieved July 02,

2017, from http://scholarlycommons.law.northwestern.edu/cgi/viewcontent. cgi?article= 7260&context=jclc.

Callon, M. (1983). Society in the making: The study of technology as a tool for

social

analysis. Retrieved July 19, 2017, from http://www.umsl.edu/~rkeel/280/class/callon.html.

Castells, M. (1998). The rise of the network society. Oxford: Blackwell Publishers Inc.

Centre of Excellence Defence Against Terrorism. (2006). Brochure on the countering cyber terrorism course. Ankara, Centre of Excelllence Defence Against Terrorism.

Ceylan, C. (2010). Siber savaşta yeni cephe: Iran-Buşehr nükleer santrali ve SCADA-PLC sistemler (New front in cyber war: Iran-Bushehr nuclear power plant and SCADA-PLC systems). Retrieved September 25, 2017, from http://www.bilgiguvenligi.gov.tr/siber-savunma/siber-savasta-yeni-cephe-iran-busehr-nukleer-santrali-ve-scada-plc-sistemler.html.

Coffman, J. L. (2006). Terrorism around us. Retrieved December 02, 2006, from http://www.usadojo.com/articles/terrorism-around-us.htm.

Commission of the European Communities, (2002). eEurope 2005: An information society for all. Retrieved April 18 , 2004, from http://europa.eu.int/information_society/eeurope/2002/ news_library/documents/eeurope2005/eeurope2005_en.pdf.

Couldry, N. (2008). Actor network theory and media: Do they connect and on what terms? London School of Economics and Political Science. Retrieved August 01, 2017, fromhttp://eprints.lse.ac.uk/52481/1/__Libfile_repository_Content_Couldry%2C%20N_Couldry_Actor_network_theory_2008_Couldry_Actor_network_theory_2008.pdf.

Crenshaw, M. (1981). The causes of terrorism. Retrieved August 01, 2017, fromhttp://courses.kvasaheim.com/hist319a/docs/Crenshaw%201981.PDF.

Dura, C. and Atik, H. (2002). Bilgi toplumu, bilgi ekonomisi ve Türkiye (Information society, information economy and Turkey). İstanbul: Literatür Yayınları.

Elmusharaf, M. M. (2004). Cyber terrorism: The new kind of terrorism. Retrieved July 14, 2017, from http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism.

Frohmann, B. (1995). Taking information policy beyond information science: Applying the actor network theory. Retrieved July 15, 2017, from http://citeseerx.ist.psu.edu/ viewdoc/download?doi=10.1.1.517.5320&rep=rep1&type=pdf.

Garrety, K. (2014). Actor network theory. Retrieved August 02, 2017, from http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1406&context=buspapers.

Goguen, J. (1998). Actor-network theory. Retrieved July 16, 2017, from http://www-cse.ucsd.edu/users/goguen/courses/268D/5.html.

Graham, L. (2017). Cybercrime costs the global economy $450 billion: CEO. Retrieved September 25, 2017, from https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo. html adresinden erişildi.

Hanseth, O. and Monteiro, E. (1998). Understanding information structure. Retrieved July 19, 2017, from http://heim.ifi.uio.no/~oleha/Publications/bok.pdf.

ITU. (2003a). Plan of action. Retrieved April 04, 2004, from http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!MSW-E.doc.

ITU. (2003b). Declaration of principles. Retrieved April 04, 2004, from http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-E.doc.

İnce, N. M. (2001). Elektronik devlet (Electronic government). Retrieved July 19, 2017, from http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Murat_Ince_E-Devlet.pdf.

Koyun, M. (2003). Etkinlik ve etkin devlet anlayışı çerçevesinde e-devlet (E-government in the framework of efficiency and effective government). Unpublished master's thesis, Selçuk Üniversitesi. Ankara: YÖK Tez Merkezi.

Lemke, J. (2001). Activity theory and actant-network theory. Retrieved July 20, 2017, from http://academic.brooklyn.cuny.edu/education/jlemke/theories.htm#AT.

Miettinen, R. (1997). The concept of activity in the analysis of hetereogenuous networks in innovation process. Retrieved June 14, 2017, from http://communication.ucsd.edu/ MCA/Paper/Reijo/Reijo.html#Introduction.

OECD. (2003). The e-government imperative. Retrieved July 16, 2017, from http://www.oecd-ilibrary.org/governance/the-e-government-imperative_9789264101197-en.

Özcivelek, R. (2003). Dünyada ve Türkiye'de elektronik devlet tartışmaları: Kavram üzerine bir sorgulama (Electronic government debates in the world and Turkey: a question on concept). Retrieved July 20, 2017, from https://documents.tips/download/link/duenyada-ve-tuerkiyede-e-devlet.

Posta Gazetesi. (2018, 13 October). Mor Beyin nedir? Nasıl Bylock tuzağına düştüler? (What is the Purple Brain? How did they fall to the Bylock trap?). Retrieved February 20, 2018, from http://www.posta.com.tr/mor-beyin-nedir-nasil-bylock-tuzagina-dustuler-haberi-1366539.

Rhodes, R. A. W. (2000). Governance and public administration. In: Edited by Jon, P. (ed.) Debating Governance: Authority, Steering, and Democracy. Oxford: University of Oxford Press.

Risan, C. L. (1997). Artificial life: A technoscience leaving modernity? Retrieved July 25, 2017, from http://www.anthrobase.com/Txt/R/Risan_L_05.htm.

Rousseau, J. J. (1762/1989) Toplum anlaşması (The social contract). Trans. Vedat G. İstanbul: Milli Eğitim Basımevi.

Scheideler, C. (2004). Network theory. Retrieved July 23, 2017, from http://www.cs.jhu.edu/ ~scheideler/courses/600.348_F04/lecture_2.pdf.

Şenel, H. (2003). İnternetin altyapısı (Infrastructure of internet). In: Cengiz H A, Yaşar H, Ali E Ö (eds) Temel Bilgi Teknolojileri (Basic Information Technologies). Eskişehir: Anadolu Üniversitesi, p. 241-261.

Tatnall, A. (2005). Actor-network theory and information system Research. Retrieved June 24, 2017, from http://www.irma-international.org/viewtitle/14208/.

Terzi, M. (2018). Bilgi ve iletişim teknolojilerine dayalı oluşumlar ile bu oluşumların uluslararası ilişkilere güvenlik bağlamındaki etkisi: Siber terörizm 2016-2019 ulusal siber güvenlik strateji belgesi kapsamında Türkiye incelemesi (The formations based on information and communication technologies and the effects of these formations on the international relations in the context of security: Cyber terrorism the case of turkey in the scope of 2016-2019 national strategy document for cyber security). Kara Harp Okulu Bilim Dergisi, 28(1):73-108.

Terzi, M. (2006). Information-based economy and e-government: Transformation in the public administration (Unpublished master thesis). METU, Ankara.

Trend Micro House Call (2014) Glossary. Retrieved October 04, 2017, from http://about-threats.trendmicro.com/us/glossary/all.

Türkiye Bilişim Şurası. (2002). e- devlet raporu (e-government report) (2002). Ankara: Türkiye Bilişim Vakfı.

United Nations. (2000). United Nations millennium declaration. Retrieved October 02, 2017, from http://www.un.org/millennium/declaration/ares552e.

htm.

United Nations (2002) Report of the international conference on financing for development. Retrieved October 02, 2017, http://www.ipu.org/splz-e/ffd08/monterrey.pdf.

University of Colorado. (2003). What is actor-network theory? Retrieved March 02, 2005, from http://carbon.cudenver.edu/~mryder/itc_data/ant_dff.html.

Uysal, A. (2016). Ulusal yargı ağı projesi-1. Eskişehir: Anadolu Üniversitesi.

Üstüner, Y. (2003). Siyasa oluşturma sürecinde ağ yönetişim kuramı (Network governance theory in the policy making process). Ankara: TODAİE.

Van House, N, (2001), Actor-network theory, knowledge work, and digital Libraries. Retrieved September, 24, 2017, from http://www.sims.berkeley.edu/~vanhouse/bridge.html.

Vera-Zavala, A. (2006). Deltagande demokrati. Trans. Naile A. Ankara: Dipnot Yayınları.

Weber, M. (1973). Bureaucracy. In the Lesson Notes of Public Administration Theories. 2005. Ankara: METU.

Wikipedia Free Encyclopedia. (2009a). Japanese embassy hostage crisis. Retrieved July 03, 2009, fromhttps://en.wikipedia.org/wiki/Japanese_embassy_hostage_crisis.

Wikipedia Free Encyclopedia (2009b) Zapatista army of national liberation. Retrieved July 03, 2009, from https://en.wikipedia.org/wiki/Zapatista_Army_of_National_Liberation.

Wilson, C. (2007). Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. Retrieved September 14, 2017, from http://www.fas.org/sgp/crs/terror/ RL32114.pdf.

Yücetürk, E. E. (2004). Türk kamu yönetiminde e-devlet uygulamaları ve tabana yayılabilme yeteneği bakımından bir değerlendirme: Bolu örneği (An evaluation in terms of e-government applications and the ability to spread in the Turkish public administration: The case of Bolu). Retrieved April 08, 2004, from http://www.bilgiyonetimi.org/cm/pages/mk1gos.php?nt=225.

Özet

Teknoloji, siber terörizm olarak nitelenen yeni bir tür terörizm ortaya çıkarmaktadır. Siber terörizm, geleneksel manada terörizm için sadece bir propaganda aracı değil, aynı zamanda siber alana gömülü bir mantığı da ifade etmektedir. Bununla birlikte siber terörizm, terörizm olgusunda olduğu gibi aynı olumsuzluğu yaşamaktadır; yani terörizm kavramında olduğu gibi siber terörizm kavramında da evrensel olarak konsensüse varılmış bir tanım yoktur ve bu da siber terörizmle mücadeleyi zorlaştırmaktadır.

Siber terörizmin, geleneksel manada terörizm için bir propaganda aracı olması veya internet sayfaları üzerinden bomba yapılmasını öğretmesinden ziyade, onun ontolojik özelliğine dikkat etmek gerekmektedir. Bilgi ve iletişim teknolojileri üzerinden kurgulanan siber terörizm, e-devlet ile aynı alt yapıyı kullanmaktadır. Devletin kimi hizmetlerini internet ortamına taşımasından çok daha fazlasını ifade eden e-devlet, bilgi tabanlı ekonomi ve bilgi toplumundan ayrı düşünülemeyecek bir olgudur ve vizyonunda katılımcı demokrasi de dâhil olmak üzere, kamu yönetiminde bilgi ve iletişim teknolojilerine dayalı bir dönüşümün hedeflenmesi de söz konusudur. Bu çerçevede devletin sunduğu tüm hizmetler ile devletin hizmet alt yapısı ve yatırımları, siber terörizmin hedefi haline gelebilir.

Bununla birlikte, toplumu oluşturan insanların çok geniş bir siyasi yelpazede temsil edilmeleriyle bir çeşit genel iradenin oluşacağını ve böylece zımnen de olsa terörizmin ortadan kalkacağını savunan ve katılımcı demokrasi için bir model sunan Aktör Ağ Kuramı, bu çerçevede incelemeye değerdir.

Aktör Ağ Kuramı, aktör (birey/insan) kavramını, cansız unsurların da (klavye, yazılım vb.) etkileşim sürecine dâhil olduğu aktant kavramı ile ikame ederek, ultra liberal bir model önermektedir. Ancak, söz konusu teoriye daha yakından bakıldığında, bu teorinin sorunsuz olduğunu söylemek mümkün değildir; çünkü tekno-determinizm sonucu, insan olmayan aktörlerin sıradan vatandaşa karşı bir üstünlüğü söz konusudur. Dahası da Aktör Ağ Kuramı çerçevesinde ortaya çıkan sonuçlardan biri, siber terörizmin zeki ve yetenekli kişilere ihtiyaç duyacağıdır. Ayrıca bilgi ve iletişim teknolojileri konusunda daha bilgili ve yetenekli olanların, kapalı gruplara dönüşme olasılığı, Aktör Ağ Kuramının katılımcı demokrasi öngörüsünü de zedelemektedir. Bu kapalı gruplar da aynı zamanda geleceğin teknik elitleri olarak yorumlanabilir.

Ulusal düzeyde, e-devlet bileşenlerinin siber tehditlerle mücadele etmek için temel bilgisayar kullanıcılığından daha fazla uzmanlığa ihtiyacı vardır. Bu doğrultuda kurumların uzman personel ekiplerini oluşturması

gerekmektedir. Türkiye'deki Ulusal Yargı Ağı Projesi (UYAP) buna güzel bir örnektir. Ayrıca kurumların, bilgi ve iletişim teknolojileri savunma altyapılarını iyileştirme kapasitelerini artırmaları gerekmektedir. Mesela Türkiye'de, ülkenin marka anti virüs yazılım şirketi ya da şirketlerine ihtiyacı vardır. Bu anlamda, devletin finansal destek ve platform sağlaması önemlidir. Aynı zamanda, siber saldırı sonrası kayıpları en aza indirmek veya bazı durumlarda bu kayıpları tolere edilebilir hale getirmek için "siber risk sigortası" yaklaşımını değerlendirmeye almak, önerilebilecek çözümler arasındadır.

Dünyada küresel suçun maliyeti göz önüne alındığında, siber suçla mücadelede, özellikle de siber terörle mücadelede küresel işbirliği yolları aranmalıdır. Ayrıca, herhangi bir bireysel devletin, kendi ulusal siber alanında, kendi siber sınır güvenliğini sağlama konusunda da önemli görevleri vardır.

Yapay zekâ tartışmalarında olduğu gibi, insanlığın bilgi ve iletişim teknolojilerinin potansiyel tehditlerini önlemek için etik kodların nasıl geliştirilebileceği üzerine araştırmalar, üniversitelerle işbirliği içinde yapılmalıdır. Bu etik kodlar nelerdir? Geleneksel manada ahlak olarak bilinen şey mi? Yoksa bu kodların kod dünyasında özel bir şekli var mı? Yoksa her ikisinin de sentezi olan eklektik bir şey midir? Bunları henüz bilmiyoruz.