Journal of Information Security, 2014, 5, 137-146
Published Online October 2014 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2014.54013

Awareness of the Potential Threat of Cyberterrorism to the National Security

Abdulrahman Alqahtani

School of Politics, Philosophy & International Studies, The University of Hull, Hull, UK
Email: qahtaniasa@me.com

Received 13 July 2014; revised 10 August 2014; accepted 5 September 2014

Abstract

The revolution of computing and networks could revolutionise terrorism in the same way that it has brought about changes in other aspects of life. The modern technological era has faced countries with a new set of security challenges. There are many states and potential adversaries, who have the potential and capacity in cyberspace, which makes them able to carry out cyber-attacks in the future. Some of them are currently conducting surveillance, gathering and analysis of technical information, and mapping of networks and nodes and infrastructure of opponents, which may be exploited in future conflicts. This paper uses qualitative data to develop a conceptual framework for awareness of cyberterrorism threat from the viewpoint of experts and security officials in critical infrastructure. Empirical data collected from in-depth interviews were analysed using grounded theory approach. This study applied to Saudi Arabia as a case study.

Keywords

Cyberterrorism, Terrorism, National Security, Critical Infrastructure, Conceptual Framework

1. Introduction

Modern technology, which consists of computers, networks, communications, satellites and others, has contributed to increasing openness, which is attributed largely to the growth of interdependence between the parts of the world, provided by the ever-expanding Internet. This very rapid growth in computers and related networks and infrastructure pushed the world into the "information age", which is generally accepted as the period covering the late twentieth century and early twenty-first century [1].

Information and Communication Technology (ICT) brought with it the importance and interest in the spread and exchange of information between continents and countries of the world, and has therefore become one of the pillars of the current era, bringing many benefits. Nevertheless, it has raised risk and security concerns. With the entry of the Web or "Internet" and the ever-increasing users of this technology, terrorist attackers, hackers

How to cite this paper: Alqahtani, A. (2014) Awareness of the Potential Threat of Cyberterrorism to the National Security. *Journal of Information Security*, **5**, 137-146. http://dx.doi.org/10.4236/jis.2014.54013

and intruders spend hours in an attempt to penetrate, or gain access to important information, which can be used for material and moral extortion.

Given the importance of the security of critical infrastructure constantly evolving in Saudi Arabia, and related networks, information systems and control systems and supervision, as well as the importance of information security to the general public, this is one of the major and important factors to achieve and maintain national security in Saudi Arabia. In contrast, any disruption or instability in national security will result in very serious consequences for the stability of the country, its economy and its political situation.

This research derives its significance from the importance of its themes. Saudi Arabia's national security is of top priority to the Saudi government. What will help to achieve this is to understand, identify and predict early indicators that may pose a threat to national security. This study by analysing qualitative data, which was obtained from the critical infrastructure helps to describe potential threat posed by cyberterrorism to national security, as compared to conventional terrorism. This pairing and comparison will help to identify the level of awareness of this threat. This in turn will provide a conceptual framework for decision-makers about the problem in question and therefore the government will be able to take the necessary action on a clear basis and within a strategic path to combat cyberterrorism.

2. Literature Review

In the literature on terrorism, Cyberterrorism might be one of the terms that is most misunderstood and misused. According to Ron Dick, Director of National Infrastructure Protection Centre (NIIPC) in 2002, cyberterrorism means "any criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies" [2]. More comprehensively, according to Dorothy Denning, "Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" [3].

From the literature on information warfare, to illustrate the difference between information warfare and cyberterrorism, it should be realised that cyberterrorism could be one of the components of information warfare. In other words, information warfare includes cyberterrorism [4]. Some suggest that information warfare is an offensive and defensive function of governments [5]. However, how effective is cyberterrorism in the nature of the warfare in the information age? According to David Lonsdale, it "will only substantially change the nature of warfare if it proves to be independently strategically effective" [6]. Hence, cyberterrorism can be defined as the intentional use of subversive activities, or the threat thereof, against computers and networks related to critical infrastructure and vital services, with the intention to cause massive physical and psychological harm, for any objective whatsoever.

In general, cyberterrorism involves a surprise attack by sub-state terrorist organizations or groups of individuals using computer technology and networks to hinder or disrupt the electronic and physical infrastructure of a state, to achieve a certain agenda. This causes the loss of critical services such as electric power, banking systems, health services, telephone, Internet and others. At the same time, the target might be individuals or groups of individuals, such as cyber-attacks against implanted medical devices which may cause death. The aim of such action is not limited to the economic impact on a particular state, but also to amplify the physical effects of conventional terrorism, through the events of more confusion and panic among the general public of the state. According to the FBI's National Infrastructure Protection Centre (NIPC), the goal of cyber-terrorism is "to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda" [7]. Terrorist organizations "generally use symbolic means to attack the sanctity of the society in which it exists. If attacks on these symbolic targets are successful, the terrorists will have accomplished their goal of isolating individuals from the society in which those individuals formerly felt secure. Such actions result in confusion and uncertainty about a government's ability to protect its citizens. This is when citizens are most vulnerable to influence by others" [8].

3. Methodology

The Grounded Theory Method is a form of qualitative method that comprises a systematic, inductive, and comparative approach for conducting inquiry for the purpose of constructing theory [9]. This methodology is de-

signed mainly to encourage the continuous interaction between the researcher and the data, through constantly engagement in emerging analysis during the study. Data collection and analysis proceed simultaneously with each other, and inform and facilitate each other. GTM builds experimental investigations in the analysis process, as it leads the researcher to test all theoretical explanations for the empirical findings of the research. An iterative process is used to move forward and backward between the empirical data and emerging analysis, which makes the collected data gradually more focused and the analysis also more theoretically successfully. GTM is currently the most widely used on a large scale and the most famous among qualitative research methods, across a broad range of disciplines and subject areas. "Innumerable doctoral students have successfully completed their degrees using GTM" [10].

Grounded Theory uses a form of purposive sampling, known as theoretical sampling, where participants are selected according to the criteria specified by the researcher and based on the preliminary results. Early analysis of the data refers to the issues that need to be explored, and thus the sampling process is guided by the ongoing development of the theory. Data collection and analysis are conducted in alternating sequences (see **Figure 1**).

Interview coding is the first step in the process of data analysis. The coding is used to capture what is in interview data, and to identify what is meant by people through their experiences. Coding helps to get away from specific statements to more abstract interpretations of these data [11]. There are several techniques used in data analysis in grounded theory methodology. This study adopted a three phase coding system suggested by Strauss [12], and Strauss and Corbin [13], namely, open coding, axial coding and selective coding. These phases were adopted because over time, they have become the most widely accepted in GTM [14]. Open coding is the first step in the process of coding; it is a good start for analysis, in which selecting and labelling categories of data take place. Therefore, aspects of the phenomenon under study are determined. It also produces a list of themes important to interviewees. Conceptual labels are attached almost to every line in the interviews transcript also known as line-by-line coding. These labels can represent the context of the interviewees' words, and when these labels are taken from their words, it is called in vivo coding. At this stage, the researcher captures the concepts that are trying to answer (what, when, where, why, who and how consequences) questions proposed by Strauss and Corbin [13].

4. Data Collection

As the problem of the research is relatively recent, and there are no studies dealing with the potential threat of cyberterrorism on the national security of the Kingdom of Saudi Arabia, compared to conventional terrorism, the research aims to explore awareness of this threat. Thus, grounded theory methodology is the appropriate option-for this search. The first stage is exploratory and preliminary findings are used to guide the ongoing data collec-

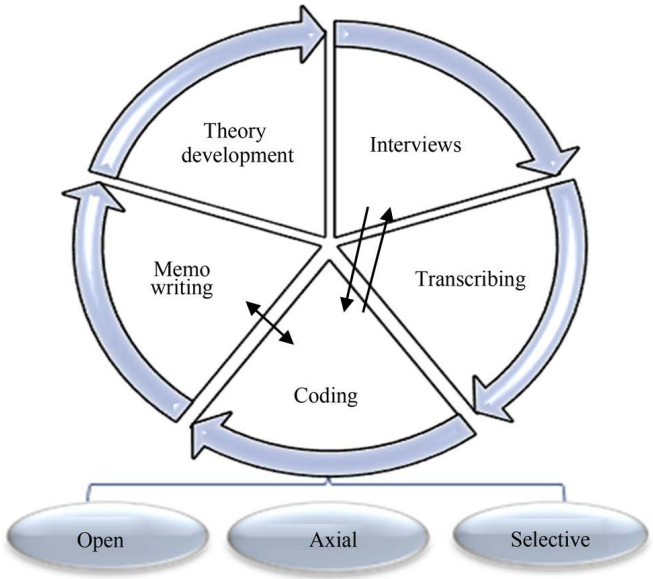

Figure 1. Process of developing a grounded theory.

tion process. The pilot study for the first phase of this study included conducting six interviews with Saudi students on scholarships to study in the United Kingdom, all of whom are studying at postgraduate level, four of them for doctoral study, two for a master's degree. All are employees working in one of the components of critical infrastructure in Saudi Arabia. These components have been divided into sectors, as also are coded for security purposes, and due to the sensitivity of the data, for example A3, F2 and so on. Interviews were analysed directly during the pilot study. Subsequently, 15 in-depth interviews were conducted based upon in the preliminary results of the pilot study. These 15 interviews were conducted with military and security officials and experts in the critical infrastructure sectors in Saudi Arabia during the collection trip.

In the pilot study for the first phase, open coding was used in the six interviews manually using pen and paper. Qualitative analysis software, such as Nvivo were not used in this phase, although it was used later in the analysis. Through open coding in the pilot study, a group of related codes emerged, which were grouped in categories, these contributed very effectively to the development of questions for subsequent interviews, and also gave initial ideas for the study. At this point, neither axial coding nor selective coding were conducted, they were left until after the conducting of in-depth interviews, in order to determine the properties and dimensions. However, instead, careful comparisons between the statements of the respondents, and between codes obtained were conducted, without being bound to a framework to determine properties and dimensions in this phase.

5. Data Analysis

5.1. Macro-Category "Awareness"

While analysing the in-depth interviews, many codes revolving around awareness emerged; they were then grouped in sub-categories under the main category "Awareness". In general, the concept of awareness is seen as helping to reduce the risk for an individual or a group, government or private installations, as well as national security, from becoming a target of terrorist threats. The answers given by security officials and experts which included the concept of awareness are represented by the sub-categories and codes presented in **Table 1**.

Despite the fact that there are many other codes (see **Appendix**), the most important codes that were repeated significantly by respondents are contained in the previous table. **Figure 2** shows the recurrence of such sub-categories in the interviews using Nvivo software.

The sub-categories and codes will be presented in detail below.

5.1.1. Importance of Awareness (Sub-Category)

The answers of the respondents indicate that there is interest in the need for awareness of possible terrorist threats among staff of critical infrastructure sectors. These views are gathered in the following codes:

- **Understanding the risks (code)**

The majority of respondents see the importance of the awareness of threats in order to understand more about the risks posed to staff and facilities. Awareness of the threat is the catalyst for seeking to understand it. C1 explained the importance of awareness,

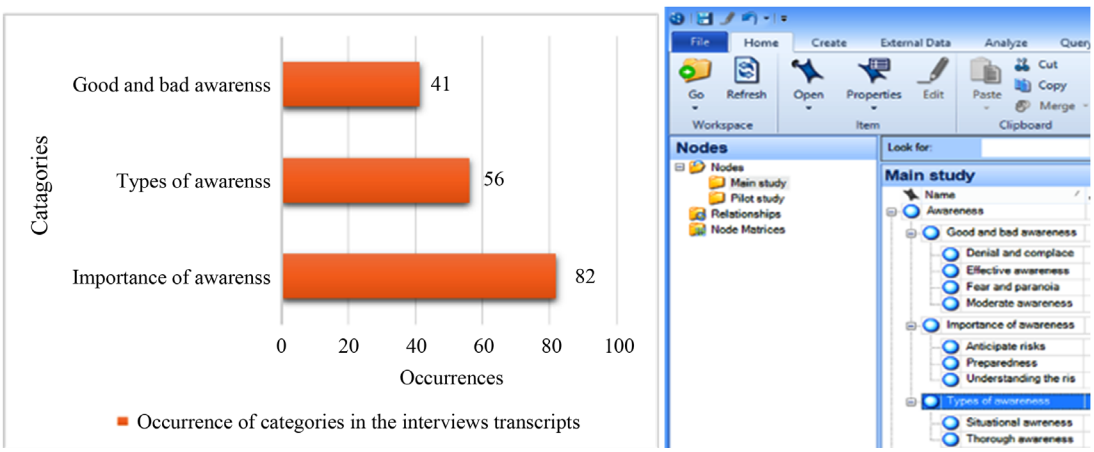

Figure 2. Occurrence of sub-categories of "Awareness" in the interviews.

Table 1. Macro-category "Awareness" and its categories.

Category	Codes
Importance of awareness	• Understanding the risks • Anticipate risks • Preparedness
Types of awareness	• Thorough awareness • Situational awareness
Good and bad awareness	• Right level of awareness • Effective awareness • Fear and paranoia • Denial and complacency

"*… we need awareness ... in order to know what actions to take to be more secure, in terms of digital and our daily activities, personal and professional, it is important to understand the nature of the risks that we face, so we can take the right decisions about the best ways to stay safe.*"

D3 added,

"*The first step in dealing with any problem is to be aware of its existence, so being aware of threats of any kind, and their existence and nature, is the basis of confronting them.*"

Also, awareness helps people to realise that it is not impossible for security threats, both cyber and conventional, to happen to employees or facilities. A3 asserted that,

"*… everyone must be aware that he is not immune to being a victim of terrorism one day, what is happening anywhere in the world could happen here* [*Saudi*]*, too, and as most security experts say, if you think now that it is impossible to penetrate your security, it just means you have not discovered the method of doing it yet.*"

- **Anticipate risks (code)**

Some officials believe that one of the important things in the face of threats is awareness, in order to be able to anticipate the risks. H1 talked about it,

"*… one of the challenges of terrorism risk analysis is the fact that the opponent is the one who can change where and when to launch attacks, and has the potential to counter-attack. So we have to be conscious of the risks in order to anticipate all possible eventualities.*"

Threats awareness is very important in assessing the likelihood of the risk, as the awareness is the result of an accumulation of experience and knowledge. F2 mentioned it,

"*I see staff who have more than ten or twenty years' experience in the work ... you find that they are more aware of such threats than their colleagues who served less ... as well as specialists in computer networks and they are more aware of the assessment of the occurrence of such threats.*"

- **Preparedness (code)**

Some respondents felt that the awareness of imminent threats leads to a state of preparedness and readiness to face them. C1 considered that,

"*… my brother, I think that whenever you are aware of, and familiar with, what is happening around you, you are inevitably going to be vigilant and prepared for what might happen next...*"

The level of awareness is important in assessing the level of preparedness. E2 introduced that equation,

"*With respect to cyber threats, we believe that the more the level of awareness, the greater the level of preparedness.*"

Memo 1: Importance of awareness

It was noted that there is variation in the consideration of awareness, some believe it is important for decision makers only, where the employee does not need to know everything, while the majority see the importance of awareness for all. There is a large connection between training and awareness, also it is observed that there is competition for training opportunities, as it not available to everyone. I sensed that there was an imbalance in the distribution of training opportunities because of personal relationships.

5.1.2. Types of Awareness (Sub-Category)

Through the interviews, it was observed that there were several types and forms of awareness, and by coding them, it was then possible to group them under the following codes:

- **Thorough awareness (code)**

There are respondents who believe in the need for thorough awareness of threats and security risks at the level of national security, represented by internal and external terrorist threats. External threats could be, for example, regional threats, whether from other states or from terrorist organisations. G1 talked about it,

"*…and decision-makers in the government must be vigilant for each potential threats surrounding such as Hezbollah, Houthis, Iran and Israel*."

This includes being vigilant for signs of cooperation with al-Qaeda in Yemen or Iraq. D4 explained that,

"*…what raises concerns is what al-Qaeda is doing by promoting their activities internally and trying to recruit naive young Saudis… young people must be aware of what is going on and that they are targeted*."

K1 also touched on it,

"*…everyone should know that many of the terrorists migrate to Yemen and then bring in weapons and explosives with the support of al-Qaeda in Yemen, exploiting the difficult mountainous borders*."

Comprehensive awareness of cyber threats and risks that may arise with knowledge about the ongoing developments in the technical world are also important, according to A4,

"*In order to protect ourselves on networks, we must be fully aware of all the developments and events in technology, and not isolate ourselves from the rest of the world*."

With regard to internal thorough awareness, infrastructure components need to be aware of their own potential threats, each sector being aware of the threats it faces, based on the nature of its function. E2 explained this point,

"*…we must understand that each facility has its own threats, for example, a bank may be exposed to cyber breakthroughs, and this is different to a car bomb attack on an oil refinery, is it not*?"

Internal awareness within each component of the critical infrastructure is key, according to F2,

"*…here we have several sections, as you know, that each section is fully aware of the problems that it might be exposed to, and that employees are aware of that too, is what we are trying to achieve*."

- **Situational awareness (code)**

There is a situational awareness, which is based on the surrounding attitudes, circumstances, and behaviour. By coding, the following codes emerged,

- **External suspicious behaviour (sub-code)**

According to some respondents, there is some specific behaviour that must be taken into account as it may indicate potential terrorist activities, especially if it has occurred in certain places. B2 said,

"*…also, the comparison of reports of some suspicious behaviour, especially in government installations, or the military, or areas where people gather, such as airports or markets, or close to one of the critical infrastructures, helps to identify the threats and deal with them*."

Examples of suspicious behaviour were given, and were seen as attempts to test security measures, physical or cyber. B2 clarified that,

"*Several reports of attempts to enter into important sites with false documents or by mistake, or attempts to penetrate government or banks' websites, all of this indicates existence of a threat.*"

There was also mention of suspicious attempts to obtain materials that could be used in terrorist activities. C1 touched on it,

"*…if there are reports about purchasing uniforms of authorities, or quantities of dangerous chemicals, or theft of identification cards or suspicious bank transfers...*"

This suspicious behaviour includes surveillance, or suspicious people in certain places, or suspicious activities. D4 pointed out that,

"*Signs that, for example, someone is filming installations or specific events, using binoculars, navigation devices or mapping or taking notes…*"

M1 added,

"*…if for example it was observed that there is traffic monitoring, by a person or persons who are not affiliated to that place, or a camera or recording device was found in their possession*."

- **Internal suspicious behaviour (sub-code)**

There may be some suspicious behaviour that people should be aware of within the facilities of critical infra-

structure. L1 emphasised that,

"*…as with strong security measures, any external threat often cannot be achieved unless there is some kind of internal collaboration, for example, an employee or a contractor or even a cleaner*."

K1 explained some methods terrorists use to request cooperation from inside,

"*Terrorists may exploit the legal access of a security guard or a clerk in order to enter the headquarters or internal network, this in my opinion is the most dangerous*."

D3 illustrated too,

"*As security personnel, we have to alert managers and staff about any unusual behaviour, such as a changing pattern of work, or sudden wealth, or a change in political attitudes or religious orientations*."

L1 also added,

"*Some of the signs that a suspected employee might be engaged in terrorist activities are unjustified absences, or an inclination to work alone or in unusual hours, or collecting donations for suspicious activities*."

Memo 2: Types of awareness
It was noted that there is a clear understanding of the concept of awareness, but I think that it is just between officials and experts, or at least at a much higher level than employees in the government sector. Also I think that material being circulated via communication programs in smart devices plays a role in raising awareness. None of the respondents provided any document or classification or official ladder of levels of threat

5.1.3. Good and Bad Awareness (Sub-Category)

Despite the importance of awareness of potential threats, there is a good and bad awareness. For example, good awareness might be finding:

- **Right level of awareness (code)**

Some respondents believe that there is a disparity in the level of awareness required for each critical infrastructure component, based on the security situation and the potential threats. For example, Ordinary Awareness was explained by B2,

"*…sometimes in normal circumstances, normal awareness of security and safety is prevailing among employees in performing tasks, where they may not have security measures in mind consciously*."

There is also a Preventive Awareness, which is a higher level of awareness. A1 talked about it,

"*…when reports are provided to us about a particular threat, the level of awareness increases as a precaution, to detect any signs and prevent it before it occurs*."

Intensive Awareness exists when a security situation is unusual. G1 suggested that,

"*…when security conditions change radically, staff must be careful and mindful, focused continuously until the situation goes back to normal*."

- **Effective awareness (code)**

Of the respondents who see that self-awareness is the basis to develop a general awareness, A3 talked about it,

"*…to be honest, it is necessary to form a self-awareness before a collective awareness, how? I tell you, first, that we have to understand that we bear the responsibility of our own personal security*."

A3 added,

"*…the same applies to service sectors and providers, government and private sectors as well, all of them are responsible for their own security in the first place, due to limited resources, and authorities cannot repel every threat alone*."

With respect to the awareness of security of information, it should be a part of the culture of the organisation. A4 emphasised that,

"*…executive directors, managers and employees might be a target for phishing for example, so everyone, without exception, must be aware of, so that it becomes an inherited culture*."

Some respondents stress that to ensure effective awareness, training and testing should be applied in the or-

ganisation. This was commented on by C1,

"*Security is important and not subject to emotions, training should be given first, and then a test, for example, by sending phishing e-mails from the department* [*IT*] *for evaluation… carelessness should be punished*."

- **Fear and paranoia (code)**

In contrast, there is over-awareness, which has a negative impact on the sense of security, and also has adverse effects on individuals and national security. D4 addressed this,

"*…try not to give into fears and precautions too much, because it leads a person to live with an exaggerated sense of insecurity, and this then achieves the terrorism goals*."

M1 warned of excessive concerns over terrorist threats,

"*…if you thought that every day, every moment and every place there would be a time bomb or a booby-trapped car, it inevitably would create a very poor sense of security, and all plans and strategies would fail*."

- **Denial and complacency (code)**

Denying or neglecting threats, is one of the most hazardous situations in terms of awareness, and may be caused by either a lack of understanding of the risk, or a failure to recognise its existence, H1 suggested that,

"*…to establish an ideal security awareness, the existence of a threat or a risk should be recognised first, as denial and neglect make it very unlikely for someone to recognise and respond to threats which emerge*."

Or it may be a result of a severe case of fear, such as in cases of terrorist bombings. G1 explained that,

"*…a person may know and be aware of the threat, but in cases of extreme fear they may not be able to take a decision or give any reaction, such as freezing* [*loughs*], *that may have happened to you*."

Category of "Awareness" and its sub-categories can be summarised in **Figure 3**.

Memo 3: Good and bad awareness

Most responses revolve around the mental state of the respondent towards the threats, so awareness is seen as being influenced by expertise, talents and instincts. This therefore sheds light on the mechanism of recruitment for cyber security jobs to defend against cyberterrorism, and how to choose the right people for the most sensitive locations, and so on. Psychology also plays an important role here, so that should be discussed in the strategy. Awareness is not always beneficial, as too much awareness can lead to unnecessary fear and insecurity which actually achieves the goals of the terrorists.

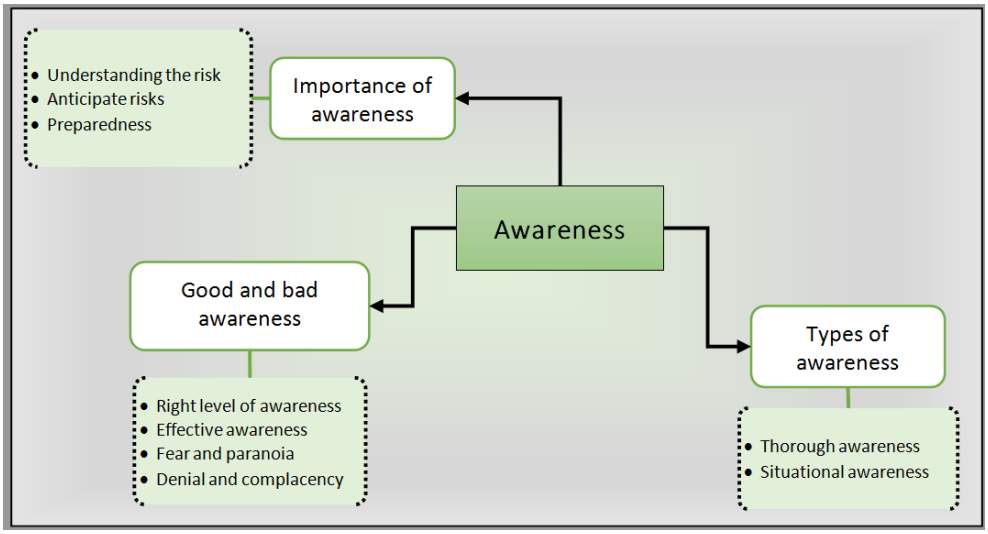

Figure 3. Category "Awareness" and its sub-categories.

6. Conclusion

Cyberterrorism is a potential threat, which could undermine the pillars of national security by targeting critical infrastructure. This seems evident in developed societies, with the increasing reliance on technology in most aspects of life. In addition, developing countries may face this threat, especially with a growing economy such as Saudi Arabia. This requires increased awareness about the potential threat to research and explore its aspects in order to confront it knowingly and perceptible. This is what this paper seeks to deliver through a conceptual framework for awareness of the threat (**Figure 3**). The researcher also in his doctorate study seeks to develop a theoretical framework to understanding and identifying the threat of cyberterrorism from a broader perspective. This is what he is trying to publish in several stages with the progress of the study.

References

[1] Lonsdale, D.J. (2004) The Nature of War in the Information Age: Clausewitzian Future. Frank Cass, London, 1.

[2] Berinato, S. (2002) The Truth about Cyberterrorism. CIO. http://www.cio.com.au/article/26124/truth_about_cyberterrorism/

[3] Denning, D.E. (2000) Cyberterrorism. Special Oversight Panel on Terrorism Committee on Armed Services US House of Representatives. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[4] Taylor, R.W. (2006) Digital Crime and Digital Terrorism. Pearson/Prentice Hall, Upper Saddle River.

[5] Pollitt, M.M. (1998) Cyberterrorism—Fact or Fancy? *Computer Fraud & Security*, **2**, 8-10.

[6] Lonsdale, D.J. (2004) The Nature of War in the Information Age: Clausewitzian Future. Frank Cass, London, 135.

[7] Garrison, L. and Martin, G. (2001) Cyberterrorism: An Evolving Concept. Highlights.

[8] Verton, D. (2003) Black Ice: The Invisible Threat of Cyber-Terrorism. McGraw-Hill/Osborne, New York.

[9] Charmaz, K. (2006) Constructing Grounded Theory. Sage Publications, London.

[10] Bryant, A. and Kathy, C. (2007) Grounded Theory Research: Methods and Practices. In: Bryant, A. and Charmaz, K., Eds., *The Sage Handbook of Grounded Theory*, Sage Publications Ltd, Thousand Oaks.

[11] Bryant, A. and Charmaz, K. (2007) The Sage Handbook of Grounded Theory. SAGE, London.

[12] Strauss, A.L. (1987) Qualitative Analysis for Social Scientists. Cambridge University Press, Cambridge.

[13] Corbin, J. and Strauss, A. (2008) Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Sage.

[14] La Rossa, R. (2005) Grounded Theory Methods and Qualitative Family Research. *Journal of Marriage and Family*, **67**. http://dx.doi.org/10.1111/j.1741-3737.2005.00179.x

Appendix

Table A1. A summary of the macro category, categories and codes of the study.

Macro-Category	Categories	Codes	
Awareness	Importance of awareness	Understanding the risks	Preparedness
		Anticipate risks	
	Types of awareness	Thorough awareness	Situational awareness
	Good and bad awareness	Right level of awareness	Fear and paranoia
		Effective of awareness	Denial and complacency

Table A2. Examples of initial codes of study interviews.

Participant category	A1	A2	B1	D1	D2	F1	Related area
Reliance	Operations built on networks	Electronic nature of work	Cessation of operations when there is a defect in Information Systems	Most citizen Services are offered online	Rapid transformation into technical	Locating accidents by Smart comprehensive databases	Cyberspace
Security	Increasing intrusions	Development of protection measures	Access to SCADA	Breakthrough government websites	Maintaining access information	Repetitive false alarms	
Trust	Not to be trusted	Probability of access to critical information	Need for continuous updating	Only for administrative services	"*Necessary evil*"	If there is an alternative option	Cyberterrorism conventional terrorism
Threat	Underestimated threat	-Renewed threat -Threat sources	-Same threats -Still under threat	Exaggerated Threat	Non-comparative threats	Changing nature of the threat	
Awareness	Perception level	Educational programmes	Personal responsibility	Means of awareness	Attention of the organisation	Media and awareness	
Impact	Impact assessment	High influence	Diverse impacts	National impacts	Psychological impact	-Limited effects -Bearable	
Role	Vital role of the organisation	Daily necessities	Major national income	-"*Indispensable*" -"*Irreplaceable*"	Security stability	n/a	
Cooperation	Coordination	Information/ Expertise exchange	Domestic/ International Cooperation	Joint body	Individual/ Everyone responsibility	Crisis management	National security
Strategy	Reforms	Research and Studies	Continuous development	Recruiting hackers	Intellectual security	Renounce extremism	
Geopolitics	Neighbouring countries	Cross-border force	Energy sources	Historical ideological antagonism	"*Arab Spring*"	Sanctities	

SCADA (Supervisory Control and Data Acquisition) in industrial control systems.

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.