

Mechanisms to Enhance Users' Responsibility on Social Networks' and Preventing Cyber Terrorism

Rasmieh Mohammad Alshogran¹

¹ School of Arts and Languages, Media and Communication Technology Dep., Jadara University, Jordan

Correspondence: Rasmieh Mohammad Alshogran. E-mail: Rasmieh-70@yahoo.com

Received: February 17, 2019

Accepted: March 13, 2019

Online Published: April 30, 2019

doi:10.5539/ass.v15n5p10

URL: <https://doi.org/10.5539/ass.v15n5p10>

Abstract

This research aims to identify the effective mechanisms in enhancing the moral and social responsibility of users of social networks and practical steps to reduce the publications of extremism and terrorism. The research is a descriptive one, which adopts analytical research comparisons of the questionnaire tool distributed to 95 public opinion leaders. The research finds:

1. One of the main causes of cyber terrorism is the lack of self-censorship and the absence of home and school roles in the control of children.
2. One of the most important dangers of cyber terrorism is spreading the extremist ideas, especially among young for exploitation in terrorist operations.
3. One of the most effective mechanisms for enhancing the ethical and social responsibility of users of social networks is carrying the State and the school the responsibility to promote social responsibility to counter the phenomenon of cyber terrorism

Keywords: social responsibility, social networks, cyber terrorism

1. Introduction

A great change occurred in social relation as a result of the huge development in technological communication fields, this change has its own impact in the context of globalization as individuals turn into virtual subjects who react within a virtual world. The social networking sites have become important institutions that play an important role in influencing social values and building individuals culture, imparting different habits and behaviors, it is therefore an important tool of social change.

In this context, and as a result of the social networking sites and networks impact, the importance of social responsibility has emerged as a very important issue because it is linked directly to human life. And this responsibility has positive and negative actions and practices within the society. In the development of social responsibility, through the establishment of youth groups to create pages on social interacting sites on these sites adopt a social issue at the center of their concerns and work to publish and defend them using the communication skills, advocacy, and social pressure.

In this study, the researcher seeks to identify the importance of social responsibility of social media users and the impact of these sites and networks, the mechanisms of combating cyber terrorism practiced by a number of extremism and terrorist people in targeting community values in unity, coexistence and peace.

1.1 Study Problem

Communication and information revolution in the twenty-first century has caused great effects in the public reception system, in its philosophy roles, and thus in its methods and means. Therefore, media and communication systems resorted to renewal, characterization of its elements in a continuous changing era, so the social networks impacts have exceeded the political and economic effects into social life and standards of coexistence and peace in all societies in general.

The space provided by social networks for users have made it a rich field for terrorists in targeting the unity of the society through their posts in various social media to break up the social structure which has dangerous effects on human life.

The study problem lies in the importance of identifying the most important threats of cyber terrorism for the individual and society, the effective mechanisms to enhance the moral and social responsibility of social networks users, and the most practical ways to reduce extremism and terrorism publications in different social media sites.

Study questions:

- What causes the spread of cyber terrorism?
- What are the risks of cyber terrorism to the individual and society?
- What are the effective mechanisms for enhancing the ethical and social responsibility of social networks users?

1.2 The Importance of the Study

The importance of this research is to identify some aspects and important points in social networking sites and their relation to social responsibility, as well as to identify the impact of social networks in the process of community communication as a means of communication characterized by technical and editorial characteristics that influence the determination of receiving patterns.

1.3 Study Objectives

The research aims to:

- Reasons of cyber terrorism spreading.
- Dangers of cyber terrorism on the individual and society.
- Effective mechanisms to promote the ethical and social responsibility of social networks users.

1.4 Procedural Concepts

- Social responsibility: "It is responsible for behavior or acts and determines the extent to which it approves specific requirements (Othman, 1996). (Dhiab, 2010) stated that; the content of social responsibility is embodied in four aspects: economic, legal, moral and good.
- Social networking: A system of networks that allows the subscriber to create a site of his own, and then connect it through a social system with other members who have the same interests and hobbies or gathering the individual with friends of the university or secondary school (Radi, 2003, p. 23)
- Cyber terrorism: Cyber terrorism can be defined as the use of cyber techniques to intimidate and subjugate others, or to attack information systems on political, racial or religious grounds. In October 2012, the United Nations identified cyber terrorism as "the use of the Internet to spread terrorist acts".

2. Theoretical Background

2.1 Uses and Gratification Theory

Uses and Gratification theory is the basis of this research, this theory explains why people communicate with the media and their needs to use it, such as entertainment, learning, social interaction and other common reasons. The theory focuses on the motives and needs, as the sense of human psychologically and socially deficient and when he gets it, he feels satisfied and happy, and to the motive as an internal stimulant or psychological or internal physiological condition that prompts the person to a certain behavior which strengthens his response to some stimuli... meets his need.

This theory is based on the fact that the public is active and effective and choose what they need in different ways. Therefore, social networks represent an effective space for meeting the needs of the public and satisfying them, while the public takes decisions in the process of exposure and understanding at three levels of selection; in the sense that the choices of the public are not random, the public choose the means, content and knowledge, the awareness of self-recognition and benefits and preoccupation as the individual recognizes a link between him and the media's content so he interacts with it.

Thus, this theory represents a theoretical basis for the research through the social networks that the user allows to make it a field for the various races which lead to be exploited by terrorists in targeting the unity of society in various media to break up the social structure.

2.2 Social Responsibility Theory

The theory social responsibility, in the field of journalism and media, is defined as: "The set of functions that the press must perform in front of society in its various political, economic, social and cultural fields, so that its

materials subjects have professional values such as accuracy, objectivity, balance and inclusiveness, provided that the press must have real freedom to make it accountable to law and society." (Hussam al-Din, 2003, p. 17).

Social responsibility theory in the media promotes the concept of media freedom, but this freedom is not absolute. "The basic idea of the theory is that freedom has responsibilities and obligations, and that the media as privileged in a democratic society is obliged to be accountable to society for certain functions" (Sadiq, 1989, p. 22). In the light of this, an American professor, Curtis Montgery, in his book "The Responsibility to Raise Standards," presented a new vision of responsibility, which states that if the media informs people and maintains their privacy and respect for their values, this is half the responsibility, but the other half is the statement of the public's responsibility towards the broadcast material and towards themselves (Hussam al-Din, 2003, p. 18), (Beshbishi, 2005, p. 83). With regard to the theory's relationship with the research, social networks must accept and fulfill certain obligations towards society by adhering to professional standards in transmitting information such as truth, accuracy, objectivity and balance, avoiding the dissemination of what can lead to crime, violence and social chaos, reflect the diversity of opinions and commit to the right of reply, that society has a right on press, and that government intervention can be a justified for the public interest (McVilley, 2005, p. 117).

3. Previous Studies

Awad Study (2012). The aim of the study was to examine the impact of social networking sites in the social responsibility development among young people through the implementation of a training program for a group of Allar Youth Council. In order to achieve the objectives of the study, the researcher applied a training program on a training group members, which was deliberately chosen from (18) young man and woman from Allar youth council, and then applied the social responsibility measure on them (the pretest measurement), which was developed by the researcher. The program content may be from the main objective and a number of behavioral goals that emerged from it, the program consists of (5) meetings which were carried out during five days at a rate of (4) hours per meeting, the researcher set several goals for each meeting, and defined the mechanism of implementation and procedures, and the researcher used the different techniques and training methods including acquaintance, clarification, formation of groups, practical training, questioning and inquiry, termination and evaluation, lecture and group discussion and games revitalization. The results showed that there were statistically significant differences between the mean scores of the experimental group at the level of significance $0.05 \leq \alpha$ (at the level of social responsibility before and after the application of the program in favor of the application of the training program. The results also found no significant differences at the level of significance $0.05 \leq \alpha$ (between the average scores of the experimental group members at the social responsibility level after program application and in view of the findings of the study. Orabi, and Aqabawi study (2012), This study sought to measure the credibility of what is presented in the social media sites from news, pictures or movies from media sources or individual's non-news sources to young people by monitoring the type of content experienced by the public in Saudi society in the social sites and their dependence on what presented on them in different fields such as (Social, cultural and economic fields) and compare between them, The study aimed to identify the awareness of the Saudi public about the concept of news content credibility and its components through a field study on users of social networking sites sample of Saudi society. The problem of study is summarized in the following main question: How credible is the social networking sites content for Saudi youth? The study based on a survey methodology of a random sample consisted of 200 young people of both sexes between the ages of (18-35), Using a survey paper to meet the objectives of the study and its mandates which included several axes to identify the social networking sites content credibility. The study showed that the sites of the social network newspapers are the most reliable in the information presentation among young people by 47% followed by Twitter and Facebook at an equal rate of 23%, while Facebook came in the last ranking by 7%. The results also indicated the totalitarianism of the newspapers websites which came in the first rank among the youth by 5.32% followed by Twitter by 25%, then Facebook by 22% and finally by YouTube by 5.20%.

Light McGrath study (2010). The aim of the study was to show the most important ethical values that are reflected through Facebook. The study was based on the qualitative approach through participatory observation. The study was conducted over two years. The study showed a great number of ethical challenges surrounding Facebook users and that communication technology has created many ethical issues related to the nature of this technology, including confidentiality, privacy, identity disclosure and the possibility of defamation and abuse of others. The study also confirmed that the ethical values of technology users can not be a sufficient or convincing framework for the development of uniformed standards that everyone can abide by in their use of Facebook as a result of differences, contradictions and even conflicts with their interests.

3.1 Theoretical Framework

Since the emergence of social networks in the beginning of the 20th century, a debate began about social phenomena, psychological, political and economic series of transformations as a result of individual collective and institutional practices in the effective use of communication technology in the information and knowledge themes. Several issues were raised for discussion such as information control, the size and speed of information transmission and dissemination. Sociologists, anthropologists and researchers in the field of ethics and media have begun to call for vigilance and warning of these networks and the effects they can have on the individual, their relations with the institutions they belong to, especially with the different political, economic and social conditions of their respective countries. Warns of the phenomenon of "technophobia" expressing the fear of new communication technology, especially social networks and the accompanying psychological and moral frustration (Eid & Ward, 2009, pp. 1-4) and Michel, Cheryl & Kimberly, 2005, pp. 9-18).

3.2 The Social Networks Concept

Social networking sites definitions differ from one researcher to another as (Palse, 2009) define it as a program used to build online communities that individuals can communicate with each other. Bryce and Maloney Krishmar (2009) define social networking sites as "a place where people meet for specific goals, and are also known as: "new ways of communicating in the cyber environment that allow smaller groups to meet and gather on the Internet and share benefits and information, it allows individuals, groups and communities to make their voices heard to the world. It is also defined as: communication channels that create an interactive, open social structure capable of innovation without compromising the structure of this environment (Kittiwongvivat & Rakkannan, 2010, p. 20). In France, researchers preferred using the term "réseaux les numériques-socio", which reflects the assertion of researchers on the one hand that these platforms are not social networks as we find in real life, because the Facebook user network does not always coincide with his network of social relations life which is not virtual. On the other hand, these platforms are not purely cyber, nor purely social because their applications are subject to individual and collective acquisitions (Stenger T et Coutant A, 2011).

Social networks include Facebook, Twitter, Instagram, Snapchat, YouTube, Whatsapp, Cyber, Imo, LinkedIn, Google Plus and other applications from social networks that have attracted people around the world, It is used by people on a daily basis to communicate with each other. It allows them to use text, images, animations, links and other communication technologies available in every application or network.

3.3 Features of Social Networks

Social networking sites allowed users to share files and images, share videos, messages, and have instant conversations. In recent years, social networks have witnessed a qualitative development that has brought about a kind of social interaction between people in virtual cyberspace, people became close to others and it demarcate borders between countries, the inter-cultural relationship, the multiplicity of networks and the presence of a wide audience. The political and natural events in the world played a role in introducing these networks. In return, these networks have also been credited with delivering what satisfies the audience (Rady, 2012).

3.4 Cyber Terrorism

Terrorism is a word derived from the act of "terror" which represent a fearful sense and the word terrorism is the source of the act of terrorization and intimidation in the sense of fear (Sayyad, 2002, p. 14). The political lexicon defines it as an attempt to spread panic for political purposes, a means used by an authoritarian or dictatorial government to compel and force the people to surrender to it rule (Zeitoun, 2006, p. 21). The political encyclopedia defines terrorism: "The use of unlawful violence, or the threat thereof, in various forms, such as assassination, mutilation, torture, vandalism in order to achieve a specific political goal, such as breaking the spirit of resistance and commitment in individuals and demoralizing institutions, or as a means of obtaining information or money. And generally the use of coercion to subjugate a party hostile to the will of the terrorist (Kayali, 1994, p. 153).

James Lewiss defined cyber terrorism as: "Using computer network tools to destroy or disrupt important national infrastructures such as: Energy and transport, or to intimidate the government and civilians." Dorothy Denning sees e-terrorism as a " computer-based attack that threatens to intimidate or force governments or communities to achieve political, religious, or ideological goals. The attack should be destructive to generate fear. Thus, "cyber terrorism" is defined as: "the aggression, intimidation, physical or moral threat emanating from States, groups or individuals against a person, in his or her religion, self, presentation, mind or property unlawfully using information resources and electronic means, in various forms of aggression and images of corruption" (Desforges, 2011) and (Denning, 2000, p. 1) and (Attia, 2014, p. 9).

It should be noted that terrorism and the Internet are linked in two ways: The first is the sabotage of computer and Internet networks, Second, the Internet has become a platform for groups and individuals to spread messages of hatred and violence, to communicate with each other, their supporters and sympathizers. With the increasing use of social networks for their various fields, terrorist groups have exploited the circumstances and begun to spread a culture of religious extremism among young people and to blur their identity and attract them to terrorist organizations, thus threatening social security. Electronic terrorism has become an obsession that scares the world, which is vulnerable to attacks by terrorists on the Internet who engage in subversive activity from anywhere in the world. These risks are exacerbated every day, because modern technology alone cannot protect people from electronic terrorist attacks which try to damage individuals, Organizations and States.

3.5 Factors for Spreading Cyber Terrorism (Osman, 2016)

1. The weakness of the information networks structure and their privacy and being hacked easily because the information networks are originally designed without restrictions or security barriers to expand and facilitate the users entry. Electronic systems and information networks contain information gaps; terrorist organizations can exploit these vulnerabilities to infiltrate Infrastructure, and the practice of subversive and terrorist acts.
2. The absence of self-censorship through education, the specificity of community culture, and the abolition of geographical boundaries leading to low level of risk, a computer professional can present himself with the identity and character that he wishes, or disguises under a fictional character, and calls himself titles or aliases, supporting that with tangible physical evidence such as pictures, or some correct information to prove his seriousness, and then after a while he can launch his cyber-attack resting in his home without a direct risk.
3. Ease of technical use and low cost. Social media, and all the electronic means of communication are low cost and available in all countries of the world, unlike the eighties of the last century, for example. The global feature of the information networks is that it is an easy-to-use, cost-effective, time-consuming and effortless solution that provides terrorists with a valuable opportunity to reach their illegal targets without the need for large funding sources, they require no more than one computer connected to the network and equipped with the necessary software.
4. The difficulty of detecting and proving cybercrime is that technology can identify the perpetrator of an electronic crime only through certain devices owned by some security institutions, but individuals cannot identify it.
5. The absence of the home and school roles in children and young people supervision, making them to use this technology in a bad way. Reasons that led to the emergence of terrorism in general and electronic especially: Extremism in some religion matters. Some young people who use technology believe that they know more than others, and that some scientists are misguided, so their views must be fought through this technology.

3.6 Cyber Terrorism Ways

Terrorist groups use sophisticated technology to disseminate their principles and perceptions and carry out various acts of sabotage through the Internet networks to reach their desired goals through the following (Ajlan, 2008, p. 19):

- Communication: Terrorist groups use the Internet to communicate among themselves and finance their operations from different areas, hundreds of kilometers away from the area of the terrorist operation, because of its speed and low cost compared to other means, in addition to the information abundance, where the Internet is an electronic encyclopedia which is rich in sensitive information that terrorists seek to obtain, such as nuclear installations, power generation, command and control facilities, international flight schedules, counterterrorism information, and other information that is a precious treasure for terrorists.
- Dissemination of extremist ideas: Terrorist groups propagate extremism through social networking sites and chat rooms with various segments of society, especially young people, to exploit them in terrorist operations, in addition to the existence of several terrorist sites, for example, there is a report revealed that the terrorist organization of ISIS has 90 thousand pages in Arabic on Facebook and 40 thousand in other languages, in addition to its site launched by the organization in seven languages to extort young people and their inclusion in the ranks of about 3400 young joined ISIS through electronic organization campaigns. According to the Association of the prospects of internal security of Tunisia that the websites of extremist and terrorist orientation attracts about a thousand young people a year, which is equivalent to 3 young men

a day, a high figure reflects the seriousness of the phenomenon, which is increasing, accounting for about 40% of the young students between the ages of 17 and 28 who study the d medicine, physics and chemistry where these groups invest their scientific skills for subversive purposes (Shawqi, 2015).

- Planning and coordination: Terrorist groups use the Internet to plan, coordinate, and manage terrorist attacks. In 2001, the September 11 attacks were extensively planned through regular e-mails and chat rooms to determine the tasks of each subject. It has also succeeded in planning and coordinating its major terrorist operations in Europe, particularly in France and Belgium, through information networks and social networking sites that cannot be monitored or erased after reading them directly through video games connected to the Internet. These attacks have killed about 200 people In November 2015. The European intelligence services failed to monitor the operations before they took place, but discovered the identities of those who executed them through their mobile phones and their mutual calls with the organization's members (Hussein, 2017).
- Electronic indoctrination: Terrorist groups, through electronic means, offer guidance and methods for making hand grenades, lethal chemical weapons, and methods of improvised explosive devices.
- E-finance: Terrorist groups receive electronic funding by exploiting compassionate hearts to pay financial contributions to legal persons representing the frontline of these terrorists, in a cunning way that the donor does not suspect of helping terrorist groups.

3.7 Effects of Cyber Terrorism

Social networks of different types allow people to communicate easily; this communication has negative aspects of ethics and values, and the most prominent of these influences (Awad, 2012) are:

1. The sense of communication.
2. Deterioration of family communication.
3. Neglect of family duties.
4. Addiction
5. Cyber-bullying
6. Lower productivity and creativity.
7. The contradiction in personality between online and offline
8. Privacy
9. Internet crimes
10. impatience and Quick Syndrome
11. Depression

Cyber terrorism has become a more dangerous activity. The daily use of social networks by terrorist organizations to organize and coordinate their scattered operations around the world. The task of these groups is to recruit young people through the implantation and recruitment of e-culture, Young people are usually the victims of this work.

The acts of terrorism are aggression against self and money, and intimidate the safe, and even aggression on religion, where terrorists portray that religion pleases blood and money. They reject dialogue, these acts portray Muslims as bloody and pose a threat to international peace and security, cultural values and human rights, and this leads to damage and harms reflected on the interests of the nation and detrimental relations with other countries economically, politically, militarily and socially with other peoples.

3.8 Social Responsibility in the Face of Cyber Terrorism

This is the basis for the theoretical approach of social responsibility, especially in business organizations and its reflection on the economic and social situation, which emphasizes that organizations and institutions should not be judged by their level of commitment to the requirements of social responsibility. The promotion of social responsibility to confront the phenomenon of cyber terrorism is the responsibility of all community institutions, which is both ethical and social responsibility at the individual and community levels. Renounce violence and inculcate the values of peace. This requires well-planned cultural, intellectual and informational plans and programs that take into consideration the needs, wishes and tendencies of the recipient and seek to change in mindset, ideas and behavior in the long term level. Here is the need to know the theoretical themes and the intellectual background on which social responsibility is based.

On the other hand, the existence of "media education" within the curriculum contributes to the immunization of society members against cyber terrorism and enables user of social networks to gain the skill of analysis and scrutiny and the dismantling of media messages, and therefore be careful of messages and requests of extremism and terrorism.

3.9 Anti-Terrorism Mechanisms

(Rustom, 2000, pp. 48-49) and (Shafiq, 2015, p. 108) indicate that:

1. Secure user accounts and identity verification systems
2. Holding training courses on combating cybercrime with the participation of international specialists to limit the spread of this type of crime locally, especially since the world suffers from its widespread after it has developed remarkably in terms of what kind of crimes, their perpetrators, their types and means of combating them, as well as the laws and regulations to limit limiting their spreading.
3. Updating of criminal regulations and procedures, including measures to ensure that sanctions on investigative authorities are adequate and evidence accepted.
4. Appropriate measures to resolve jurisdictional problems raised by trans boundary or transnational crimes.
5. International agreements involving the regulation of cross-border direct inspection and control procedures for related information systems and other forms of mutual assistance and ensuring the protection of individual and State rights at the same time.
6. Blocking malicious websites that call for corruption and evil, including those that call for and teach terrorism, aggression and abuse of others which the rightful and useful methods to combat cyber terrorism.
7. To issue a set of laws, regulations, instructions and resolutions to confront cyber-attacks and electronic terrorism, in addition to holding training courses on combating computer crimes with the participation of international specialists.
8. Keeping pace with the huge development of information technology, which has enacted systems to control electronic transactions, and included those penalties for violators in electronic transactions and the fight against cyber terrorism.
9. Refrain from accessing or attempting to access any computer systems connected to the Internet, or to any special information or sources of information without the consent of the owners, or those who have ownership rights to such systems, information or sources.
10. Refrain from sending or receiving encrypted information without obtaining the necessary licenses from the concerned network administration.

4. Study Methodology and Procedures

4.1 Study Methodology

The researcher used an analytical descriptive approach based on theories and theoretical literature, comparisons and analysis of the study findings.

4.2 The Study Sample

The study was based on a simple random sample that reflects the nature of the society (opinion leaders) in the city of Amman. The sample of the study was (95) person. The study adopted a questionnaire tool. (100) questionnaire were distributed on the sample of the study. The researcher obtained (95) questionnaire valid for the study, and was excluded (5) questionnaires were the answers invalid, and returned empty. (95) questionnaire processed statistically.

Table 1. The demographic characteristics of the sample

Sex	frequency	Average	Job	frequency	Average
Male	54	56.8	education	33	34.7
Female	41	43.2	Police	26	27.4
Total	95	100.0	Media	36	37.9
Age	frequency	Average	Total	frequency	Average
22-32	15	15.8	Years of experience	95	100.0
33-43	35	36.8	Less than 1 year	17	17.9
44-54	31	32.6	1-5 years	38	40.0
Above 55	14	14.7	6-10 years	23	24.2
Total	95	100.0	More than 10 years	17	17.9
Academic degree	Frequency	Average	Total	frequency	Average
BA	56	58.9	Total	95	100.0
Master degree	15	15.8			
Ph.D.	24	25.3			
Total	95	100.0			

4.3 Study Tool

To achieve the objectives of the study, the researcher constructed a questionnaire consisting of (35) paragraphs. Its themes were as follows:

The first dimension: the causes of the spread of cyber terrorism

The second dimension: Dangers of cyber terrorism on the individual and society

The third dimension: Effective mechanisms to enhance the moral and social responsibility social networks users.

4.4 Tool Credibility

The credibility of the study tool was tested by presenting it to the specialized and experienced people of university professors specialized in journalism, media, scientific research methods, and some experts in the field of journalism. After receiving the observations, the investigative paper was modified to become practical.

4.5 Reliability of the Measuring Instrument

To calculate the Reliability of the study instrument, the researcher used the method of comparing internal consistency using the Cronbach Alpha Test. The values of Kronbach Alpha for all the variables of the study and for the questionnaire in general were 88%, which is higher than 60%. Stability values ranged from (0.86-0.91) and Table 2 illustrates this.

Table 2. The reliability of the questioner themes

Arithmetic mean	theme	Alpha reliability
1	causes of the spread of cyber terrorism	0.86
2	dangers of cyber terrorism on individuals and society	0.91
3	Mechanisms to promote the ethical and social responsibility of users of social networks	0.88
	General average	0.88

The above table shows that the degree of stability of the tool according to the Kronbach Alpha scale is 0.88, which is high in human and social researches. It indicates the validity of all the dimension of the study to reach the desired results.

4.6 Statistical Analysis

After the questionnaire was verified, (SPSS) was adopted to analyze the data obtained from the questionnaire. The results of the descriptive statistical analysis of the data, which include the arithmetical averages and standard deviations of all independent study themes and the constituent parts of each dimension, were taken into account. The Lycert scale used in the study was as follows:

I totally agree	Agree	I agree a little bit	I don't agree	I don't agree at all
1	2	3	4	5

Based on the above, the values of the arithmetic averages of the study will be treated as follows: (3.68 - above: high), (2.34-3.67: average), (2.33 - below: low). According to the following equation:

The upper value - the minimum value of the alternatives answer divided by the number of levels, i.e:

This value is equal to the length of the class.

$$\frac{(5-1)}{3} = \frac{4}{3} = 1.33 \text{ and This value is equal to the length of the class.}$$

Thus the low level of $1 + 1.33 = 2.33$, the average level of $2.34 + 1.33 = 3.67$, and the high level of $3.68 - 5$

5. Results of the First Theme: The Causes of the Spread of Cyber Terrorism

To obtain the results of the sample responses obtained from this theme, the statistical averages and standard deviations of the sample responses were extracted as shown in Table 3:

Table 3. The arithmetical averages of the sample responses on the causes of the spread of cyber terrorism are arranged in descending order

Arithmetic mean	Paragraph	Arithmetic mean	standard deviation	Rank	Agreement degree
2	Lack of self-censorship through education, and the specificity of community culture.	4.41	.900	.900	High
8	Absence of national dialogue on fundamental and fateful issues	4.24	.780	2	High
6	Absence of home and school role in supervising of children and young people	4.12	.890	3	High
1	The weakness of the information network structure and its privacy and being hacked easily	3.60	.890	4	Medium
4	The difficulty of detecting and proving cybercrime	3.54	.780	5	Medium
11	Political and religious conflicts	3.50	.910	6	Medium
10	surrounding security events	3.42	0.95	7	Medium
7	Lack of public participation in political events	3.41	0.99	8	Medium
9	unemployment	3.34	0.93	9	Medium
3	Ease of technical use and low cost	2.86	0.91	10	Medium
12	External interventions	2.77	1.03	11	Medium
5	The weak regulations and the absence and the of control on information networks	2.23	1.44	12	Low
	General arithmetic mean	3.45	0.95		Medium

Table 3 shows that the general arithmetic average of the axis [causes of the spread of cyber terrorism] is (3.45) and is within the intermediate level.

Paragraph (2), which stated that one of the reasons for the spread of cyber terrorism is the absence of self-censorship through education and the specificity of the community culture, has an average of 4.41 and a standard deviation of (0.90), It is within the high level. Followed by paragraph (8), which stated that one of the

reasons for the spread of cyber terrorism is the absence of national dialogue on fundamental and fateful issues, on a mean of (4.24) and a standard deviation of (0.78), it is also within the high level. paragraph (6), which stated that one of the reasons for the spread of cyber terrorism is the absence of the house and school role in monitoring children and young people, on a mean of (4.12) and a standard deviation of (0.89), It is also of a high level.

Paragraph (12), which states that one of the reasons for the spread of cyber terrorism is (external interference), on the mean of (2.77) and the deviation standard of (1.03) in the low level.

Finally, paragraph (5) stated that one of the reasons for the spread of cyber terrorism is the regulatory and legal absence and the absence of the control on information networks. It is based on an average of (2.23) and a standard deviation of (1.44) which is also low.

It is concluded from the results of this theme that one of the most important causes of cyber terrorism is the lack of self-censorship through education, the specificity of community culture, the absence of national dialogue on fundamental and fateful issues, and the absence of the home and school role in monitoring children and young people.

6. Results of the Second Theme: The Dangers of Cyber Terrorism on the Individual and Society

To obtain the results of the sample responses obtained from this theme, the mean and standard deviations of the sample responses were extracted as shown in Table 4.

Table 4. The arithmetical averages of the sample responses on the cyber terrorist risks theme on the individual and society are arranged in descending order

Arithmetic mean	Paragraph	Arithmetic mean	standard deviation	Rank	Agreement degree
3	Terrorist groups spread extremist ideas through social networking and chat rooms with various segments of the society, especially young people, to exploit them in terrorist operations	4.45	.990	1	High
8	Isolating the individual from his society and causing depression and neurological, psychological and organic diseases to be an easy prey for terrorist groups.	4.42	.880	2	High
4	Exploitation of terrorist groups of social communication in planning and coordination of terrorist attacks	4.11	.870	3	High
1	terrorist Exploitation of networks to finance their operations	3.43	.890	4	High
4	The difficulty of detecting and proving cybercrime	3.54	.780	5	Medium
11	Political and religious conflicts	3.50	.910	6	Medium
10	surrounding security events	3.42	0.95	7	Medium
7	Lack of public participation in political events	3.41	0.99	8	Medium
9	unemployment	3.34	0.93	9	Medium
3	Ease of technical use and low cost	2.86	0.91	10	Medium
12	External interventions	2.77	1.03	11	Medium
5	The weak regulations and the absence and the of control on information networks	2.23	1.44	12	Low
	General arithmetic mean	3.45	0.95		Medium

Results of the third theme: Effective mechanisms in promoting the moral and social responsibility of social networks users:

In order to obtain the responses results the research sample for this theme, the arithmetic mean and the standard deviations of the sample responses were extracted as shown in Table 5:

Table 5. The mathematical averages of the sample responses on the of the active mechanisms in enhancing the moral and social responsibility of users of social networks theme are arranged in descending order

Arithmetic mean	Paragraph	Arithmetic mean	standard deviation	Rank	Agreement degree
8	The school is responsible to promote social responsibility to counter the phenomenon of cyber terrorism	4.47	.990	1	High
14	State should support holding forums, constructive dialogue boards and entertainment centers	4.42	.880	2	High
7	To establish «Media Education» course within the curriculum, contributes in immunizing society members against cyber terrorism.	4.11	.870	3	High
5	The role of media institutions in educating users of social networks on the need for mutual respect between cultures and peoples	4.21	.890	4	High
6	The role of media institutions in educating users of social networks on the need to distinguish between personal freedom and national responsibilities.	3.74	.780	5	high
2	To sensitize families to promote social responsibility among its citizens to confront cyber terrorism phenomenon	3.68	.910	6	Medium
3	worship places to develop and implement well-planned cultural, intellectual and information plans and programs to warn against and respond to electronic terrorism, to renounce violence and inculcate the values of peace.	3.54	0.95	7	Medium
15	State support investment projects and employment opportunities for young people	3.46	1.08	8	Medium
9	Promoting a culture of non-circulation of negative rumors	3.41	.780	9	Medium
10	Ease of technical use and low cost	2.86	0.91	10	Medium
4	External interventions	2.77	1.03	11	Medium
11	Security settings in respect of information received or issued via the internet that are incompatible with religion and law.	3.35	.910	10	Medium
4	Media organizations should be aware of the need not to publish news without verifying its authenticity and the credibility of its sources	3.32	0.95	11	Medium
11	Holding training courses on combating computer crimes with the participation of international specialists	3.31	1.08	12	Medium
13	Developing security capabilities services to deal with and prevent computer crimes	2.30	0.95	13	low
12	Block harmful websites that call for corruption, terrorism and aggression.	2.19	1.08	14	low
1	Secure user accounts and identity verification systems	2.11	1.09	15	low
	General arithmetic mean	3.44	0.94		Medium

Table 3 shows that the general arithmetic mean of the [effective mechanisms for enhancing the ethical and social responsibility of social networks users] which is 3.44 at the intermediate level.

Paragraph (8), which states that one of the effective mechanisms to enhance the moral and social responsibility of social networks users is the school's responsibility to promote social responsibility to counter the phenomenon of cyber terrorism. It has an average of 4.47 and a standard deviation of 0.99. The level is high. Followed by paragraph (14), which states that one of the effective mechanisms for enhancing the moral and social responsibility of social networks users is the state support on holding forums, constructive dialogue boards and

entertainment centers, on an average of 4.42 and a standard deviation of 0.88, it is also a high level. Paragraph (7), which stated that one of the effective mechanisms to enhance the moral and social responsibility of social networks users is to create a "media education" course within the school curriculum which will contribute to immunizing members of the society against cyber terrorism with an average (4.30) and standard deviation of (0.65) in the high level also. Paragraph (12) ranked in the penultimate which states that one of the effective mechanisms to enhance the moral and social responsibility of social networks users is the (blocking of harmful sites that call for corruption, terrorism and aggression) with a mean of (2.19) and a standard deviation (1.08) and located in the intermediate level. Finally, paragraph (1) stated that one of the effective mechanisms in enhancing the moral and social responsibility of social networks users is (securing user accounts and identity verification systems), on an arithmetic average of (2.11) and standard deviation (1.09) it is also from the intermediate level.

It is concluded from the this theme results that one of the effective mechanisms in enhancing the moral and social responsibility of social networks users is the school responsibility in promoting social responsibility to confront cyber terrorism followed by the state support in holding forums and constructive dialogue boards and entertainment centers contributes to society members immunization against cyber terrorism.

7. Conclusions and Recommendations

1. One of the most important causes of cyber terrorism is the lack of self-censorship through education, the specificity of community culture, the absence of national dialogue on fundamental and fateful issues, and the absence of home and school roles in monitoring children and young people.
2. One of the most important dangers of cyber terrorism is the spread of terrorist groups extremist ideas through social networking and chat rooms with various segments of society, especially young people for exploitation in terrorist operations, isolate individual e from society and causing depression and neurological, psychological and organic diseases to be an easy victim for the terrorist groups.
3. One of the most effective mechanisms in enhancing the moral and social responsibility of social networks users is the school responsibility to promote social understanding and responsibility in confronting cyber terrorism. State support to hold forums and constructive dialogue boards and entertainment centers, and to create a "education media" course about electronic terrorism.

8. Recommendations

1. Preaching establishments and educational institutions work to look after the family to follow up their children and to establish awareness workshops so as to make them aware of the danger of cyber terrorism and its effects.
2. State support to establish cultural, sports and artistic centers to attract young people and invest their energies for the benefit of their country.
3. The Ministries of Education should develop a curriculum on media education to immunize students and society from the dangers of cyber and media terrorism.

References

- Ajlan, A. bin A. bin F. (2008, June). *Cyber terrorism in the information age*. Research presented to the First International Conference on Protection of Information Security and Privacy in Internet Law, Cairo.
- Al Aishi, W. (2006). *Combating Terrorism between Politics and Law*. (Algeria: Dar Al Khaldounia for Publishing and Distribution)
- Al-Qasim, M., Al-Zahrani, R., Alsind, A., & Al-Amri, A. (2003). *Study of the experiences of countries in the field of informatics in the draft national plan for information technology*.
- Al-Sakarna, B. K. (2009). *Work ethics* (1st ed.). Oman: Dar Al Masirah for publication and distribution.
- Al-Sayyad, A. A. (2002). *Terrorism and Globalization Version 1 (Riyadh: Center for Academic Studies and Research, Naif Arab University for Security Sciences)*.
- Attia, A. M. (2014). *The Role of Modern Mechanisms to Reduce and Detect New Crimes*. Lecture delivered at an international forum entitled Crimes that have been created in the light of regional and international changes and changes (p. 9).
- Awad, H. (2012). The impact of social networking sites on the development of social responsibility among youth groups, the experience of the Allar Youth Council as a Model, the Social and Family Development Program, Al Quds Open University. *172 Arab European Journal of Media and Communication Sciences*, Special Issue.

- Ben Daddoush, I. *Social networks are building a virtual struggle*. Arab - European Conference.
- Beshbishi, A. T. (2005). *Mass Communication and Contemporary Society*. Cairo: Dar Al Ma'arefah.
- Denning, D. E. (2000). *Cyber terrorism* (Global Dialogue, Autumn, p. 1).
- Desforges, A. (2011). *Cyberterrorisme: Quel perimeter*. Fiche de l'Irsem n° 11, décembre, p.3.
- Dhiab, Y. (2010). *A Guide to Community Responsibility*. Al Quds Open University Publications.
- Doaa, S., & Abdou, Z. Z. (2013). The Egyptian revolution and post socio economic impact. *Journal of Topics in Middle Eastern and African Economies*, 15(1).
- Eid, M., & Ward, S. J. A. (2009). Ethics, New Media, and Social Networks. *Global Media Journal (Canadian Edition)*, 2(1), 1-4.
- Hossam El-Din, M. (2003). *Press Social Responsibility (Version 1)*. Cairo: Egyptian Printing House.
- Hussein, A. (2017). *Cyber terrorism is the most dangerous battles of space wars*. From: Posted on 13-02-2018 at 12:14 pm <http://alwatan.com/details/166324> Date Published: 14/01/2017
- Kafi, M. Y. et al. (2015). *Media and cyber terrorism (Version I)*. (Jordan: Al Issar House for Scientific Publishing and Distribution.
- Kayali, A. W. (1994). *Political Encyclopedia (Part 7)*. (Beirut: Arab Foundation for Studies and Publishing).
- Kittiwongvivat, W., & Rakkannan, P. (2010). *Facebooking your dream* (Master Thesis).
- Light, B., & McGrath, K. (2010). Ethics and social networking sites: A disclosive analysis of Facebook. *Information Technology & People*, 23(4), 290-311. <https://doi.org/10.1108/09593841011087770>
- McVile, T. (2005). *International Media: Theories, Trends, and Ownership*. Translated by Hosny Mohamed Nasr and Abdullah Al Kindi, Al Ain: University Book House.
- Michel, L. Y., Cheryl, A., & Kimberly, J. M. (2005). Depressive symptomatology, youth internet use, and online interactions: A national survey. *Journal of Adolescent Health*, (36), 9-18. <https://doi.org/10.1016/j.jadohealth.2003.10.012>
- Orabi, D. A., & Al-Akbawi, B. A. (2012). The credibility of social networking sites content for young people, a field study on a sample of Saudi youth, paper presented at the sixth annual forum of the Saudi Association for Media and Communication. *New Media, Theoretical and Applied Challenges*. King Saud University-Riyadh 23-24 April 2012, corresponding to 15-16 Jumada al-Awal 1433 HA.
- Radi, Z. (2003). The use of social networking sites in the Arab world. *Journal of Education*, (15). Amman Private University, Amman.
- Rustam, H. M. F. (2000). *Information crimes, the origins of the technical criminal investigation and the proposal to establish a unified Arab mechanism for specialized training*. A research presented to the Conference of Law, Computer and Internet organized by the Faculty of Sharia and Law at the United Arab Emirates Univ.
- Sadiq, K. M. (1989). *Social Responsibility for Public Relations in Economic Units* (PhD Thesis). Public Relations Department, Faculty of Information, Cairo University.
- Shafiq, N. (2015). *The Impact of Electronic Threats on International Relations* (p. 108). Cairo: Arab Knowledge Office.
- Shawki, E. (2015). *Cyber terrorism and its crimes*. Retrieved from <http://www.annntv.tv/new/showsubject.aspx?id=121062>
- Weimann, G. (2004). *Cyber terrorism: How real is the threat?* United States Institute of Peace, Special Report.
- Zaitoun, W. (2006). *The Political Dictionary. vesion I*. (Jordan: Osama Al-Mashreq Cultural House).
- Zoubi, N. (2017). *Social responsibility through social networks*. Retrieved from <http://akhbar-alkhaleej.com/news/article/1085655>

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).