Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

A Strategic Vision for Combating Cyberterrorism

Mathkar Alsubaie*

Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.

Received 06 Sep. 2021; Accepted 27 Oct. 2021; Available Online 30 Dec. 2021

Abstract

Cyberterrorism has become a well-known cybersecurity subject in today's digital world. The spread of cybercrimes calls for disseminating ethical values and peace between countries and individuals. Because of this phenomenon's danger to society, this study sought to lay down directives for security strategies to confront cyberterrorism. Hence, the study's main research problem revolves around highlighting the role of security authorities in addressing cyberterrorism according to the specialists in information technology (IT) centers in Saudi universities in Riyadh. Hence, a descriptive analysis method was adopted as a research methodology. We distributed questionnaires as a study tool to 150 specialists in IT centers in Saudi universities in Riyadh. The study yielded different views regarding the types and ways of cyberterrorism committed through the internet. Results showed the respondents' opinions regarding the essential types of cyberterrorism. Moreover, they emphasize the need to raise awareness in dealing with cyberterrorism by enforcing cybersecurity with the most prominent means and procedures that the authorities are responsible for. The most critical recommendations are: (1) the need to provide the employees with the technical skills to know how to deal with any potential security breach, (2) the need to provide specialized training courses in protection methods for workers, and (3) the need to develop the means of security and legal protection through developing e-government security agreements.

I. Introduction

The world is witnessing significant development in communications and information technology (IT). Nowadays, we are living in the information revolution age. Rapid and continuous changes resulting from scientific and technological advancement have revolutionary effects on human life and lifestyles. Accordingly, the term cyberterrorism is commonly used because of the escalating danger and complexity of terrorist crimes originating from accessible communication between terrorist groups to coordinate their crimes. Moreover, technological progress assists criminals in innovating criminal methods and techniques that are more advanced. In this regard, the American expert in international terrorism, Gabriel Weimann, indicates that websites administered by terrorist organizations witnessed a significant increase from (12) in 1998 to (4,800) in

Keywords: Cybercrime, Strategic vision, Cyberterrorism, Saudi IT centers, Information security.

Production and hosting by NAUSS

* Corresponding Author: Mathkar Alsubaie
Email: malsubaie@nauss.edu.sa
doi: 10.26735/HFWE4609

2010. He added that modern terrorism has become more dangerous, as it depends on state-of-the-art technology, the internet. Subsequently, the crime scenes of terrorist operations have become more comprehensive. It is difficult to catch the new cyber monster [1].

Today, the world encounters terrorist organizations and gangs that practice criminal activities through the world wide web. They have thousands of websites for communicating with financiers, supporters, and advocates. In addition, such organizations and gangs utilize the internet to recruit terrorists and spread aberrant and destructive ideas. They plan, coordinate, and exchange experiences to commit terrorist crimes. And they employ terrorist cyber education as a new criminal tool on the web. This tool threatens countries' infrastructures by penetrating financial and economic institutions, such as banks, hacking emails, and disseminating programs to sabotage information systems [2].

The wise leadership of the Kingdom of Saudi Arabia realizes the creeping danger of cyberterrorism. A supreme decree was issued on 11/2/1439 H, corresponding to 31/10/2017, to establish the National Cybersecurity Authority (NCA). This authority seeks to develop a national strategy for cybersecurity, protect the infrastructure of sensitive information, and develop national cooperation between the government and the communications and information sectors. The deterrence of cybercriminals, creation of nationwide capabilities for managing cyber incidents, and promotion of a national culture of cybersecurity are also objectives of the NCA [3].

II. Study Problem

Cyberspace has become the fifth arena of war and terrorism. The other four arenas are land, sea, air, and outer space. There is no difference between the use of IT for committing terrorist crimes and the use of information and communication technology as a weapon of attack in cyberspace [4].

Al-Harbi [5] demonstrates that cyberterrorism harms and destroys infrastructures of communications and information technology facilities. It also interrupts the natural performance of electronic control and command systems and causes breakdowns of important and strategic facilities. The website of the NCA indicates that cyber threats increased during the first quarter of 2018 by 13.5%, compared to the same quarter of 2017. These cyberthreats are as follows [6]:

- 31% Malware.
- 2% Service breakdown.
- 2% Destructive attacks.
- 6% Misuse.
- 6% Phishing.
- 14% Leakage of information.
- 20% Unauthorized access or modification.
- 22% Hacking attempts

Hence, the study questions are:

1. What are the types and forms of cyberterrorism, according to the viewpoints of specialists at IT centers in Saudi universities in Riyadh?
2. What is the role of IT centers in raising awareness of the threat of cyberterrorism, according to the viewpoints of specialists at IT centers in Saudi universities in Riyadh?
3. What are the most prominent means used to address the phenomenon of cyberterrorism?
4. Are there statistically significant differences in the responses of the sample of the study individuals on the axes of the study according to age, academic degree, specialization, and training courses?

III. Study Objectives

The study seeks to achieve some objectives. The most important objectives lie in identifying the following:

1. The types and forms of cyberterrorism, according to the viewpoints of specialists at IT centers in Saudi universities in Riyadh.
2. The role of IT centers in raising awareness of the threat of cyberterrorism, according to the viewpoints of specialists at information and technology centers in Saudi universities in Riyadh.
3. The most prominent means used to address the phenomenon of cyberterrorism.
4. To find out if there are statistically significant

differences in the viewpoints of the sample of the study individuals on the axes of the study according to age, academic degree, specialization, and training courses.

IV. Theoretical Background of the Study

A. The Theoretical Framework

The term cybersecurity is considered one of the terms that are subject to scientific developments and global policies. It is related to the areas and fields of digital, electronic, and technological processes that have many scientific aspects and complicated issues. These processes seek to create, store, save, modify, and utilize information through innovative systems of information engineering. We can define and demonstrate the concept of cybersecurity and its importance [7] as follows:

Cybersecurity

The internet is associated with the construction of a new space called virtual cyberspace. This concept appeared for the first time in a science fiction novel by the American-Canadian writer William Gibson in the 1980s. Gibson wrote many books that included the concept of cyberspace combined with the internet to constitute the new space for communication. This space is created by man to be an imaginary virtual place governed by clicks on a computer keyboard [8].

Frederick Mayor defines cyberspace as "A new human and technological environment for expression, information, and exchange". It primarily includes people of all countries, cultures, languages, ages, and careers connected with each other through a communication infrastructure allowing information exchange and transmission digitally. Therefore, the word cyber refers to the most famous expression in the information age. The concept of cyberspace has become more comprehensive than the internet. It includes all communications, networks, and databases. Cyberspace also encompasses information packages available online and can be exchanged upon their usage [9].

Cyberspace is governed by non-traditional physical conditions. It plays the mediator role through working on computers and communication networks. Everyone is looking forward to accessing such virtual spaces as they facilitate communication by their digital nature, with no geographical limit [10].

In addition, the digital nature of virtual spaces eliminates all obstacles impeding the communication process. It allows fair access to all information by enabling all people to access such data with no discrimination. Cyberspace gives everyone all over the world a chance to express their opinion with no hesitation or fear. Everyone can create their interactive tool with no restrictions on time or place. Therefore, they can access all information at the speed of light and eliminate all distances. Cyberspace is a public field and open market where users can communicate and interact. All life activities, including media, education, and health, have turned to cyberspace, a new sphere of life encompassing new forms of social relationships [8].

Motivations for Cybercrimes

Cybercrimes are committed with multiple and various motivations:

1. Leakage information and reveal sensitive information.
2. Challenge the information systems capacities and surpass the complexity of technological tools.
3. Harm some individuals or bodies through extortion, threat, or slander.
4. Misuse the internet for human trafficking and organized crimes.
5. Threaten national and military security through information war, cyber espionage, and cyberterrorism [11].

Types of Cybercriminals

There are many categories of cybercriminals. They may violate state security through local or foreign activities. In addition, cybercrimes may be categorized as aggression against individuals or funds. This criminal activity can lead to unlimited damages, surpassing damages caused by traditional crimes. However, there are four types of cyber criminals [21]:

1. Cybercriminals who are individuals using their computers and phones in order to illegally penetrate computer systems to explore, get information, or merely out of curiosity.
2. Cybercriminals categorized as employees not satisfied with their organizations. After working hours, they try to devastate or damage their organizations' websites, or they seek to defame their organizations.
3. Cybercriminals categorized as hackers, including amateurs or people seeking amusement. Some professionals hack some selected websites, damaging the system or stealing the system's content. Most cybercrimes are classified under the two sections of such a type.
4. Cybercriminals categorized as perpetrators of organized crimes, such as drug groups and car-theft gangs. They use the internet to sell stolen spare parts.

Cybercriminals have specific characteristics that distinguish them from other criminals [12]. They are as follows:

1. Age: From 18 to 47 years old with an average age of 25 years.
2. Knowledge and technical capabilities: cybercriminals are usually educated; most of them are specialists and internet users.
3. Personality traits: Very cautious and afraid of arrest and exposure.
4. Mental capabilities: High level of intelligence.
5. Technical skills: High-level technical skills.
6. Ability to conceal Identity: cybercriminals can hide their identities through internet routes. They can wear a technical mask, appearing in different ways from one country to another [12].

B. International and National Efforts for Combating Cybercrimes

The increase of cybercrimes has pushed the United Nations (UN) to conclude the Convention on combating the abuse of technology for criminal purposes in December 2000, under No. (63/55) during the plenary session. Indeed, it emphasized the need to strengthen coordination and cooperation efforts between countries to combat the use of technology for criminal purposes. In addition to the vital role that the organization and regional organizations can have, the UN held the 12th congress on crime prevention and criminal justice in Brazil from April 12 to 19, 2010. In this congress, member states discussed different ways of using technology by criminals and the ways to combat it by the authorities concerned [13].

C. Kingdom of Saudi Arabia Efforts for Combating Cybercrimes

Cyber dangers have recently increased. Therefore, the Kingdom of Saudi Arabia has been keen to maintain the safety and flexibility of cyberspace in order to protect national security priorities. A supreme decree was issued on 31/10/2017 to establish the National Cybersecurity Authority (NCA). This authority provides policies and procedures to safeguard networks, information technology systems, and operational technology systems and their components, including hardware, software, services, and data. The supreme decree reflects the critical importance of cybersecurity for communities and seeks to establish a base for a national industry in the cybersecurity field. The kingdom is looking forward to occupying a pioneering rank in this field to achieve its Vision 2030 [14].

D. Literature Review

Many previous studies on scientific portals have been reviewed. In [15], a strategic vision for protecting the cyberspace of the KSA has been explored. The study aimed at putting a general perspective on the importance of adopting a national strategy to protect the kingdom's cyberspace. The researcher employed the descriptive analytical approach, content analysis, and inductive deductive approach to achieve the best reliability for research methods. Its main findings were:

1. Exploring the real state of cyberspace protection in the Kingdom of Saudi Arabia.
2. Indicating the cyberspace dangers affecting the sovereignty of the kingdom.

3. Highlighting how officials responsible for maintaining information security in the kingdom are aware of cyberspace dangers.

The study in [2] has highlighted the clear evidence and indicators predicting that cyberterrorism would be the main component of a future world war. It also defined the concept, motivations, and tools of cyberterrorism. The mechanisms and strategies that should be adopted to counter cyberterrorism were demonstrated in this study. The most important findings of the study were:

1. Cyberterrorism crimes originate from traditional terrorist crimes; cyberterrorism crimes represent the electronic form of terrorism.
2. The relationship between computer and information crimes and cyberterrorism crimes is clear. Both types of crimes are criminal activities, and the place they are committed is the same, the electronic environment.

The study in [16] tried to identify the mechanisms that countries' governments may activate for promoting international cybersecurity. It discussed the relationship between cyberpiracy and changes affecting the global security cyber environment. The study applies the descriptive-analytical approach. The most important findings of the study were:

1. The current age that we witness is a digital one governed by knowledge, information, and communication. It is a reality that highlights those who have the ability will have everything.
2. Cyberspace has become a reality, and cyberwars are an inevitable fact of our lives. Cyberwars represent the fifth generation of wars, and many academics believe that such wars will be the wars of the future.
3. In this digital age, digitization is the standard form of money, governments, cyber sovereignty, cybersecurity, and cyber diplomacy.

The study in [17] focuses on terrorism that utilizes digital and electronic tools. This kind of terrorism is called digital terrorism or cyberterrorism. It aimed to increase social awareness of this kind of terrorism and shed light upon its aspects, forms, dangers, and ways to confront it.

The researcher employed the descriptive analytical approach. The most important findings of the study are that cyberterrorism has many forms. The most common forms are as follows:

- Devastation of websites, data, and information systems .
- Exchange and publication of terrorist information on information networks.
- Threatening and frightening other people and governmental hacking websites.

P. Korovessis in [18] had an objective to measure the level of knowledge and awareness concerning information security in the academic sector. The study also explored the students' need to recognize information security. The study was based on a case study. It was applied to a sample selected from the American College of Greece. A questionnaire was distributed to 160 students registered on the Introduction to Information Systems course (bachelor's degree).

This questionnaire covered many aspects, including how students use the internet and their level of knowledge on information security. The most important methods employed by students to protect their computers set passwords, and use e-mails are also highlighted in the study. The study presented some findings, including the following:

1. Most students spend long hours on the internet using instant messaging applications, email, and social media for social and entertainment purposes. The study indicates that the awareness level of internet usage for educational objectives is not enough.
2. The students believe that using passwords is one of the most common ways to gain unauthorized access to computers. However, 40% of students are prepared to disclose their passwords to their colleagues or instructors.
3. The study indicates that students frequently use antivirus and firewall programs for protecting data. However, many students do not recognize the need for substantial data backup and program updates.

H. Chan and S. Mubarak in [19] focused on how aware employees in the higher education sector in South Australia are about information security.

The explorative research study was based on a questionnaire for data collection. This questionnaire was sent by email to all employees (2,400) at a higher education institution in South Australia. Three hundred eight responses were received in total, representing (12.8%) of the study sample.

The questionnaire included (17) questions distributed into five sections. The first section is related to knowledge of information security concepts to explore employees' awareness level of the most important concepts in this field. The second section highlights how employee behaviors are compatible with information security concepts. The third section concentrates on the employees' consciousness of the information security policies of the organization. The fourth section focuses on computer crimes and how employees are aware of security incidents. It also explores employees' previous experiences to identify their perceptions of procedures and measures taken. The last section identifies demographic groups of respondents, such as the job field and its relevance to information security. The study yielded numerous findings, the most prominent are as follows:

1. Employees had weak knowledge of the concepts related to information security, as only (17.9%) indicated their knowledge of the concept of social engineering as an example of concepts related to information security.
2. About (40%) of the employees were not aware of the policies related to information security in their institutions, while (32.8%) were not aware of the password policies.
3. (75.3%) of the employees who understood the concepts of phishing and spam mail opened untrusted links. This revealed that the knowledge of concepts is not related to employees' behavior in protecting information security.

Comment on Previous Studies

By referring to previous studies, the researchers found that all studies focused on cyberterrorism.

Aspects of Similarity:

- Most obtained studies focused on the impact of cyberterrorism.
- The current study is consistent with most of the previous studies in terms of methodology, reliance on the descriptive method, and the use of the questionnaire as a tool to collect data.

Aspects of Difference:

- The present study is distinguished from previous studies in that it studies the development of a strategic vision to combat cyberterrorism.
- The current study differs from previous studies in terms of the spatial and temporal limits of the study.
- The current study differs from previous studies in terms of the sample of the study.

Aspects of Benefit

The researchers benefited from the previous studies in several aspects, such as writing the theoretical framework, building and preparing the tool of the study, defining the terms of the study, choosing the methodology and appropriate procedures for the study, as well as benefiting from the recommendations and suggestions included in those studies.

V. Methodological Procedures of the Field Study

A. Study Methodology

In conducting this study, the researchers used the descriptive method in its analytical and survey forms. They referred to books and scientific literature about the study and collected data from the study individuals using the questionnaire.

B. Study Population

The study population consists of specialists at information and technology centers in Saudi universities in Riyadh (King Saud University, Prince Sultan University, Princess Nourah Bint Abdulrahman University, and the Saudi Electronic University). The study was conducted during the first semester of 1441 H. Their total number is (150) specialists.

C. Study Sample

This step requires that all characteristics of the population of the study individuals be available in the individuals chosen to be members of the sample [20].

The researchers used statistical equations to determine the appropriate minimum limit of the sample size. It was determined by (108), with 95% confidence degree and 0.05 error in ratio estimation. The researcher distributed many questionnaires and finally obtained (113) questionnaires valid for statistical analysis.

D. Study Tool

In preparing the questionnaire, the researchers used the sources and books related to the subject of the study in addition to previous studies that addressed the research subject with the directives of the supervisor and the observations of the reviewers after presenting the questionnaire to them. Through their opinions, some phrases were modified and rephrased, and the final form of the questionnaire was produced. The questionnaire consists of two parts:

The first part: This is dedicated to the primary data related to demographic data.

The second part: the questionnaire axes:

- The first axis is entitled "Types and Forms of cyberterrorism". It includes (10) phrases.
- The second axis is entitled: "The Role of Information and Technology Centers in Raising Awareness of the Threat of Cyberterrorism". It includes (8) phrases.
- The third axis is entitled: "The Most Prominent Means Used to Address the Phenomenon of Cyberterrorism". It includes (14) phrases.

Each phrase in these axes corresponds to the following alternatives: (Strongly Agree - Agree - Neutral - Disagree - Strongly Disagree).

E. Validity and Reliability of the Study Tool

The validity of the study tool was verified by two approaches:

1) Face Validity

The questionnaire was presented to a group of reviewers to verify its face validity and to obtain their opinions on the questionnaire phrases in terms of clarity and importance. Some modifications were made, and some phrases were deleted, modified, and rephrased until the final form of the questionnaire was produced.

2) Reliability and Validity of Internal Consistency

The validity of the internal consistency of the questionnaire was verified by calculating the Pearson correlation coefficient between the degree of each phrase and the total degree of the axis to which the phrase belongs. The Alpha Cronbach coefficient was used to calculate the reliability of the study tool, and the results are shown in Table I.

The results are shown in Table I clarify that the reliability of the axis "Types and Forms of Cyberterrorism" is high and reached (0.948), which indicates the reliability and validity of this axis for field application.

Table II shows that all phrases of the first axis contributed to the reliability increase of this axis. All correlation coefficients between the phrases forming this axis and the total sum are significant at level (0.05).

The results in Table III demonstrate that the reliability of the second axis is high and reached (0.792), which indicates the reliability and validity of this axis for field application.

Table IV shows that all phrases of the second axis contributed to the reliability increase of this axis and that all correlation coefficients between the phrases forming this axis and the total sum are significant at level (0.05).

The results in Table V demonstrate that the reliability of the third axis is high and reached (0.938), which indicates the reliability and validity of this axis for field application.

Table VI shows that all phrases of the third axis contributed to the reliability increase of this axis. All correlation coefficients between the phrases forming this axis and the total sum are significant at level (0.05).

F. Correction Method of Questionnaire Scale (Questionnaire Tool)

Data were collected, reviewed, and then processed by the computer for statistical analysis. Data were given numbers by converting verbal answers to digital (coding), where the answers (Strongly Agree) in the first and third and fourth axes were given 5 degrees: (Agree) 4 degrees, (Neutral) 3 degrees, (Disagree) 2 degrees, and (Strongly Disagree) one degree.

The researchers calculated the arithmetic mean for the answers of the sample of the study individuals, where the length of the pentameter scale cells (lower and upper limits) used in the study axes were determined. Accordingly, the range was calculated (5-1 = 4) and then divided by the number of the scale cells to get the correct cell length, i.e. (4/5 = 0.80). Then this value was added to the lowest value in the scale (or the beginning of the scale, which is the integer (1)) to determine the upper limit of this cell. The length of the cells is represented in Table VII.

TABLE I
THE ALPHA CRONBACH COEFFICIENT TO CALCULATE THE RELIABILITY OF THE FIRST AXIS

Axis	Number of Phrases	Alpha Cronbach Coefficient Value
Types and Forms of Cyberterrorism	10	0.948

TABLE II
THE PSYCHOMETRIC ANALYSIS OF THE PHRASES OF THE FIRST AXIS N = 30

Phrase number	Alpha coefficient if the element is deleted	Corrected correlation coefficient	Axis correlation coefficient	Phrase number	Alpha coefficient if the element is deleted	Corrected correlation coefficient	Axis correlation coefficient
1	0.939	0.892	**0.912	6	0.938	0.882	**0.907
2	0.939	0.863	**0.893	7	0.948	0.695	**0.763
3	0.940	0.865	**0.891	8	0.948	0.563	**0.652
4	0.944	0.766	**0.813	9	0.938	0.910	**0.928
5	0.946	0.709	**0.768	10	0.943	0.774	**0.821

** Correlation is significant at level (0.01)

TABLE III
THE ALPHA CRONBACH COEFFICIENT TO CALCULATE THE RELIABILITY OF THE SECOND AXIS

Axis	Number of Phrases	Alpha Cronbach Coefficient Value
The Role of Information and Technology Centers in Raising Awareness of the Threat of Cyberterrorism	8	0.792

TABLE IV
THE PSYCHOMETRIC ANALYSIS OF THE PHRASES OF THE SECOND AXIS N = 30

Phrase number	Alpha coefficient if the item is deleted	Corrected correlation coefficient	Axis correlation coefficient	Phrase number	Alpha coefficient if the item is deleted	Corrected correlation coefficient	Axis correlation coefficient
1	0.789	0.353	**0.502	5	0.777	0.445	**0.586
2	0.754	0.611	**0.712	6	0.750	0.661	**0.743
3	0.793	0.385	**0.581	7	0.773	0.479	**0.641
4	0.730	0.706	**0.811	8	0.777	0.445	**0.578

** Correlation is significant at level (0.01)

TABLE V
THE ALPHA CRONBACH COEFFICIENT TO CALCULATE THE RELIABILITY OF THE THIRD AXIS

Axis	Number of Phrases	Alpha Cronbach Coefficient Value
The Most Prominent Means Used to Address the Phenomenon of Cyberterrorism	14	0.938

TABLE VI
THE PSYCHOMETRIC ANALYSIS OF THE PHRASES OF THE THIRD AXIS
N = 30

Phrase number	Alpha coefficient if the item is deleted	Corrected correlation coefficient	Axis correlation coefficient	Phrase number	Alpha coefficient if the item is deleted	Corrected correlation coefficient	Axis correlation coefficient
1	0.938	0.501	**0.545	8	0.936	0.644	**0.709
2	0.936	0.575	**0.631	9	0.937	0.611	**0.681
3	0.934	0.684	**0.737	10	0.930	0.838	**0.862
4	0.933	0.690	**0.739	11	0.929	0.868	**0.888
5	0.933	0.732	**0.786	12	0.931	0.771	**0.806
6	0.935	0.659	**0.698	13	0.928	0.875	**0.898
7	0.935	0.618	**0.672	14	0.930	0.805	**0.839

** Correlation is significant at level (0.01)

TABLE VII
CORRECTION METHOD OF QUESTIONNAIRE SCALE

Alternatives	Weight	Arithmetic Mean
Strongly Disagree	1	From 1.00 to less than 1.80
Disagree	2	From 1.80 to less than 2.60
Neutral	3	From 2.60 to less than 3.40
Agree	4	From 3.40 to less than 4.20
Strongly Agree	5	From 4.20 to 5.00

VI. RESULTS AND DISCUSSION

1) Summary of the findings related to the characteristics of the sample of the study individuals:

The study revealed that most of the targeted sample individuals (62), representing (54.9%) of the total sample of the study individuals, hold academic degrees (university/diploma), while (51) individuals, representing (45.1%) from the total, hold postgraduate degrees.

Findings also revealed that most of the targeted sample individuals (33), representing (29.2%) of the total sample of the study individuals, are aged from 30 years to less than 35 years, while (24) individuals, representing (21.2%) of the total, are aged 40 years and over. Also, findings showed that (27) of the sample of study individuals, representing (23.9%) of the total, are specialized in computer science, and (29) individuals, representing (25.7%) of the total, are specialized in other fields, such as systems protection and data analysis.

The findings also indicated that most of the targeted sample individuals (43), representing (38.1%) of the total, did not take any training courses in the field of information security. In contrast (36) individuals, representing (31.9%) of the total took more than three courses, and (34) individuals, representing (30.1%) of the total, took from 1 to 3 courses.

2) Summary of the findings related to the study questions:

a) Most prominent findings of the first question: What are the types and forms of cyberterrorism?

Findings showed variance in the viewpoints of the specialists at IT centers in Saudi universities in Riyadh in their answers on the types and forms of cyberterrorism. The arithmetic mean of the first axis reached (3.61 out of 5). Moreover, these specialists believe that the most prominent types and forms of cyberterrorism can be summarized as follows: flooding governmental networks with harmful files, hacking governmental websites in order to block the service or promote misleading information, recruiting people by certain authorities to hack important websites, disseminating rumors through various technical means to threaten community security, and blackmail through social media platforms and technical means.

b) Most prominent findings of the second question: What is the role of IT centers in raising awareness of the threat of cyberterrorism?

Findings showed variance in the viewpoints of

the specialists at IT centers in Saudi universities in Riyadh in their answers on the role of information and technology centers in raising awareness of the threat of cyberterrorism. The arithmetic mean of this axis reached (4.40 out of 5). Moreover, these specialists believe that the most prominent roles of IT centers in raising awareness of the threat of cyberterrorism can be summarized as follows:

- Deterrent laws should be enacted for hackers, families should educate their children on electronic threats, schools should organize workshops on cyberterrorism to raise awareness of their students.
- Various authorities within the state should coordinate their efforts to raise awareness of the threat of cyberterrorism.
- The role of preventive control against the threat of cyberterrorism should be activated through information centers, and the NCA should rely on awareness-raising programs to address cyberterrorism.

c) Most prominent findings of the third question: What are the most prominent means used to address the phenomenon of cyberterrorism?

The findings revealed a variance in the viewpoints of the specialists at IT centers in Saudi universities in Riyadh in their answers on the most prominent means used to address the phenomenon of cyberterrorism. The arithmetic mean of this axis reached (4.41). Moreover, these specialists believe that the most prominent means used to address the phenomenon of cyberterrorism can be summarized as follows:

- It is necessary to use firewalls to protect the information network of the organization or institution.
- Government authorities websites should be protected against unauthorized access, it must be ensured that data and information resources will not be exposed to illegal use, confidential means of information should be used, and information should not be shared with unauthorized persons.
- Specialized programs against electronic piracy should be used, staff should be technically qualified with the know-how to address any potential security breach.
- Specialized training courses on protection means should be provided for staff, and legal and security protection means should be developed by developing security e-government agreements.

d) Most prominent findings of the fourth question: Are there statistically significant differences in the viewpoints of the sample of the study individuals on the axes of the study according to age – academic degree - specialization - training courses?

There were no statistically significant differences at level (0.05) and less in the responses of the sample of the study individuals on the axes (The role of information and technology centers in raising awareness of the threat of cyberterrorism and the most prominent means used to address the phenomenon of cyberterrorism), according to an academic degree.

There were statistically significant differences at level (0.05) and less in the responses of the sample of the study individuals on the first axis depending on academic degrees since the level of significance (0.01) is less than the level of significance (0.05). These differences are in favor of the sample of the study individuals holding postgraduate degrees.

There were no statistically significant differences at level (0.05) and less in the responses of the sample of the study individuals on all axes according to age and training courses in the field of information security.

VII. Conclusion And Perspectives

This study tried to address the role of security authorities in identifying cyberterrorism from specialists in IT centers in Saudi universities in Riyadh. The study applied the descriptive-analysis approach and used the questionnaires as a study tool. (150) specialists working in the IT centers in Saudi universities in Riyadh were questioned. The following recommendations emerged:

1. Enact deterrent laws and to increase penalties for cybercriminals and hackers.
2. Families should work on raising the awareness of their children about the danger of cyberthreats on social media.
3. Schools should organize workshops on cybercrimes to educate students.
4. It is helpful to coordinate efforts between different authorities within the state to raise awareness of the threat of cyberterrorism.
5. The role of preventive control against the threat of cyberterrorism should be activated through societal institutions of various specialties.
6. The NCA should rely on awareness-raising programs to address cyberterrorism.
7. It is of great importance to use a firewall to protect the information network of the organization or institution.
8. Websites of government authorities should be protected against unauthorized access.
9. It is imperative to ensure that data and information resources cannot be exposed to illegal use.
10. It is helpful to use confidential means of sharing information, not sharing information with unauthorized personnel, and use specialized programs against electronic piracy.
11. Staff should be technically qualified with the know-how to address any potential security breach, and they should be provided with specialized training courses on protection methods.
12. Security and legal protection means should be developed through establishing security e-government agreements.

Main perspectives of this study are conducting in depth research on the relationship between the quality of the firewalls and the level of protection of the information networks of governmental organizations and institutions. Also, the effect of staff training in governmental institutions on reducing the risks of cybercrimes at work.

References

[1] A. A. Alfeel, "Electronic terrorism," (in Arabic), in *Gulf Univ. J. Law Division*, vol. 2, no. 2, pp. 237-285, Jan. 2010.

[2] H. A. Al-Shehri, "Electronic Terrorism: Network Warfare," (in Arabic), in *Int. Arab J. Inf. Technol.*, vol. 4, no. 8, pp. 1-23, Jan. 2015.

[3] https://nca.gov.sa

[4] A. Abdul Sadiq, "Book Review: Electronic Terrorism: Power in International Relations, a New Pattern and Different Challenges," (in Arabic), in *al-Nahḍah*, vol. 11, no. 4, pp. 196-203, Oct. 2010.

[5] F. M. Al-Harbi, "Cyber Terrorism," (in Arabic), Information Security Forum, 2018.

[6] https://twitter.com/nca_ksa?lang=ar

[7] A. E. Salim, "What is cyberspace," (in Arabic), in The National Magazine, vol. 51, pp. 66-69.

[8] S. M. Abdul Hamid, *Media and Cyberspace*, Egypt: Atlas Publishing House & Media Production, 2015.

[9] S. Qasimi, "Cyberspace and E-Gourds: The Problem of Creating a Virtual Public Space According to Habermas Perspective," (in Arabic), in *Al-Hikma J. Philosophical Stud.*, vol. 7, pp. 60-75, June 2016.

[10] W. Smiche, *Electronic forums: among interactivity and the art of virtual dialogue*, Jorden: Dar Osama, 2016.

[11] M. A. AlMinshawi, Internet security risks, A published research through the studies and research site, (2012), available at: www.minshawi.com

[12] M. M. AlAlfi, "Cybercrime and cybercriminal," (in Arabic), in *Combating Cyber Crimes*, Cairo, Egypt: the Arab Organization for Administrative Development, 2010.

[13] M. Mashosh, "International Efforts to Combat Cybercrime," (in Arabic), in *J. Law Bus.*, vol. 37, pp. 167-199.

[14] M. A. Almagsodi, "Cyber Security and International Efforts in Combating Transnational Crime," (in Arabic), in *Al Amn Wa Al Hayat*, vol. 37, no. 427, pp. 102-107, Nov. 2017.

[15] H. Q. Al-Shammari, "A strategic vision in protecting the cyberspace of the Kingdom of Saudi Arabia," M.S. thesis, The College of Strategic Studies, Naif Arab University for Security Sciences, Riyadh, 2015.

[16] N. Shalouch, "Cyber piracy in cyberspace: The growing threat to state security," (in Arabic), in *J. Babylon Humanities Studies*, vol. 8, no. 2, pp. 185-206, 2018.

[17] G. A. El-Dahshan, "Terrorism in the Digital Era (Cyber Terrorism): Types, Risks & Mechanisms of Encountering," (in Arabic), in *Int. J. Res. Edu. Sci.*, vol. 1, no. 3, pp. 83-121, Jul. 2018, doi: 10.29009/ijres.1.3.3.

[18] P. Korovessis, "Information Security Awareness in Academia," *Int. J. Knowledge Society Res. (IJKSR)*, vol. 2, no. 4, pp. 1-17, 2001, doi: 10.4018/jksr.2011100101.

[19] H. Chan and S. Mubarak, "Significance of Information Security Awareness in the Higher Education Sector," *Int. J. Comput. Appl.*, vol. 60, no. 10, pp. 23-31, Dec. 2012, doi: 10.5120/9729-4202.

[20] M. A. Al-Nooh, *mbada' albahth al tarboui*[Principles of Educational Research], Saudi Arabia: Al Rushed Bookstore, Jan. 2004.

[21] A. I. STANCU, 'Cybercriminals and the Victims of Cybercrime," *J. Law Admin. Sci.*, vol. 14, pp. 127–136. 2020.