2018

# Developing a Cyberterrorism Policy: Incorporating Individual Values

Osama Bassam J. Rabie
*Virginia Commonwealth University*

## Developing a Cyberterrorism Policy: Incorporating Individual Values

By: Osama Bassam J. Rabie, Ph.D. Candidate

Dissertation Committee Chair:

Prof. Heinz Weistroffer, Professor at Department of Information Systems, School of Business, Virginia Commonwealth University, Richmond, Virginia, United States of America

Dissertation Committee Co-Chair:

Prof. Gurpreet Dhillon, Professor and Department Head at Department of Information Systems and Supply Chain Management, Bryan School of Business and Economics, University of North Carolina at Greensboro, Greensboro, North Carolina, United States of America

Dissertation Committee Members:

- Dr. Lemuria Carter, Associate Professor and Chair at Department of Information Systems, School of Business, Virginia Commonwealth University, Richmond, Virginia, United States of America
- Dr. Manu Gupta, Associate Professor at Department of Finance, Insurance and Real Estate, Virginia Commonwealth University, Richmond, Virginia, United States of America
- Dr. Romilla Syed, Assistant Professor of Management Science and Information Systems, University of Massachusetts Boston, Boston, Massachusetts, United States of America

## Acknowledgement

I dedicate this dissertation to God then to all who supported me.

## TABLE OF CONTENTS

# LIST OF TABLES

## Abstract

DEVELOPING A CYBERTERRORISM POLICY: INCORPORATING INDIVIDUAL VALUES

By Osama Bassam J. Rabie, Ph.D. of Business with a concentration in Information Systems Fall 2014 – Spring 2018

A dissertation submitted in partial fulfilment of the requirements for the degree of Doctoral of Philosophy in Business at Virginia Commonwealth University

Virginia Commonwealth University, 2018

Chair: Prof. Heinz Weistroffer*

Co-Chair: Prof. Gurpreet Dhillon**

* Professor at Department of Information Systems, School of Business, Virginia Commonwealth University, Richmond, Virginia, United States of America

** Professor and Department Head at Department of Information Systems and Supply Chain Management, Bryan School of Business and Economics, University of North Carolina at Greensboro, Greensboro, North Carolina, United States of America

Preventing cyberterrorism is becoming a necessity for individuals, organizations, and governments. However, current policies focus on technical and managerial aspects without asking for experts and non-experts values and preferences for preventing cyberterrorism. This study employs value focused thinking and public value forum to bare strategic measures and alternatives for complex policy decisions for preventing cyberterrorism. The strategic measures and alternatives are per socio-technical process.

# Chapter 1: Introduction

“Ignorance leads to fear, fear leads to hate, and hate leads to violence. This is the equation.” – Abū l-Walīd Muḥammad Ibn Aḥmad Ibn Rushd (a.k.a. Averroes). Jarvis et al. (2014) state two reasons why cyberterrorism has risen to prominence; first, assigning cyberterrorism as potential risk after the collapse of the Soviet Union. It seems like humans want to always classify something as potential risk so, when the Soviet Union no longer existed, humans assigned cyberterrorism as potential risk. Second, security experts and political elites predicted that a terrorist can make more harm with a keyboard than with a bomb, because of the spread of the Internet and the interconnectivity it made possible.

In the United States of America, The President’s Information Technology Advisory Committee (PITAC) found that cybersecurity research community is too small to support cybersecurity educational programs and fundamental cybersecurity research (Benioff & Lazowska, 2005), thus, the size of cybersecurity research community is not sufficient and more scholars ought to do research on cyberterrorism. PITAC asked the Federal government to increase and sustain funding for cybersecurity research to encourage the increment of the size of cybersecurity community. The National Coordination Office for Information Technology Research and Development’s report said that cybersecurity needs to have new development methods that include solutions to improve the design and engineering of secure systems. The report asks cybersecurity research community to discover best practices to sustain the security of a system and discuss socio-technical issues of cybersecurity. This dissertation proposal method of designing and engineering secure systems employees value-focused thinking and value theory, hence, it is different than methods usually used in designing and developing secure systems. This study is neutral; it does not praise certain beliefs over others, nor it picks a side of certain conflicts and ideologies the study describes. It is simply seeking to discover an objective truth, as Al-Farabi said "truth is universal" (Najjar, 1964).

During Kosovo War, government and nongovernment actors used the web to support their positions by propaganda, yet common people could share their stories on the web without the need to be on TV or radio stations. Several scholars consider Kosovo War the first war that used the web as a medium to serve political war agenda (Denning, 2001). In addition, hackers hacked governmental computers and websites to condemn Yugoslav and NATO aggression. NATO did not bomb ISPs to help the spread of content condemning Milosevic regime, thus, supporting the NATO's operation (Denning, 2001). Hence, by using the web to support a side during the conflict over Kosovo, it has shown the effectiveness and potential of using the web to support war effort since the infancy of the web.

Using cyber technology to promote and help political agenda is becoming more influential than the 1990s. Moreover, the assertation of political agenda by using cyberterrorism is growing and it will become a permanent part of political movements. Per Washington Post (Williams, 2017), hackers were able to hack into 123 of 187 network video recorders in a closed-circuit TV system. These cameras belong to Washington D.C. police department. The hack happened eight days before President Trump's inauguration. The hackers used forms of ransomware to disable recoding between January 12 and January 15. Per Archana Vemulapalli, the city's Chief Technology Officer, the city did not pay the ransom, but had to go reinstallation efforts. This is an example of who hackers can access surveillance cameras and can watch public places across a city.

The internet is one of the most convenient communication tools. A special attribute that sets the internet apart from other communication tools is its usability. All types of people can share their thoughts over the internet through words, images, sound, and/or video. The internet is also the first medium with at once accessible dissemination materials that are available 24/7. People can post any audiovisual material on the web and contribute to other posts dialogically. Therefore, the internet is the biggest source of information that individuals can now reach. The social aspect of terrorists urges them to use existing technology of cyber-attacks to conduct cyberterrorism. Additionally, experts suggest that the wars are going to include cyberattacks along with conventional military attacks. Per Ferguson et al. (2011), cyber security is mainly about trusting several people to access the system and preventing others and trust has several sources:

1) Ethics that influence society and cause people to behave ethically most of the time;
2) Caring about self-reputation;
3) Consideration of legal consequences;
4) Fear of physical harm upon mistrust;

5) Being in a mutually assured destruction situation where upon mistrust the victim will oppress and harm the person she mistrusts.

Regrettably, the research on the socio-technological aspects of cyberterrorism does not match the size of the issue. There are over 31,300 magazine and journal articles written on cyberterrorism. However, there is not enough literature and practices about what to do in the case of cyberterrorism.

Another security challenge is the technical aspect of information security. The enhancement and obtain of cyberspace technologies are at a faster rate than the security systems built to protect them (Conley-Ware, 2010). In addition, the use of these cyberspace technologies is changing faster so that it is harder for the developers of security systems to adjust their systems to accommodate. This issue happens because there are more apps developers than security systems developers, thus, offering more creative and nimble fields to accommodate the rate at which security systems developers develop. According to Wall Street Journal (Obama, 2016), nine out of ten Americans stated that they do not feel they have control over their personal information. In addition, more than 100 million Americans' personal data, e.g., credit-card information and medical records, compromised in recent years. President Barack Obama's budget proposal for the 2017 fiscal year seeks $19 billion for cyber security across the U.S. government, a surge of $5 billion over 2016 (Reuters, 2016).

“Security… it’s simply the recognition that changes will take place and the knowledge that you’re willing to deal with whatever happens” Harry Browne as quoted in (Dhillon, 2015). There are three purposes of Information security (Dhillon, 2015). First, an information systems designer should prevent any access without proper authority and support confidentiality of disclosed information. Second, information integrity within a system assures effective functionality and integrity of modified information. Finally, information systems security offers availability and accessibility to users during the time of their security privileges. As with any form of media, the content on the internet must be regulated. The web holds content that needs to be removed because of its potential harmfulness. The most notable example of this type of post is the ideas of terrorists, which overtly ask for people to attack a target constituency. This type of information dissemination is known as cyberterrorism.

Cyberterrorism consists of two words cyber and terrorism. The word cyber refers to the use of cyber space via digital means. The word terrorism is vague and has different connotations depending on the perspective of the definition. This article will use the term terrorism to refer specifically to any violent act conducted by followers of any ideology. Per Kramer (Kramer, 2002), the definition of terrorism can be broad and does not distinguish between terrorism and other crimes. It can also be specific meaning many will not accept its existence. Violent attacks are deemed terrorist or patriotic based on history and background. For example, Afghan Mujahideen, in the 1980s were considered libertarians by Kingdom of Saudi Arabia and terrorists by Union of Soviet Socialist

Republics. Moreover, the classification of groups as terrorist and patriotic can change. It is influenced by "perspective, political motivations, and agenda of the observer" (Kramer, 2002). Through the history there are political groups that were classified as terrorist groups only to later be classified as libertarians, e.g., Provisional Irish Republican Army (IRA). On the other hand, several groups were classified as patriotic to later be classified as terrorist, e.g., the Ku Klux Klan (KKK).

This study defines cyberterrorism as the use of cyberspace via digital means to serve the ideology of violent followers including propaganda, recruitment and training, fundraising, communication, and hacking. This definition focuses on the acts not on the actors. Anyone can become a cyberterrorist if they carry on the acts of cyberterrorism regardless of the group they identify with. Per Kramer (Kramer, 2002), the act of terrorism can be done to deliver a message. Jarvis, Nouri, and Whiting (Jarvis, Nouri, & Whiting, 2014) states that cyberterrorism definition should reconcile cyber acts with characteristics of terrorism. The definition of cyberterrorism in this study reconciles cyber acts with characteristics of terrorism, thus it is a correct definition of cyberterrorism based on the criteria by Jarvis, Nouri, and Whiting. Cyberterrorism is a social and security threat (Conley-Ware, 2010). It is different than terrorism in the sense that terrorism does not necessarily use the cyber space to serve violent followers of any ideology in regard to propaganda, recruitment and training, fundraising, communication, and targeting. Terrorism implements it attacks in the physical world not the virtual. Nonetheless, terrorists can use cyberterrorism and terrorism at the same time, e.g., they can communicate via cyberspace with their people on the ground while they are carrying on their terrorist operation.

There are many practices on what people should do in the case of fire or atomic bomb. However, there is not enough literature and standards about what to do in the case of cyberterrorism. The lack of standards to prevent cyberterrorism is alarming. Experts suggest that the wars are going to include cyberattacks along with conventional military attacks. The majority of research in information systems security does not focus on the human aspect of security; it focuses on the "formal automated part of an information system" (Dhillon & Backhouse, 2001). According to (Dhillon & Backhouse, 2001), focusing on the formal automated part of an information system works for organizations that have the traditional hierarchy. It assumes that all members of an organization are trustworthy and knowledgeable to be responsible for maintaining security. This strict hierarchy works for military. It does not function well with the new socio-organizational perspective of involving employees in decision-making and assigning responsibility. Narrowing the focus on the technical aspect of information systems security is a liability that might cause it to be ineffective or vulnerable to security flaws. The new technology-interdependent culture requires research in information systems security to consider the human factor and build security around the user. Developing public policy based on public opinion to be used by individuals goes a long way to ensuring the involvement of the human factor in preventing cyberterrorism.

Keeney (1999) stated that using fundamental and means objectives can reveal different perceptions of the value of the same internet purchase among different customers of internet commerce. Based on this line of argumentation, logically categorizing objectives into means and fundamental objectives and showing their relationships can reveals different intimate perceptions of how to prevent cyberterrorism amongst internet users. The perceived value of preventing cyberterrorism can be different among different internet users. One may consider the development of governmental counter-cyberterrorism competencies as invading her privacy, while another may find it important for preventing cyberterrorism.

"It is better to concentrate our efforts on high-level application of policies and principles as opposed to detailed specifications" (Aiken, 2010). Organizations and governments need communication using the internet as a communication medium. Preventing cyberterrorism by not using the internet is an impractical solution because of the dependency on the internet. Therefore, data collectors should elicit values to apply to design security policy and security measures to this medium. To this end, this paper present information to practitioners and researchers to provide them with the measures to use to prevent cyberterrorism in such a manner.

People tend to ignore the cyber threats despite it can have serious consequences. Per Jones, Chin, and Aiken (Jones, Chin, & Aiken, 2014), a high percentage of five hundred undergraduate students at a regional public university were ignoring the potential risk when using their smart phones.  Jones, Chin, and Aiken concluded that increasing the awareness of these students about potential risks will motivate them to employ security measures.  This study offers awareness about objectives that prevent cyberterrorism. Contribution of this study is deriving values in the generic form from interviews about the individuals' perception on how to prevent cyberterrorism at personal, organizational, and governmental levels.  Then, logically categorizing these objectives into means and fundamental objectives and show their relationships.  These results explain the concerns that individuals have about cyberterrorism.  In addition, they show how these objectives relate and connect to one another.  These objectives apply to design security policy and security measures.

The rest of this study is structured as follows; In chapter 2 a review of the literature takes place, describing important aspects of IS literature relevant to this study.  The third section discusses the proposed methodological process for extracting the necessary values and converting them to cyber-terrorism prevention objectives.  The fourth chapter presents both the fundamental and means objectives for preventing cyberterrorism.  Lastly, the fifth chapter provides a final discussion of the implications of this research as well as proposed future directions and any limitations of this work.

### 1.1. Problem Domain: The relationship between technology and terrorism

The availability of the web caused technology to become cheaper and that increased technology adaption.  The availability of technology meant that terrorists may use it to support their causes as they use means available to them to support their causes. Cyber attacking and online recruiting are two means by terrorists to carry their operations.

### 1.2. Research Argument and Proposed Research Questions

Anderson (2015) says that despite the lack of experience of young scientists they can solve scientific questions that seasoned scientists are unable to solve. Anderson's reassurance to young scientists about their abilities to tackle challenging questions inspired me to tackle two of the hardest scientific questions. Additionally, my dissertation committee and I decided to tackle those research questions well knowingly that they are hard to answer. Replicating existing research is safer than tackling new prospective of security research. However, Alter (2015) says adding to the body of knowledge requires the courage to tackle new scientific prospective. Alter say replicating research prevents scientific advancement.

Cyberterrorism is a major threat to national and international security on all levels; personal, organizational, and governmental. Being at University of Washington, Seattle and seeing the Space Needle, I ask for the rationality of having six floors at 605.0 ft tall building. Since I was a student at University of Washington, Seattle, I saw that using the area between the floors increases the practicality of the Space Needle (figure 1.2.1). This study proposal fills several gaps in the area of cyberterrorism prevention to increase the practicality of that field. Many proposals that focused only on technology had failed to ensure cybersecurity against cyberterrorism. These proposals did not employee the prospective of the users and their perceived value of cybersecurity. Current literature on cyberterrorism prevention focuses on isolated fragments of cyberterrorism prevention and do not seem to use the area connecting these chunks. That is several literatures talk about four aspects conceptualization of cyberterrorism, technological measures for preventing cyberterrorism, policy for preventing cyberterrorism, and assessment of cyberterrorism prevention means.

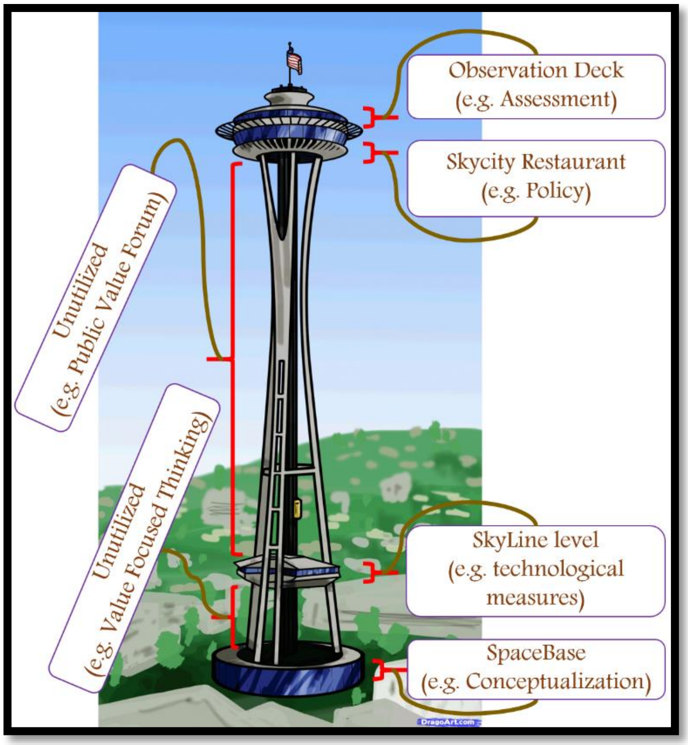

**Figure 1.2.1. Explaining the State of Literature on Cyberterrorism Prevention Using the Usage of Space Needle at Seattle, Washington, United States of America**

First, conceptualization of cyberterrorism includes cyberterrorism definition and that controversial since it depends on the belief of the definer. In addition, it theorizes about what the motivation behind cyberterrorism and that discussion usually yields to say that social impact of cyberterrorism, e.g., fear that change the political decision of the government of that society, is the reason and motivation of cyberterrorism. Second, technical literature focuses on developing algorithms and applications to help securing information systems, tracking cyberterrorists, assessing security measures, and training employees. Experts participate in this study say that the usefulness of these innovations, e.g. Supervisory Control And Data Acquisition (SCADA), depends on other factors, e.g., developing competencies for dealing with cyber terrorism activities of training, policy, and decision making. Third, literature that proposes policy for preventing cyberterrorism. However, policies that are for general information systems security and not specifically for cyberterrorism prevention derive policies these literatures propose. Additionally, they assume based on their experience what clients need in a policy for preventing cyberterrorism. Moreover, these policies communicate with system officer and technical personal without addressing common user. Fourth, literature assessing the preventing of cyberterrorism. However, these literatures are a route to propose new technical measures or new prevention policies.

Implementing an application or policies that are not based on the perceived value of the users of these applications or policies had proven to be ineffective against insider's attacks and misconduct. Several cyberterrorism attacks were successful not because of lack of security applications or policies, but because these applications' and policies' misrepresentation and appeal to their users' values. This study proposes using the perceived values of the users of information systems. The users express their values for preventing cyberterrorism on personal, organizational, and governmental levels. The premise is that using these values will result in objectives for preventing cyberterrorism that represent and appeal to the users' values more than other proposals. The result should give researchers and practitioners list of values that is effective for preventing cyberterrorism and users will follow.

1) What are cyberterrorism prevention objectives?

2) How to design public policy for cyberterrorism prevention?

    A) What are the objectives for preventing cyberterrorism?

    B) How could a decision maker prioritize those objectives?

3) How to build decision model that uses values to reach decision?

The study produces a policy specifically and uses objectives to prevent cyberterrorism. Policies literature propose tend to be general and do not meet the need to prevent cyberterrorism. Using the value focused thinking of Keeney (1993) helps in developing frameworks with prioritization and tailor to address a specific policy problem (Mishra & Dhillon, 2007).

### 1.3. The Impact of Cyberterrorism

Cyberterrorism has devastating impact on society by terrifying people and recruiting them to serve cyberterrorists agenda. In addition, it has economic impact that drains resources of individuals, organizations, and governments that affected by cyberterrorism acts. Cyberterrorism endangers properties and lives and invades privacy of individuals, organizations, and governments. Organizations and governments can lose resources and infrastructures from cyberterrorism attacks. (Hua & Bapna, 2013) used game theory to reveal that securing organizations handling infrastructure is a matter of national security, thus, organizations should invest heavily in information security. Per (Gross, Canetti, & Vashdi, 2017), cyberterrorism has psychological and cognitive effects on individuals like psychological and cognitive effects on individuals of other types of terrorism.

### 1.4. Study Structure

In section one, the outline of the research nature, impact, and concept. Section one also outlines the research questions and establishes them. Section two reviews and evaluates literature of cyberterrorism prevention including definitions, proposals, and gaps. Section three establishes the theoretical basis for addressing the research questions and discusses the proposal to use objectives to establish public policy design for cyberterrorism prevention. Section four shows the process of establishing and revealing the objectives for cyberterrorism prevention. In addition, section four shows the objectives for cyberterrorism prevention. Section five demonstrates how to use of the objectives from section four to create a decision model for alternatives of cyberterrorism prevention. Section six discusses the impact and implementation of this study for from the prospective of practitioners and researchers. Section seven concludes this study and summarizes its implementation, impact, and result.

### 1.5. Research Contribution:

This research fills the gap that cyberterrorism prevention does not have a public policy or public value forum. This study has several contributions including:

1) Revealing goals;

2) Evolving decision alternatives for single decisionmaker and multiple decisionmakers;

3) Finding decision opportunities.

This study uses (Ralph L. Keeney, 1992) method through using four steps (figure 2.4.1)

1) Qualitative thinking to find and structure goals of the value focused thinking;

2) Quantitative thinking to give values to the goals;

3) That reveals decision alternatives of public policy;

4) Decisionmakers have value focused decision-making process.

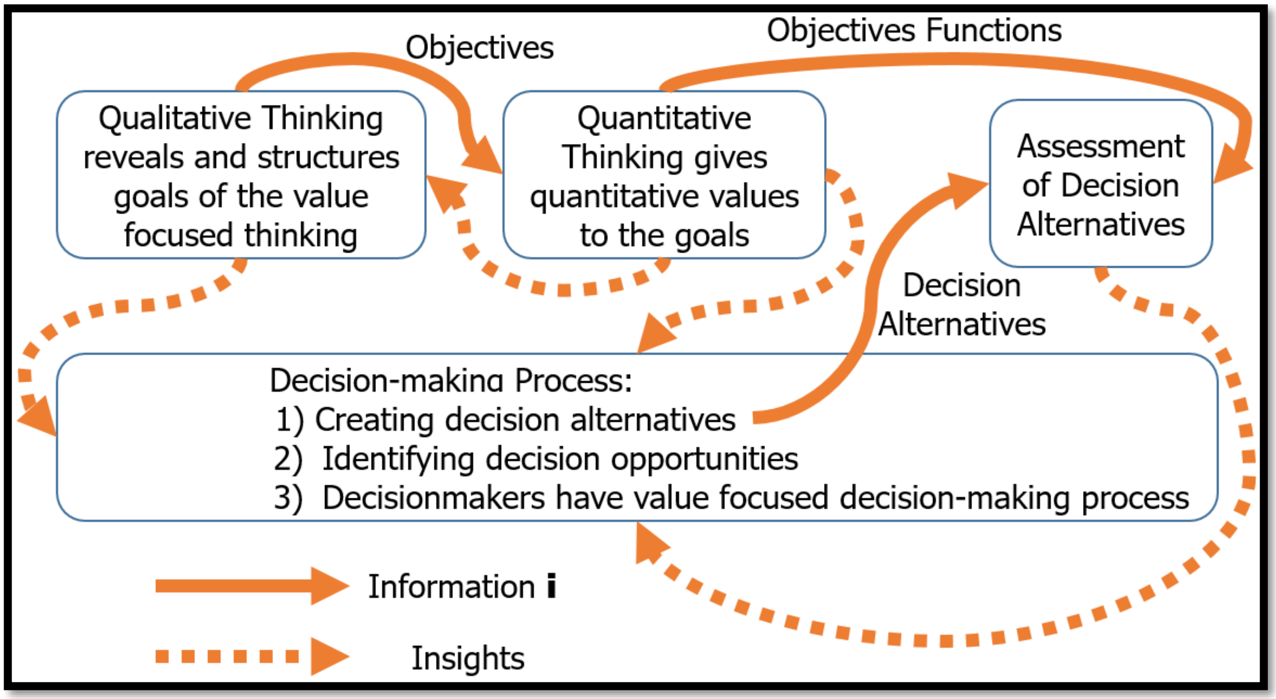
Objectives
Objectives Functions
Qualitative Thinking reveals and structures goals of the value focused thinking
Quantitative Thinking gives quantitative values to the goals
Assessment of Decision Alternatives
Decision Alternatives
Decision-makina Process:
1) Creating decision alternatives
2) Identifying decision opportunities
3) Decisionmakers have value focused decision-making process
Information i
Insights

**Figure 1.5.1. The Process of Value Focused Thinking (Ralph L. Keeney, 1992)**

The paper uses interviews, which are qualitative thinking, to provoke goals for preventing cyberterrorism. Next, it uses qualitative analysis of interview transcripts to formulates the structure of goals for preventing cyberterrorism.

### 1.5.1. Revealing Goals

Attributes of a goal or objective is a list where an attribute defines an aspect and functionality of the objective. Per (Ralph L. Keeney, 1992), attributes can reveal more aspects of an objective and specify components of an objective. Decisionmakers can use attributes to reveal decision alternatives.

In addition to define their objectives, users of value focused thinking use attributes to measure how much their objective applies them.  An objective is valid if it is applying its attributes.  However, an objective without its attributes can have several meanings which can make decision alternatives unclear and open for interpretations by decisionmakers. An important use of attributes that they specify the definition of their objective, thus, allows for one meaning of the objective instead of multiple meanings.

### 1.5.2.  Evolving Decision Alternatives

Decisionmakers make better decision based on available decision alternatives.  Decision alternatives should be clear to help decisionmakers make informed decision.

## Chapter 2: Informing Literature

### 2.1. What is Cyberterrorism?

In this section, the definitions of cyber terrorism. Although few scholars have noted the difficulties in defining cyberterrorism (Jarvis et al., 2014 and Jarvis & Macdonald, 2015), the definitions identified in the extant literature are listed in table 2.1.1, define cyberterrorism is the use of cyberspace via digital means to serve the ideology of violent followers including propaganda, recruitment and training, fundraising, communication, and hacking.

The term cyberterrorism existed since the 1980s (Jarvis & Macdonald, 2015). However, Jarvis and Macdonald found that despite the importance of defining cyberterrorism, there is no definition that satisfies policymakers or researchers. Their study found that whether a cyber-attack may be described as cyberterrorism depends on the means of an attack more than the kind of target or digital preparation of an attack. They concluded, however, that disagreeing on the definition of cyberterrorism is important in assessing and reconsidering the understandings of terrorism itself.

For example, several authors divide cyberterrorism to two types; pure and other types. Pure cyberterrorism consists of cyberattacks targeting digital assets and via digital means. On the other hand, other types of cyberterrorism use cyberspace to incorporate propaganda or fundraising. Jarvis et al. (2014) divide cyberterrorism to preparation (like target surveillance), conduct (like virus release), and consequence (like technology damage). The definition used by this study includes cyberterrorism's preparation, conduct, and consequence. Moreover, the definition used by this study includes politically motivated acts and non-politically motivated acts. Therefore, it goes a step further than the definition offered by Jarvis, Nouri, and Whiting. Not narrowing cyberterrorism to political motivation is better since the existence of political affiliation does not seem to matter when labeling a cyber act as cyberterrorist.

This literature review uses articles and books obtained from VCU Libraries, Microsoft Academic, and Google Scholar. The search terms included "cyberterrorism" and “cyberwarfare.” Articles that do not focus on cyberterrorism were eliminated from the review. Table 1 summarizes main studies presented in the literature review.

The term cyberterrorism existed since the 1980s (Jarvis & Macdonald, 2015). However, Jarvis and Macdonald found that despite the importance of defining cyberterrorism, there is no definition that satisfies policymakers or researchers. Their study found that whether a cyber-attack may be described as cyberterrorism depends on the means of an attack more than the kind of target or digital preparation of an attack. They concluded, however, that disagreeing on the definition of cyberterrorism is important in assessing and reconsidering the understandings of terrorism itself.

**Table 2.1.1. List of Cyberterrorism Definitions Per Several Literatures**

| Article | Definition |
|---|---|
| Hansen, Lowry, Meservy, & McDonald, 2007 | Cyberterrorism is the use of hacking techniques by politically motivated group of people to spread fear and influence public and decision makers |
| Denning, 2001 | Cyberterrorism as the use of cyberspace to carry terrorist activities |
| Kramer, 2002 | Cyberterrorism is defined as the cyber activities of terrorists. However, she said that defining terrorism is not important to prevent it. Terrorism is psychological warfare conducted by politically motivated group of people, but it is debatable if terrorism should be defined by the acts or actors |
| Van Hoogenstyn, 2007 | "[T]he use of the computers and networks to execute a terrorist attack" (Van Hoogenstyn, 2007) |
| Fuentes, 2016 | Cyberterrorism is defined as the use of cyberspace to further terrorists' objectives. She said Fuentes notes that the intention of the actor to conduct cyberterrorism makes him cyberterrorist |
| Conway, 2011 | Cyberterrorists are terrorists using the Net |
| Weimann, 2004 and 2005 | "[T]he use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)" (Weimann, 2005)<br>In his 2004, Weimann notes the use includes eight activities: psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, sharing information, and planning and coordination |
| Gordon & Ford, 2002 | Gordon & Ford (2002) insist that cyberterrorism should be defined as a type of terrorism and without fragmenting the definition of cyberterrorism and terrorism. They note two two issues in Denning's (2001) definition: first, it is limited to causing harm through cyber hacking (pure cyberterrorism) and second, it is different than the operation definition used by the media and the public. They propose not to define cyberterrorism, but rather, "breaking it down into its fundamental elements" (Gordon & Ford, 2002) that constitutes the technical, legal, social, educational, or policy driven of cyberterrorism. They suggest using terrorism matrix to find terrorist act. The matrix includes perpetrator, place, action, tool target, affiliation, and motivation |
| Embar-Seddon, 2002 | Terrorists may use cyberterrorism along with traditional terrorist attack to manipulate media, gain supporters, and increase the damage of the traditional terrorist attack |

Although cyberterrorism is not limited to intrusion, intrusion detection will block a major operation of cyberterrorism (Hansen, Lowry, Meservy, & McDonald, 2007) since this form of protection can (at least) inform organizations of intrusion before they see significant damage. Terrorists can enter systems and alter information, destroy crucial files, create false identities, and so forth (Hansen et al., 2007). In other words, terrorists will do anything they can to complete their task and/or send their message.

Potential threats to power plants, as analyzed by the United States Government Accountability Office (Protection, 2004), come in the following categories.

- Crackers: the highly skilled hackers who use outside computers to enter a system
- Insiders: they may be employees or outsourcing organizations. They do not need special skill to access their company's/contractor's protected system because they often have enough permission to access related areas. According to Dhillon, Syed, and de Sá-Soares (Dhillon, Syed, & de Sá-Soares, 2017), organization and vendor should agree on three essential requirements before the organization outsource its operations to the vendor: first, vendor's ability to ensure the security of information; second, vendor should comply with the organizational and external regulations and policies; third, vendor should ensure that the information will not be abused.
- Malware writers: people who write or create programs to harm specific systems
- Organized crime: a group of people with intrusion skills that may bond together to harm an organization
- Terrorist groups: people who may attack people or property by using the internet. The damage itself is the means to an end, which is to send a threatening message about the group's power and potential
- Hacktivists: politically motivated people who may attack people or property by using the internet to send a message
- Information warfare: nations or organizations those are eager to gain information through illegal means to secure competitive advantage.

Due to the vast amount of information on these websites, manual analysis of the content is impossible, high-level policy and automated software is the only practical choice (Qina, Zhoub, Reidc, Laid, & Chenc, 2007). The first thing to do to study and analyze terrorists' websites is to store their contents in a repository (Qina et al., 2007) that any artificial intelligence applications can use for analysis and observing tasks.

In her chapter, Denning (2001) distinguishes between activism, hacktivism, and cyberterrorism based on activities and focuses on activities by non-state individuals and organizations that may influence foreign policy. She defines activism as using the web to ask for support for activist's position through spreading and gathering of information over the web and email. She defines hacktivism as activism using hacking, thus, it is the use of hacking techniques to support activist's position without causing severe damage. She defines cyberterrorism as the use of cyberspace to carry terrorist activities. Although Denning categorized the activities in three classes, she acknowledges that "boundaries between them are somewhat fuzzy" (Denning, 2001).

Therefore, affiliation influences the categorization of certain activities and an individual can play all three roles. Denning regards activists as more effective in carrying out their foreign policy goals than hacktivists and cyberterrorists, and she offers examples from the Kosovo conflict, cryptography policy, human rights in China, support for the Mexican Zapatistas, and other areas of conflict. Additionally, Despite the difference between the web and the internet, Denning used the two terms as exchangeable throughout her chapter and used the term internet when it should be web.

Kramer's dissertation (2002) studied the way terrorists use the internet. The challenge is having networked terrorists using cyberspace to facilitate their operations. In doing so geographical boundaries do not restrict them, thus, they decentralize their command to make it more resilience to counter terrorism efforts. In addition, she claims there is a lake of understanding of the definition of terrorism.

Her study investigated thirty-six groups that the U.S. State Department named as Foreign Terrorist Organizations. She analyzed the content of their websites. She found that their websites focus on "emotionally compelling language or images" (Kramer, 2002) to propagandize about the group's mission. She said that these websites serve as a communication tool between their members and outreaching media to improve their public image.

Kramer acknowledged that the classification of what is terrorism and what is not depends on the classifier's perception and side. In addition, it is hard to find a unified definition of terrorism that scholars and governments can accept and distinguishes terrorism from other crimes. She said that it is controversial to name an organization as terrorist or activist like classifying Irish Republican Army (IRA) or Palestinian Liberation Organization (PLO) as terrorist organization or political activist.

In his thesis, Van Hoogenstyn (2007) "examined media exposure, knowledge of cyberterrorism, fear of terrorism and perceived seriousness of cyberterrorist." Van Hoogenstyn (2007) stated that, despite the threat of cyberterrorism, there are many factual misconceptions in the media about the nature of cyberterrorism. The thesis measured these factors by conducting survey of college students: participant's media consumption, participant's fear of terrorism, participant's knowledge of cyberterrorism, and participant's perceived seriousness of cyberterrorism. The survey measures the effect of media consumption on knowledge of cyberterrorism and perceived seriousness of cyberterrorism. In addition, it measures the relation between perceived seriousness of cyberterrorism and fear of terrorism.

Van Hoogenstyn's thesis found that women are more fearful than men when it comes to terrorism and cyberterrorism. The thesis justifies that by saying that women are more aware of terrorist and cyberterrorist events due their higher consumption of related news media. In addition, the thesis found that fear of terrorism and perceived seriousness of cyberterrorism are positively related. It explained that terrorism has a psychological effect of the people, for example, Americans reported having more anxiety disorders at the first anniversary of September 11 attacks. It used a paper that related the dramatic media attention with having an increment in Americans reporting anxiety disorders, thus, thesis has the premise that if a group of people consumes media then they will have more fear. However, the thesis did not use extensive literature to justify the use of the instrument of analysis.

Per Fuentes master's capstone project Fuentes (2016), cyberterrorism is defined as the use of cyberspace to further terrorists' objectives. She said Fuentes notes that the intention of the actor to conduct cyberterrorism makes him cyberterrorist.
According to Conway (2011), cyberterrorism is the use of the Net by terrorists to achieve their politically motivated goals.

Weimann (Weimann, 2004; G. Weimann, 2005) stated that, "the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)" (G. Weimann, 2005). In his 2004, Weimann notes the use includes eight activities: psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, sharing information, and planning and coordination.

Based on Gordon and Ford (2002), cyberterrorism is a type of terrorism and without fragmenting the definition of cyberterrorism and terrorism. They said that Denning's definition raises two issues: first, it does not embrace to causing harm through cyber hacking and second; it is different than the operation definition used by the media and the public. They propose not to define cyberterrorism, but rather, "breaking it down into its fundamental elements" (Gordon & Ford, 2002) that constitutes the technical, legal, social, educational, or policy driven of cyberterrorism. They suggest using terrorism matrix to find terrorist act and their matrix includes perpetrator, place, action, tool target, affiliation, and motivation.

Once studies set up how to defend infrastructures, governments can prioritize which structures to defend and how to defend them. It is the main responsibility of each government to insure the security of its people and their access to necessities. Attacks on critical infrastructure can result in loss of lives or irreversible damages.

As does any illegal organization or groups of people, terrorists capitalize on the vulnerabilities in different legal systems to carry out their activities. The internet has undergone steady assaults of hacking for more than fifteen years, and hackers infiltrate systems for various reasons: cybercrime, stealing information, send a message, etc. (Furnell et al., 2001). Terrorist hackers find ways to send information to their target audiences while covering their tracks to avoid government control. Estimation shows that the number of hacker attacks between 2005 and 2006 is higher than the number of total hacking attacks in the previous twenty-five years (Adam & Ofori-Amanfo, 2000).

The year 2005 marks the moment when different software and hardware vendors began to produce products specifically for the internet. It makes sense that a higher number of internet products create a higher number of vulnerabilities in products, especially when many vendors are unaware of security measurements. Due to their illegal nature and their involvement of highly sensitive information, it is difficult for companies to obtain information about hackers and their attacks (Adam & Ofori-Amanfo, 2000). Moreover, most hacker attacks are sudden and undetected before they complete their damage to catch companies off guard. It is difficult to understand the reason for hacking, since it is always "obscure" and varies from intellectual, economic, and social motives (Papadimiyriou, 2009).

However, most of the terrorists, and people who similarly have a message to send, claim responsibilities for their actions. Most hackers follow place anonymity as a part of their hacking activity so that companies cannot strategize against them. The literature suggests five main psychological reasons for hacking:

- An uncompromising belief in the freedom of access to all information (Wark, 2004);
- Dissatisfaction with an employee for whatever reason (Bainbridge, 1997)
- Age: hackers are usually young people who feel freedom from their family and society when they hack (Yar, 2005);
- Personality also plays a role in the mentality of hacker: for example, in January of 2006, a twenty-five-year-old French man was arrested after hacking several websites for his own pleasure, according to his account (Filiol & Richard, 2006); and
- Males are more likely to be hackers than females (Papadimiyriou, 2009).

Per Hardy and Williams (2014), United Kingdom (UK) defines terrorism in section 1 of Terrorism Act 2000 (TA2000). UK includes cyberterrorism in the legal definition of terrorism. TA2000 has three requirements for an act to qualify as terrorism. TA2000's definition of terrorism can be used to identify cyberterrorism. Therefore, cyberterrorism is the use or threat to use cyberspace that includes the following:

- Harm requirement: Includes violence against a person, damage to property, endanger to person's life, health or safety risks of the public, or interference or disruption of electronic system;
- Intention requirement: Where the intension of the design is to influence governmental organization or the public;
- Motive requirement: It is to advance a political, religious, racial, or ideological cause;
- Then it is an act of terrorism.

Per Hardy and Williams, the UK's legal definition of terrorism (TA2000) defines cyberterrorism legally in the UK. TA2000 criminalize supporting terrorists by posting propaganda online.

Per Hardy and Williams (Hardy & Williams, 2014), the legal definition of terrorism in the Australian criminal code legally defines cyberterrorism. The Australian criminal code used UK's TA2000 when drafting its own legal laws of terrorism. The Australian criminal code developed Security Legislation Amendment (Terrorism) Act 2002 which has three requirements for an act to be qualified as terrorism: intention, harm, and motive. There are several differences between the Australian criminal code and TA200. First, the motive requirement includes political, religious, or ideological cause and does not include racial cause. Second, the intention requirement is to intimidate the government of the Commonwealth or a State, Territory, or foreign country, or of part of a State, Territory, or foreign country.

However, Act 2002 exempts political protesters. Third, the harm requirement is for acts that cause personal harm, property damage, death, or life endanger. Harm requirement also includes the creation of risk to the health or safety of the public or the destruction of electronic system, e.g., information system, telecommunication system, financial system, e-government, public utility systems, or transportation system. The Australian criminal code criminalizes downloading schematics of power grids and other utilities. The Canadian Criminal Code developed the Anti-Terrorism Act 2001 (ATA) based on TA2000 (Hardy & Williams, 2014). ATA's motive requirement: an act or omission, in or outside Canada that is in whole or in part for a political, religious, or ideological purpose, objective or cause. However, ATA exempts political protesters.

ATA's harm requirement: an act or omission, in or outside Canada that intentionally causes death, harms a person by the use of violence, endangers a person's life, causes risk to the health or safety of the public, causes property damage, or "causes serious interference with or serious disruption of an essential service, facility or system, whether

public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm" (Hardy & Williams, 2014)
ATA's intention requirement: an act or omission, in or outside Canada that intimidating the public, or "with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada" (Hardy & Williams, 2014).

New Zealand legally defines terrorism in Terrorism Suppression Act 2002 (TSA) (Hardy & Williams, 2014). TSA's definition of terrorism legally defines cyberterrorism.

- TSA's motive requirement: an act to advance ideological, political, or religious cause;
- TSA's harm requirement: an act that causes death or injury, risk the health and safety of population, cause economic loss, cause environmental damage, disrupt an infrastructure facility, and engender human's life, or release a disease and harm the economy. However, TSA exempts acts occurring in armed conflicts and if a person "engages in any protest, advocacy, or dissent, or engages in any strike, lockout, or other industrial action, is not, by itself, a sufficient basis for inferring that the person" (Hardy & Williams, 2014) is a terrorist. In addition, TSA does not criminalize cyber-attacks that cause environmental or economic disruption if they do not endanger human lives;

- TSA's intention requirement: an act to terrorize people, force government or international organization to act in certain way.

## 2.2. Handling Cyberterrorism

In 2010, Conley-Ware's dissertation proposed a proof of concept model to discover vulnerabilities and threats cyberterrorists can use to commit the terrorist act. Conley-Ware (2010) claims that cyber-technologies are not intentionally with vulnerabilities and threats, however, terrorists manage to use them to commit the terrorist act. This study states that despite that developers of cyber-technologies may not have the intention to include vulnerabilities and threats, many of these technologies have vulnerabilities and threats that are adjustable.

The proposed model combines ideas from different disciplines to ensure its effectiveness. The model is from three disciplines: medical differential diagnosis (MDD) form clinical medicine, knowledge architectural modeling from knowledge management, and vulnerability detection and threat identification from crisis/risk reduction. MDD tools ate based on Decision Support Theory. Using these disciplines provides structured roadmap for detecting vulnerability and threat. In addition, using the three disciplines offer development and testing methods of the proposed model. Moreover, using development and testing methods from three disciplines can increase the results' validity. However, using multiple development and testing methods does not justify the conclusion; the conduction and reason of using these multiple development and testing methods can justify the results. The proposed methodology is CVCT KML (cyber-crime or cyber-terrorism knowledge model) methodology. CVCT KML methodology consists of three phases: first, developing the MDD knowledge model; second, using the MDD knowledge for CVCT domain; third, detecting CVCT risk and vulnerability.

However, the proposed methodology of Conley-Ware (2010) requires the availability of science and technical professionals each time the results evaluation is at the third phase. Middle and small organizations that want to conduct her methodology will encounter the challenge of availability of science and technical professionals each time for results evaluation at the third phase. This imposes a serious challenge to the practicality of the proposed methodology.

Fuentes (2016) proposed a guide for law enforcement to prevent terrorist from using social networking to recruit westerners. She found that terrorists are using social networking to recruit Westerners. She proposed that websites belong to terrorist groups can self-radicalize Westerners without the need for Westerners to communicate with these terrorist groups and without the need for physical interaction. She urges law enforcement to gain awareness and intelligence of terrorists' activities to prevent the threats of radicalizing Westerners. She stated that terrorists are focusing on using social networking to recruit Westerners rather than attacking infrastructure. She defines law enforcement based on the definition by Bureau of Justice Statistics in 2015 as agencies that use "prevention, detection, and investigation of crime and the apprehension of criminals" for sustaining the rule of law. She defines cyberterrorism as attacks against computers with the intension to help terrorist group.

Fuentes concluded her capstone with four recommendations: first, social networking websites to deactivate accounts associated with radical content. Second, governments and social networking websites should collaborate to identify these accounts. Third, more information sharing among governmental agencies using Information Sharing Environment (ISE). Fourth, train law enforcement on using social networking to find suspicious accounts and contents.

However, Fuentes (2016) did not offer enough evidence to prove terrorists are no longer planning to attack infrastructures and are focusing on recruiting Westerners through social networking. In addition, terrorists use social networking to recruit people from different backgrounds not only Westerners. They use social media to spread their propaganda. People from different backgrounds (not only westerners) use social networking, thus, terrorists use social networking to reach them. In addition, Fuentes (2016) defines cyberterrorism as an act of terrorism that transcending national boundaries, but her examples are focusing on certain group of people, i.e., non-westerner Muslims. Scholars should not name terrorism as a characteristic that is only related to non-westerner Muslims.

Based on Fuentes argument, Westerners are different from Jihadists. Nonetheless, a Westerner can become a terrorist and terrorists recruit westerners using social networking. Therefore, a westerner turned terrorist can use social networking to recruit other westerners. That is, unless she wants to argue that once a Westerner becomes a Jihadi she is no longer Western. This argument is invalid. It is better not to categorize a group of people as being terrorists.

Fuentes' (2016) definition of cyberterrorism focuses only on the intention to support a terrorist group. However, she did not offer a clear way to distinguish intention to harm from honest mistake and did not offer a definition of terrorist group that people from different backgrounds can agree upon.

### 2.3. Is Cyberterrorism Real?

In August 2012 and November 2016, Kingdome of Saudi Arabia faced major destructive malware attacks by Shamoon disk-wiping trojan and fresh wave of Shamoon attacks. However, few scholars like Conway (2011) suggest that cyberterrorism threat only exists in academia and contemporary media. Conway claims that it is unlikely to occur given it is statistically insignificant to be a victim of terrorism. She said that it is a part of the contemporary media's claim that technology will become the head and humankind the servant.

Conway and Weimann's psychological perspective (G. Weimann, 2005) behind the fear of cyberterrorism is that cyberterrorism combines the two modern fears of technology and terrorism. She has three arguments against the possibility of cyberterrorism. First, technology is complex and jihadis do not have the required IT knowledge. Moreover, only 4.5% of members of violent Islamist groups had trained in computing, thus, it is harder for them to carry successful cyberattacks. Second, often "real-world" attacks are hard to carry successfully. Therefore, there is a slim chance of success of virtual attacks. Third, based on the first and second arguments, terrorists might have to hire outsider hackers to carry out the hacks for them. However, this is operationally risky since terrorists would not be able to control the outsider hackers and would have to trust them.

However, back at the time of Conway's paper publication there were far fewer cyberterrorist attacks taking place. For example, she only mentioned the cyberattacks on Estonia in 2007 and Iran in 2010. Additionally, the sophistication of cyberterrorist attacks and the number of attacks has increased dramatically by the end of 2011 and moreover, several of these attacks were from servant countries. For example, In December 2012, a cyber-attack on Saudi Aramco that destroyed 35,000 computers within hours (Habboush et al., 2016). The attack caused difficulties of oil production to Aramco, which supplies a tenth of the world's oil (Reuters, 2012). Another example, On Thursday, December 1, 2016, the computer systems of Saudi Arabia's aviation agency was under cyber-attack by a malware called Shamoon, which targeted Saudi energy companies four years ago (Kerstetter, 2016).

Conway (2011) states that the chance of being a victim of terrorism attack is statically insignificant. Scholars may counter argue this point in three ways. First, the likelihood of being a victim of terrorism is statistically insignificant for certain group of people. For example, being a victim of terrorism is statistically insignificant for Saudis, but not for Palestinians, i.e., by looking at the murder rate. This research on cyberterrorism is for the sake of all humanity. Second, there is a difference between terrorism and cyberterrorism. This study defines cyberterrorism as using the cyber space to serve violent followers of any ideology in regards of propaganda, recruitment and training, fundraising, communication, and targeting. Based on that definition, cyberterrorism is more successful than terrorism. Terrorists' propaganda, recruitment and training, fundraising, communication, and targeting is among several countries across the globe.

Conway (2011) seemed to imply that terrorism is exclusive to Muslims. However, terrorism is not exclusive to certain group of people. There are several terrorists who are not Muslims like Wade Michael Page, who fatally shot six people and wounded four others before committing suicide at a Sikh temple in Wisconsin. Moreover, several people do not seem to fully understand the concept of Jihad. Jihad can be defined as discipline. By itself discipline is neither good or bad. It is what one disciplines herself to do is what makes it good or bad. For example, Muhammad Yunus disciplined himself to serve humanity, where Ted Bundy disciplined himself to kill people. Based on defining jihad as discipline, a student disciplining herself to study is jihadi.

Conway's (2011) paper did not seem to take into consideration humanity and it was before cyberterrorism became an alarming threat.  Hence, Conway (2011) said that cyberterrorism threat is made-up by contemporary media, however, this study suggests that cyberterrorism threat is a challenge to all humans.  In addition, Conway (2011), did not discuss Gordon's and Ford's (2002) new terrorist organizations that are highly funded and recruit groups with technical background that can use cyberterrorism to remotely attack a wide range of targets.

Per Weimann (2005), cyberterrorism is undeniable threat that should be addressed without exaggeration.  Challenges are best handled when people have a realistic understanding about their severity.  Overstating or understating the threat of cyberterrorism hinders the effort of preventing it.  Weimann (2005) said that forces of psychology, politics, and economy overstate the severity of cyberterrorism.  Weimann (2005) agrees with Denning (2001) that traditional terrorist attacks are more threating than cyberterrorism, but the severity of cyberterrorism may surprise people.  In addition, he agrees with her about the importance in distinguishing between cyberterrorism and hacktivism.  Weimann (2005) offers five reasons psychological, political, and economical forces promote overstating the threat of cyberterrorism:

- Based on psychological perspective, cyberterrorism combines the fear of becoming a victim in a random violent attack (terrorism) and the fear of artificial intelligence taking over humans (cyber);

- Mass media bombards consumers with fear tactics by using fearful headlines when discussing cyberterrorism;
- Ignorance and lack of understanding of technology and terrorism create the fear of the unknown;
- Politicians use the fear of cyberterrorism to use the public anxiety to advance their agenda;
- Economic benefit for security company and personal urge them to keep overstating the threat of cyberterrorism.

Weimann (2005) also offers five reasons cyberterrorism is appealing for terrorists:

- It is cheaper than traditional attacks;
- Cyberterrorism offers better anonymity than traditional terrorist methods;
- Cyberterrorism offers variety of targets to attack;
- It can be conducted remotely;
- It can affect more number of people than traditional terrorist methods.

Weimann (2005) said that vulnerabilities cyberterrorist attack can exploit are growing with the increase in demand of using cyberspace to handle civil, governmental, and military tasks. He makes a distinction between hackers and terrorists by categorizing hackers as thrill seekers that seek out the sense of bravado and generally do not damage systems, affect e-commerce, or take down websites. Per Weimann (2205), hackers are help software developers to discover security threats in their software to be able to fix.

On the other hand, Weimann categorizes terrorist as groups, states, and sympathizers that conduct cyberattacks to cause severe damage that can disrupt critical infrastructure because of political motivation.

Weimann (2005) takes more moderate approach by not denying the threat of cyberterrorism or exaggerating the severity of it. He promotes realistic understanding of cyberterrorism and its implications. However, he mentioned that cyberterrorism is cheaper than traditional terrorist methods, but that is only true when attacking unsophisticated systems. Governmental cyber infrastructure has complex systems that are hard to hack without enough equipment and expert hacker. In addition, sophisticated and expensive software is needed to keep anonymity of the attacker.

In contemporary times, the Russian government hacked the email address or addresses that belong and related to the campaign of Hilary Clinton presidential campaign of the American elections of 2016 (Gilsinan & Calamur, 2017; Lipton, Sanger, & Shane, 2016). The hack resulted in leaking confidential information that damaged the public image of the American presidential candidate, her party, and her other party members (Sanger & Shane, 2016). This demonstrates that while cyberterrorism may not have been a major perceived threat at the time on Conway's (2011) paper, presently cyberterrorism is making a greater and greater impact in people's daily lives.

Embar-Seddon (2002) states that, humans are threaten that cyberterrorist attack can happened at any moment and cause a catastrophic results.  However, there is no need to be panic, but to realize that the internet was not designed to be secure.  Terrorists may use cyberterrorism along with traditional terrorist attack to manipulate media, gain supporters, and increase the damage of the traditional terrorist attack.

Terrorists can complete their mission by taking advantage of web vulnerabilities, of which there are still vast amounts.  Usually, they send an unambiguous message while keeping their individual identities and locations anonymous.  They get a broader audience's attention, while less people would pay attention to the terrorist group if they did not attack organizations.  Some networks are more vulnerable than others because they were before the web and the internet or because the platform's builder assumed intruders, least of all terrorists, would not specifically target it.  Some critical infrastructures are prime terrorist targets.  Taking down a critical infrastructure can cause severe damage to a society and may be more dangerous than terrorist attacks on the ground, so governments need to work much harder to stop cyberterrorism.

In conclusion, terrorists attack using a new media, they prefer the web, through which millions of people can reach them.  They are using websites to recruit and convey their messages to their followers and to any civilians who are open to political persuasion. There are many reasons why terrorists prefer the web.  For example, it is cheaper and safer to carry an attack through cyberspace than through common domains (i.e., land, air, and sea).

### 2.4. Conjoint Analysis and Multidimensional Scaling

The paper analyzes data using two statistical techniques conjoint analysis and multidimensional scaling. They are multivariate techniques as conjoint analysis understands the development of subjects' preferences for an object and multidimensional scaling is to transform subjects' preferences to points on graph (Anderson et al., 2009). This study uses Value Focused Thinking (VTF) and Public Value Forum (PVF). VFT embeds conjoint analysis and PVF embeds multidimensional scaling.

#### 2.4.1. Conjoint Analysis

Conjoint analysis's fundamental concept is utility. Utility says that each subject has a unique preference and judgment. There are three conditions for utility:

1) Utility should stand for subject's overall preference and show all tangible and intangible features of an object;

2) Utility has several preference aspects and attributes that have different values, e.g., include features of size and quality and subjects will choose based on what they perceive as more important between size and quality;

3) Utility is from relationships of attributes combination.

Utility definition requires conjoint task. It is a statistical analysis of the factors that affect the preference values of participants. Conjoint task defines attributes to construct hypothetical choice situations. Conjoint task includes four aspects:

- Attributes that are the more important than others;
- How subjects can understand the level of each attribute, e.g., understating the difference between price and quality;
- Prediction of subject's evaluated aspects of attributes;
- The number of profiles that are subjects evaluate.

### 2.4.2. Multidimensional scaling

Multidimensional scaling is to discover the perceived subject's perception of an object, thus, creating a multidimensional space to represent subject's preferences as distances to compare objects (Anderson et al., 2010). There are three steps to perform multidimensional scaling:

- Measuring the similarity of the set of objects;
- Using factor analysis and cluster analysis to estimate the objects' positions in multidimensional space;
- Using similarity between objects for overall similarity feeling to infer the subject's preference based on the objects' positions on the multidimensional space.

# Chapter 3: Theory and Methodology

The proposed public policy framework is based on several theories. The dissertation uses the value theory by Catton Jr. (1959) and value-focused thinking by Keeney (1990). The dissertation combines these two theories and adds to them to customize them for cyberterrorism prevention. The combination of the value theory and value-focused thinking is shown throughout the methodology and the results show the effectiveness of theories combination in the methodology implementation to develop public policy for cyberterrorism prevention. There are three characteristics of the research approach of this study: first, it is comprehensive and offers extensive alternatives for decision makers. Second, formalization and implementation of rules and procedures to guide the planning process of developing public policy for preventing cyberterrorism. Third, it uses strict rules and procedures, but it implements them creatively to get the most out of the data and approach.

## 3.1. Value Theory, Value Focused Thinking (VFT), and Alternative-Focused Thinking (AFT)

The study uses Catton's value theory (Catton Jr, 1959) that is based on allowing individuals to express their preferences among alternatives. Value Focused thinking (VFT) is a methodology that Keeney proposes (1990) and it uses Catton's value theory to identify a value. Per (Ralph L. Keeney, 2009c), VFT detects decision opportunities and forms decision alternatives.  This study uses the VFT to bare fundamental objectives and means objectives.

There is another methodology that uses values in decision making; alternative-focused thinking (AFT).    Keeney (1992) proposed value focus thinking approach (VFT) and AFT and it offers decision makers a tool to offer decision alternatives that are based on the stakeholders needs.  AFT is a methodology Keeney consider to be limited and less effective than his VFT.

### 3.1.1. Value Theory By Catton (Catton Jr, 1959)

Catton's theory of value is about the pattern of humans' choice preference among alternative desires and the pattern's attribute to values.  The theory puts socialized human in the center of social organization that influences her ambition towards different desires. The theory has six basic hypotheses and three corollary hypotheses.  Six basic hypotheses:

1) Every new social discipline or value influences all other social disciplines or values;
2) Valuing depends on three factors: first, the new social discipline or value; second, the meaning social discipline or value adds; third, the motivation for a given object or value;

3) The desire for given object or a value varies based on perceived continuous similarity of the object and "to other objects strongly desired at that time" (Catton Jr, 1959);
4) A valuer's reaction to related objects or values is more predictable than her reaction to unrelated ones;
5) A valuer's reaction to congruent objects or values is more predictable than her reaction to unrelated ones;
6) Order of preferences vary among people based on that person's failure to be fully aware of the value added by an object.

Theory of value has three corollary hypotheses of the six basic hypothesis:

1) At any given time, significant correlations be found between values and personal desires;
2) The correlation in A tends to be stronger through time within socially isolated system;
3) Socially acquired knowledge of objects and values can influence person's choices.

Catton's value theory explains the pattern in which social humans order their preferences based on the social organization and desire. Humans use the internet to interact with within a network of machines and persons. Based on the value theory, cyber users have patterns of their desires and the social organization influences their preferences order. Their order of preferences among different desires to preventing cyberterrorism offers rich values to prevent cyberterrorism that is consist with Catton's value theory and with the desires of interviewed cyber users. The values offer alternative desires and ways to preventing cyberterrorism. It is important for cyber security policy makers to understand how cyber users want to prevent cyberterrorism and using Catton's value theory helps cyber security policy makers gaining that knowledge. By gathering values to prevent cyberterrorism, Catton's value theory offers cyber security policy makers with different security dimensions that they should consider, and they usually overlook.

### 3.1.2. Value Focus thinking (VFT) approach

When the need to solve a decision problem arises, decision-makers need to elucidate decision opportunities that help in reaching the decision. For example, the Saudi government wants to choose a technique to watch cyberterrorism activities. Decision making approaches other than value-focused thinking (VFT) starts with evaluating the alternatives of techniques to choose from. However, VFT elucidate that the decision to evaluate the ethics of watching cyberterrorism activities needs to pre the decision of the technique to watch cyberterrorism activities. VFT elucidate the other decisions that decision-maker should make to effectively solve the decision problem.

Value-focused thinking (VFT) forms decision alternatives per individual values and preferences. Thus, the decision alternatives address goals and aims of decision making.

Other decision-making approaches list decision alternatives before understanding the values and preferences that base the goal of decision making.

Per (Mishra & Dhillon, 2007), Keeney used the value theory of Catton (1952) to create a decision making methodology. Value focus theory offers cyber security policy makers with decision alternatives at different security dimensions that other decision-making methodologies may overlook. Keeney's value-focused thinking consists of two activities: finding the information to get and figuring out the best way to get it. Keeney said that using the value-focused thinking will get you most of getting all the needed information. It helps decision makers in narrowing alternatives and select the most suitable one.

Using Catton's value theory allows employees and managers to share their individual preferences about aims. Therefore, Keeney creating a decision making methodology using Catton's value theory allows an environment where managers and employees have shared goals (Mishra & Dhillon, 2007). Revealing the objectives using employees and managers shared values aligns these goals. According to (Mishra & Dhillon, 2007), this has a long-lasting impact of the information systems security in an organization. AFT bares decision alternatives in addition to their assessment and prioritization from individual preferences and values.

Keeney (1992) divides the activities of value-focused thinking (VFT) to two types: decision problem and decision opportunity. In addition, he says that decision opportunities are discoverable before or after the specification of the fundamental aims of the decision making.

### 3.1.3. Alternative-Focused Thinking (AFT)

Alternative-focused thinking (AFT) is a methodology that Keeney references to compare it to his value-focused thinking (VFT) methodology (Ralph L Keeney, 1996). VFT uses the values to reveal the objectives of the policy and uses values to evaluate and prioritize decision alternatives. On the other hand, AFT decision maker concentrates on alternatives and afterwards creates an evaluation criteria to evaluate the alternatives (Ralph L Keeney, 1996). Therefore, AFT is backward thinking Keeney (1996).

Per Keeney (1992), there are five phases of decision making with alternative-focused thinking (AFT):

1) Knowing the need to solve a decision problem;
2) Finding the decision alternatives;
3) Naming values according to decision maker's goal without deep thinking;
4) Using an evaluation measure that is based on the decision alternatives and not fundamental aims of decision making;
5) Picking a decision alternative.

Alternative-focused thinking (AFT) is typical decision-making approach.

### 3.1.4. Comparing Alternative-Focused Thinking (AFT) and Value-Focused Thinking (VFT)

This study focuses on discovering decision alternatives that bare from individual values and preferences. In addition, it uses individual values and preference to evaluate and prioritize decision alternatives. Therefore, it does not use alternative-focused thinking (AFT) and uses value-focused thinking (VFT). There are several differences between AFT and VFT that table 3.2.3.1 summarizes per (Ralph L. Keeney, 2009a). According to Keeney (1996), there are three ways that VFT is different than AFT paradigm:

1) Logical and systematic concepts qualitatively reveal values and preferences;
2) VFT focuses on the values before analyzing the decision alternatives;
3) VFT bares decision values and alternatives.

Table 3.2.3.1. Comparing Alternative-Focused Thinking (AFT) and Value-Focused Thinking (VFT)

| Aspect | Alternative-Focused Thinking (AFT) | Value-Focused Thinking (VFT) |
|---|---|---|
| Approach | Reactive | Proactive |
| Core Element | Decision alternatives | Individuals' values and preferences that create the fundamental aims of decision problem |
| Initial Steps | Starts with analyzing decision alternatives | Starts with elucidating individual values of the decision problem |
| Outcome | Only solves decision problem | Solves decision problems in addition to elucidate decision opportunities |
| Decision Evaluation | Use decision alternatives as basis to create an evaluation measure | Use individuals' values and preferences to evaluate and prioritize decision alternatives |
| Objective | Finding decision opportunities | Creating decision opportunities |

## 3.2. Methodology

Jabir ibn Hayyan, who is the founder of applied chemistry, said that a scientist should only include findings based on deductive methodologies to assure accuracy of the findings. In addition, he said that scientist should include results that she accepts and can test. Generalization is to abstract instances to make a general notion predicts the behavior of similar instances (Lee & Baskerville, 2003). Per Lee and Baskerville (pp. 232-236) if done correctly, empirical statements to empirical statements (EE) or generalized from empirical statements to theoretical statements (ET) generalize empirical findings. EE is to generalize from data to "a measurement, observation, or other description" (pp. 233). ET is to generalize description of "measurement, observation or other description to a theory" (pp. 233).

Generalizability is controversial among different methodologists. However, generalizability should not be an exclusive right to statistical studies, sampling studies, or laboratory studies. It should be a privilege given to studies that satisfies formal logic. Jabir ibn Hayyan said that a scientist should only include findings based on deductive methodologies to assure accuracy of the findings.

Hypothetico-deductive logic uses deductive reasoning and makes research more generalizable. Deductive reasoning is the process of logical reasoning from theoretical statements (major and minor premises) to empirical or conclusion statements. It can lead a scientist to craft logically consist and empirical theory's propositions (Lee & Baskerville, 2003) (p. 229). Performing controlled deduction is harder than in mathematical analysis since qualitative analysis does not have the "corresponding body of rules as succinct or easily applies as the rules of algebra" (Lee, 1989) (p. 40). However, using proper qualitative analysis, i.e., deduction with verbal propositions, "does not deprive itself of the rules of formal logic, to which it may therefore still turn when carrying out the task of making controlled deductions" (p. 40). Hypothetico-deductive logic starts with a theory and "employs the deductive logic of the syllogism, in contrast to inductive logic" (Lee & Baskerville, 2003) (p. 229).

Increasing the size of the sample does not increase generalizability. Increasing the size of the sample can simply mean more variation within a population. Moreover, increasing the sample size does not mean that the inductive general statement is correct. Scientific theory has the ability to use rational abstraction for prediction and replication of the behavior of certain instances thus generalize based on Lee and Baskerville definition of generalization (Lee & Baskerville, 2003) (p. 221). "Scientific theory employs hypothetico-deductive logic" (pp. 229) thus hypothetico-deductive logic is more generalizable over inductive logic. Increasing sample size of a random sample increases reliability of that sample-based estimates and does not give more generalizability to any population characteristics (Lee & Baskerville, 2003) (p. 226). This research employs hypothetico-deductive logic to generalize. It uses theories that are valid per experts and literature and combine them with input of the subjects to use in the objectives emerged.

People behavior at an organization is becoming the focus of nowadays information systems security management (Abed & Weistroffer, 2016). Per Dhillon and Torkzadeh (Dhillon & Torkzadeh, 2006), the research in information systems security is categorized as checklists, risk analysis, formal approaches, or soft approaches. They said that checklists are to use lists of known computer threats to check. Knowing the threats can help in analyzing and calculating their risk. However, new threats keep emerging so checklists tend to become impractical and hard to keep them updated. Therefore, a number of formal models were developed to offer a proactive security management approach "to ensure the confidentiality, integrity and availability of data held in their computer systems" (Dhillon & Torkzadeh, 2006).

However, confidentiality, integrity and availability are obtained if organization and people are aligned to support them, thus, soft approaches emerged to include socio-organizational aspects in information systems security research. People are the ones going to be working on securing and using the information system so, understanding their aspects is important to support the security of information systems. The information interpretation of the data to be collected focuses on the subjects' prospectives, thus, it is subject-centered stance on information (Boell, 2017). According to Boell (Boell, 2017), subject-centered stance on information is to relate information to a subject.

The values elicitation is on the basis that "values can be systematically elicited from nonexperts and combined with the factual inputs from experts" (Keeney et al., 1990), nonexperts are the research subjects and the factual inputs from experts are derived from literature.  Asking internet users about their values for preventing cyberterrorism can be the best way to find what work best for them.

The aims that value focused thinking (VFT) bares are from participants that are undergraduate and master's students from three universities while they were taking security classes, and participants that are employees at a security firm.  They offered their input on how to prevent cyberterrorism from the prospectives of individual, organization, and government.  This study offers the results of semi-structured interviews of the VFT participants.  Data analysis bares several measures and values for preventing cyberterrorism.

The public value forum (PVF) participants are information security experts (listed at appendix 2) and non-experts (listed at appendix 3).  Data analysis bares a decision model for preventing cyberterrorism.

Figure 3.2.1 summarizes the study's methodology.  This study divides the process to three steps.  First, developing fundamental and means objectives.  The proposal is to conduct interviews to find values for cyberterrorism prevention.  Next, script from the interviews structure the values that will become fundamental objectives and means objectives.  Second, is developing value forum.  Value focus theory is to develop value forum derived from fundamental objectives and their attributes.  Third, prioritizing objectives to develop decision alternatives. A panel of experts prioritize objectives based on each fundamental objective and its attributes in different scenarios. Finally, these prioritized objectives based on the category of cyberterrorism and scenario will help develop a framework of public policy for preventing cyberterrorism and create decision alternatives.

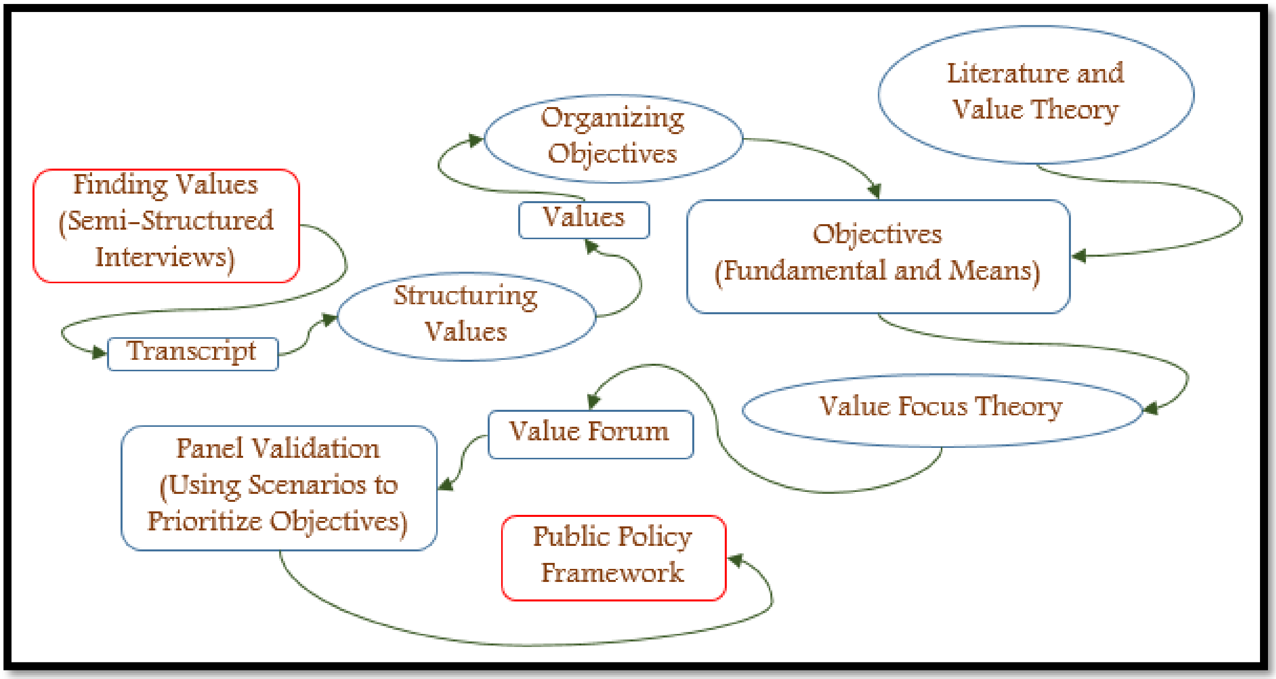
Literature and Value Theory
Organizing Objectives
Finding Values (Semi-Structured Interviews)
Values
Objectives (Fundamental and Means)
Structuring Values
Transcript
Value Forum
Value Focus Theory
Panel Validation (Using Scenarios to Prioritize Objectives)
Public Policy Framework

Figure 3.2.1. The Methodology Process

This section explains the main methodological concepts this study uses, but chapter 4 explains how this study used them and their findings. Section 3.2.1 explains the main methodological concepts of value-focused thinking (VFT) and section 3.2.2 explains the main methodological concepts of public value forum (PVF).

### 3.2.1. Value-Focused Thinking (VFT)

VFT uses four-step process to elicit and classify the values that participants have about cyberterrorism (Dhillon, Challa, et al., 2016; Keeney, 1999; Keeney et al., 1990): First, the researcher defined cyberterrorism and discussed study's goals with participants for around five minutes. Second, each participant wrote how to prevent cyberterrorism from the prospectives of individuals, organizations, and governments based on her belief (henceforth values). Third, the values of everyone become common value format, such as an objective oriented statement. Then similar objectives are clustered together. Finally, each cluster of objectives classification is: fundamental objective or means objective, means objectives are means to achieve fundamental objectives. The objectives' organization shows how these objectives relate or connect to one another. Figure 3.2.1.1 shows the relationship between finding values and the process of developing values.

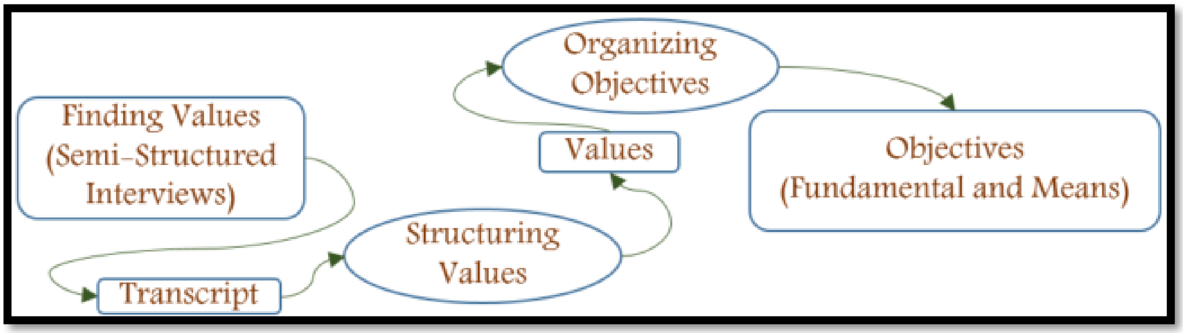
Organizing Objectives
Finding Values (Semi-Structured Interviews)
Values
Objectives (Fundamental and Means)
Structuring Values
Transcript

Figure 3.2.1.1. Developing Values

#### 3.2.1.1. Value-Focused Thinking (VFT): Finding Values

Semi-structured interviews of participants find the values. It is important for all participants to understand the concepts of cyberterrorism. Thus, at the beginning of the interview, participants will discuss about cyberterrorism concepts in addition to the purpose, context, and scope of the interview. Cyberterrorism is "the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society" based on Oxford dictionary. It includes using the internet and the web to send harmful software program and post the ideas of terrorists, which overtly ask for people to attack a target constituency. The core goal Is to elicit the objectives to prevent cyberterrorism. Participants scope their answers for the prospective of individuals, information systems, and governments. The questions were: What should individuals do to prevent cyberterrorism? What should information systems do to prevent cyberterrorism? What should governments do to prevent cyberterrorism? All of them were open-ended questions.

The participants can answer each question they find the most relevant and suitable, i.e., they can discuss any concepts. They know the study wants to discover their opinion so, the researchers are not looking for a certain kind of answer. This allowed natural elicitation of values from individuals. A challenge appeared as everyone expressed values differently. However, redundancy is not a shortcoming when developing a comprehensive list of all values (Keeney, 1999). Probing techniques is to find latent values that includes making implicit values explicit.

### 3.2.1.2. Value-Focused Thinking (VFT): Structuring Values

Next step is structuring the identified values to develop objectives. Structuring values is a five-step process (Dhillon, Challa, & Smith, 2016). First, all statements are restated in a common form. Objective has three attributes (Keeney, 1999): decision, object, and preference. They will have an object in the form of noun and preference in the form of verb (see table 3.2.2.1). All the values show a decision on how to prevent cyberterrorism. That will produce a long list of objectives.

Table 3.2.2.1. An Example of value’s decision, object, and preference

| | |
|---|---|
| Value | Ensure the successful defense of the proposal |
| Decision | Defense of the proposal |
| Object | Successful |
| Preference | Ensure |

Second, remove duplicate statements. Third, common form values become into cyberterrorism sub-objectives. Fourth, content of sub-objectives that discuss similar aspects are clustered. Finally, each cluster of sub-objectives has a label based on its common theme, which becomes the main objective of the cluster. For example, the objectives of “understand related literature when writing the proposal,” “clarify the significance of proposal while presenting,” and “offer yummy refreshers during the presentation" are categorized into main objective: "ensure the successful defense of the proposal." Figure 3.2.1.1 shows the relationship between structuring values and the process of developing values.

### 3.2.1.3. Value-Focused Thinking (VFT): Organizing Objectives

Last step is organizing the clusters based on their main objectives (Dhillon, Challa, et al., 2016). The main objectives initially include both means objectives and fundamental objectives. The means objectives and fundamental objectives categorization uses iterative process. The process includes linking objectives together through means-ends relationship to specify the means objectives and fundamental objectives and show their relationships. The means objectives and fundamental objectives are categorized and related based on their importance in the decision context of how to prevent cyberterrorism. Means objective is an implication of other means objectives and fundamental objectives. Fundamental objective is an essential reason for means. Means objectives specify the logical parts of their fundamental objectives.

- For example:

Transcript: I really love to become a Ph.D. qualified. When I'm 77-year-old, I want to be able to share my stories about earning my Ph.D. In the process of Ph.D., there is proposal defense. Many say that it is the main phase of PhD program. The proposal should set the roadmap for earning the Ph.D. degree. The proposal comes after comprehensive exam. Per Randy Pauch, comprehensive exam is the second worst thing after chemotherapy. Figure 3.2.3.1 shows the creation of objectives and the relationship between values, means objectives, and fundamental objectives.

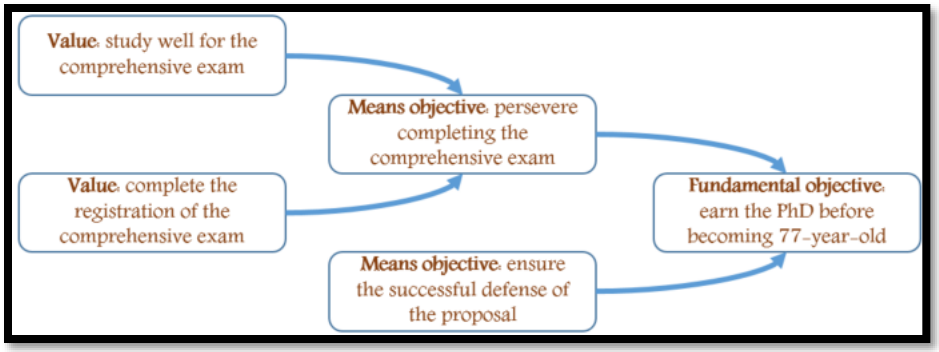
Value: study well for the comprehensive exam
Means objective: persevere completing the comprehensive exam
Value: complete the registration of the comprehensive exam
Fundamental objective: earn the PhD before becoming 77-year-old
Means objective: ensure the successful defense of the proposal

Figure 3.2.3.1. Shows the Relationship Between of the Values Elicited from the Transcript

Figure 3.2.1.1 shows the relationship between organizing objectives and the process of developing values.

### 3.2.2. Using Public Values for Creating Decision Alternatives of Cyberterrorism Prevention Policy

This study uses the fundamental objectives and means objectives from value focused thinking (VFT) in public value forum (PVF). Therefore, adding dependability and objectivity to the data PVF uses. Generally, PVF input is from personal preference of its user, but this study uses the results of VFT as PVF input. Moreover, PVF needs three experts and twenty non-experts to be valid; this study has eight experts and thirty-ne non-experts.

Making better decision relays on predicting the consequences of the alternatives based on the stakeholders' prospectives (Gregory & Keeney, 2017), thus, it is useful to study cyberterrorism prevention by focusing on governments, organizations, and individuals. Each cyberterrorism stakeholder, i.e., governments, organizations, and individuals, has her own requirements and beliefs on how to better prevent cyberterrorism and serve her needs. Public opinion implementation into policy making is an effective methodology (Smith & Dhillon, 2016).

When several individuals share their public values on policy decisions, it covers most policy aspects. Therefore, including public values into decision making process is important "despite being a difficult task" (Smith & Dhillon, 2016). Despite its importance, no other work elicited public values to incorporate in decision making process for cyberterrorism prevention policy. It is useful to tackle such a new policy making by implementing public values in decision making process for cyberterrorism prevention policy. Per Keeney (Keeney, 1999, 2013; Keeney, Von Winterfeldt, & Eppel, 1990; Siebert & Keeney, 2015), this will include:

- How to operationalize public values?
- What roles experts play based on their values?

- How to implement experts' recommendations and their values in policy making?

The answer to these questions becomes a challenge if the policy scope and domain complexity increase (Smith & Dhillon, 2016). This paper uses survey, focus group, and direct values elicitation in public value forum. Based on (Smith & Dhillon, 2016), public value forum model examines several objectives and scenarios with regards to prevent cyberterrorism. Value-relevant information is from a focus group using multi-attribute utility-based tradeoff procedure to get preferred policy alternative.

There are three steps to prepare the objectives and scenarios for the public value forum (Smith & Dhillon, 2016). First, conducted interviews to find the objectives and their attributes for preventing cyberterrorism. Second, finding the fundamental objectives by evaluating objectives importance. Third, create scenarios that in policy implementation to evaluate different alternatives. Figure 3.2.4.1 shows the relationship between fundamental objectives and means objectives, value focused theory, and value forum within the process of developing value forum.

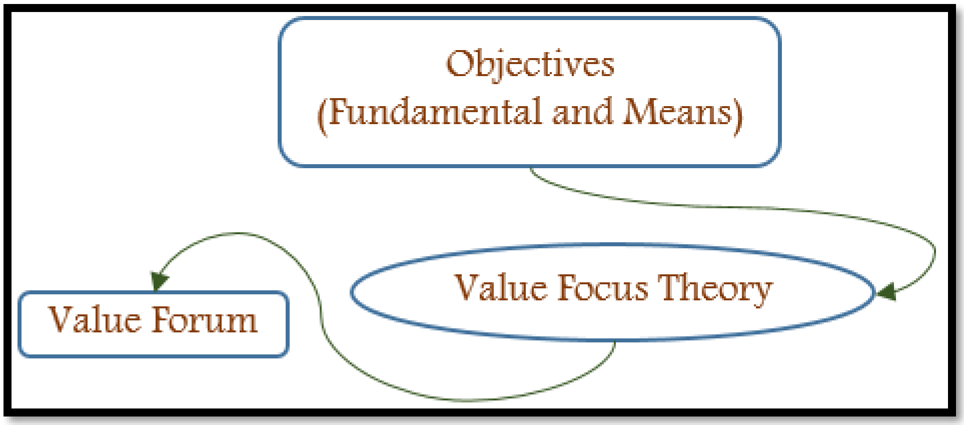

Figure 3.2.2.1. Developing Value Forum

The public value forum (PVF) elicit public value information about the preference of each member at an experts' panel of implementing each objective in each scenario. Nonetheless, in addition to the panel of experts that PVF needs, this study conducted non-experts panel. The panel of experts had eight information security experts (listed at appendix 2) and the panel of non-experts had thirty-one participants who declared that they do not have information systems security expertise (listed at appendix 3). Figure 3.2.1 summarizes the relationship of fundamental objectives and means objectives to value forum development.

### 3.2.2.1. Public Value Forum of Cyberterrorism Prevention

This study combines value-focused thinking (VFT) with public value forum (PVF). Figure 3.2.2.1 shows that this study applies value focused theory to fundamental objectives and means objectives then starts PVF. After revealing the fundamental objectives and means objectives using VFT, those objectives become the input of PVF. PVF proposal uses values that researcher suggests, but this study uses the objectives from VFT to increase reliability by systematically generating the PVF input. Additionally, this study uses participants for PVF that are other than the ones offered their input for VFT. Using different participants increases the trustworthiness of the evaluation participants made for PVF. This study uses two groups of participants for PVF; experts and non-experts. Experts are participants that claim knowledge in information systems security, experts list at appendix 2. On the other hand, non-experts are participants that do not name themselves as information systems security experts, the list of non-expert participants is at appendix 3.

Value-focused thinking (VFT) revealed fundamental objectives and means objectives. Means objectives are the attributes of the fundamental objectives. The fundamental objectives to create three alternate scenarios based on different presentations of the fundamental objectives. After discovering them, the fundamental objectives, means objectives, and their relationship become the input for public value forum (PVF). PVF participants weigh and rank the fundamental objectives without their means objectives then with their means objectives based on the scenario and category of cyberterrorism. The purpose for asking participants to rank and weigh objectives twice is to measure the change of objectives' rank and weight between when participants knew only the operationalized definition of each objective and after they use each objective in different scenarios.  Participants rank each fundamental objective based on their perceived importance in preventing cyberterrorism (1=least important, 5= most important).

Next, they weighted each fundamental objective based on importance in each scenario (1=least important, 5= most important).  Next, the weights were coded 100 points for the highest rating of 5, 0 points for the lowest rating of 1, and all other ratings between 0 and 100 (Smith & Dhillon, 2016).  Participants also rank the scenarios, i.e., how good is a good scenario or how bad is a bad scenario?  Scenarios are based on each fundamental objective.  Finally, participants rank and weight fundamental objectives for preventing cyberterrorism.

### 3.2.2.2.  Scenarios

This study has five scenarios: Best Scenario, Scenario A: Governmental, Scenario B: Organizational, Scenario C: Global, and Worst Scenario (tables 3.2.2.2.4 and 3.2.2.2.3 show the attributes that outline the five scenarios).  All participants said that they agree that all the objectives, attributes, and scenarios are important for preventing cyberterrorism.  Security experts created attributes of Best Scenario and Worst Scenario offering best practices to prevent cyberterrorism and worst respectively.  Researcher directly asked security experts to outline best and worst practices and without arising them from empirical analysis.

The five scenarios should meet fundamental objectives the value-focused thinking (VFT) revealed. However, five different scenarios use themes to try to meet the fundamental objectives. This study takes the attributes defining fundamental objectives and adjusts them to create scenario's theme. Table 3.2.2.2.1 shows the attributes of the fundamental objectives as VFT revealed. On the other hand, tables 3.2.2.2.4 and 3.2.2.2.3 show the attributes matching the themes of different scenarios.

Table 3.2.2.2.1. Fundamntal Objectives and Their Attributes as VFT reveals

| Objectives | Attributes |
|---|---|
| **Ensure governance of technical infrastructure** | • Allocate clear roles and responsibilities for cyberterrorism governance<br>• Assure constant monitoring of threats<br>• Ensure there is learning from past events |
| **Ensure critical infrastructure protection mechanisms are in place** | • Develop contingency plans for governmental data loss<br>• Treat backup locations as a national security issue<br>• Prevent spam<br>• Increase use of Supervisory Control and Data Acquisition (SCADA) systems |
| **Define a media response for cyberterrorist actions** | • Increase media coverage to match the danger of cyberterrorism<br>• Develop a media response strategy for cyberterrorism |
| **Engage in counter cyberterrorism activities** | • Engage in intelligence gathering for cyberterrorism detection and prevention<br>• Counter cyberterrorists attacks proactively |
| **Develop competencies for dealing with cyber terrorism activities** | • Ensure technical staff have up to date knowledge |

| | |
|---|---|
| | • Engage in strategically thinking about cyberterrorism protection<br>• Define mechanisms to get security feedback from individuals<br>• Train individuals on modern technologies |

This study has five thematic scenarios, i.e., best, worst, governmental, organizational, and global. The attributes for best and worst scenarios are from one on one interview between the researcher and the Chief Information Security Officer at an American public research university at the state of Virginia. The process of the interview went as follows:

1) The premise is that it is better to start the interview with an incident that engages the mind of the interviewee and gives her the chance to give more thoughtful answers. This study wanted the Chief Information Security Officer to start recalling cyber-attack incident. The researcher asked the Chief Information Security Officer about a cyber intrusion incident that her school faced. She explained that investigation led to think that most of the computers led the intrusion were from the Islamic Republic of Afghanistan and the Gaza Strip;
2) The researcher asked her about the best scenario to prevent such cyber attack from happening, and the worst scenario;
3) She gave values the researcher took and plugged them into the attributes of the fundamental objectives from value-focused thinking (VFT) creating the attributes that define best and worst scenarios.

During the value-focused thinking (VFT) participants gave values that the researcher clustered to governmental, organizational, and global. Those values were about suggesting that local government should prevent cyberterrorism, other values suggesting that preventing cyberterrorism is a global effort, and other values suggesting that preventing cyberterrorism is an organizational responsibility. Therefore, this study has the scenarios of governmental, global, and organizational in addition to best and worst scenarios. Table 3.2.2.2.2 shows that Chief Information Security Officer at an American public research university at the state of Virginia is the source where researcher derived the best and worst scenarios. on the other hand, participants from VFT, i.e., internet users with basic acquaintance of cybersecurity, are the source where researcher derived government, global, and organizational scenarios.

**Table 3.2.2.2.2. Scenarios and their Source**

| Scenario | Creator |
|---|---|
| **Best Scenario** | Security expert |
| **Worst Scenario** | |
| **Scenario A: Governmental** | Subjects of internet users with basic acquaintance of cybersecurity |
| **Scenario B: Organizational** | |
| **Scenario C: Global** | |

The Chief Information Security Officer at an American public research university at the state of Virginia gave values of the best scenario to show her belief and preference of what preventing cyberterrorism should include (table 3.2.2.2.3 shows best and worst scenarios). She prefers that information systems security should include those attributes for it to be effective. On the other hand, she believes that if an information systems security follows the attributes of the worst scenario, preventing cyberterrorism will be challenging for them. Per the interview, several information systems security facilities at her school use the attributes of the worst scenario thus they are unlikely to have the competencies for preventing cyberterrorism.

**Table 3.2.2.2.3. Best and Worst Scenarios Subjects Developed and Evaluated**

| Objective | Best Scenario | Worst Scenario |
|---|---|---|
| **Ensure governance of technical infrastructure** | -Allocate clear roles and responsibilities of different local governmental local organizations (e.g. NSA & CIA) for cyberterrorism governance<br>- Local governmental local organizations cooperate in monitoring of cyber threats<br>- Local governmental local organizations exchange knowledge about past cyber attacks | - No roles and responsibilities are allocated among different local governmental local organizations (e.g. NSA & CIA) for cyberterrorism governance<br>- Local governmental local organizations do not monitor cyber threats<br>- Local governmental local organizations do not exchange knowledge about past cyber attacks |
| **Ensure critical infrastructure protection mechanisms are in place** | - Local governmental local organizations cooperate in developing contingency plans for data loss<br>- Local governmental local organizations ensure the secrecy of governmental data backup locations<br>- Local governmental local organizations develop spam prevention policy<br>- Local governmental local organizations use SCADA | - Local governmental local organizations do not develop contingency plans for data loss<br>- Local governmental local organizations publicly share governmental data backup locations<br>- Local governmental local organizations do not prevent spam<br>- Local governmental local organizations do not use SCADA |
| **Define a media response for cyberterrorist actions** | - Local governmental local organizations use media to inform people about the danger of cyberterrorism<br>- Local governmental local organizations develop a media response policy | - Local governmental local organizations do not use media to inform people about the danger of cyberterrorism<br>- Local governmental local organizations do not develop a media response policy |

| | | |
|---|---|---|
| **Engage in counter cyberterrorism activities** | - Local governmental local organizations cooperate in intelligence gathering for cyberterrorism detection and prevention<br>- Local governmental local organizations plane a counter cyberterrorists attacks | - Local governmental local organizations do not engage in intelligence gathering for cyberterrorism detection and prevention<br>- Local governmental local organizations do not respond to cyberterrorists attacks |
| **Develop competencies for dealing with cyber terrorism activities** | - Local governmental local organizations standardize national skill's level of technical staff<br>- Local governmental local organizations develop a strategy about cyberterrorism protection<br>- Local governmental local organizations get security feedback from citizens via online feedback<br>- Local governmental local organizations develop national technical training policy | - Local governmental local organizations do not standardize national skill's level of technical staff<br>- Local governmental local organizations do not develop a strategy about cyberterrorism protection<br>- Local governmental local organizations do not get security feedback from citizens via online feedback<br>- Local governmental local organizations do not develop national technical training policy |

The value-focused thinking (VFT) participants gave values that bare a theme in their values. The VFT values are in three main clusters:

1) Several participants expressed their preference to have their local government ensure the prevention of cyberterrorism. They said that their local government should represent them and protect them from cyberterrorism and put laws that regulate information systems security practices in the nation. Per them, governments can have a conflict of interest and be unable to cooperate, but their government should protect them from cyberterrorism;
2) Other participants said that no one government can prevent cyberterrorism. They prefer global cooperation for preventing cyberterrorism;

3) Other participants prefer to give power distribution through allowing organizations to handle preventing cyberterrorisms. They said that allowing organizations to have their own roles adds agility that cyberterrorism prevention needs. In addition, they consider governmental and global solutions take a long time.

This study creates government, global, and organizational scenarios for the public value forum (PVF). Their definitions are based on the attributes of the fundamental objectives from value-focused thinking (VFT). Table 3.2.2.2.4 shows the governmental, global, and organizational scenarios.

**Table 3.2.2.2.4. A, B, and C Scenarios Subjects Developed and Evaluated**

| Objective | Scenario A: Governmental | Scenario B: Organizational | Scenario C: Global |
|---|---|---|---|
| **Ensure governance of technical infrastructure** | - Government supervises cyberterrorism governance<br>- Government analyzes and exchanges information about cyberterrorist attacks | - Local organizations handle their own infrastructure without supervision of the government<br>- Local organizations check their information systems for threats<br>- Local organizations analyze information about cyberterrorist attacks | - UN suggests guidelines to handle cyberterrorism governance<br>- UN analyzes and exchanges information about cyberterrorism attacks among its members |
| **Ensure critical infrastructure protection mechanisms are in place** | - Government develops a plan for data loss<br>- Government owns backup servers and do not outsource their maintenance<br>- Government implements spam | - Local organizations develop their own data loss plan<br>- Local organizations own their own backup servers<br>- Local organizations implement their own spam prevention | - UN develops guidelines for data loss plan<br>- UN supply its members with backup servers<br>- UN suggests spam prevention guidelines |

| | | | |
|---|---|---|---|
| | prevention on all servers in the nation<br>- Government demands local organizations to use SCADA | - Local organizations decide to use SCADA or not without governmental supervision | - UN offers guidelines and suggests using SCADA |
| **Define a media response for cyberterrorist actions** | - Government supervises the comments related to cyberterrorism of all employees in the nation<br>- Government controls the media response for cyberterrorism | - Local organizations supervises the comments related to cyberterrorism of all their employees<br>- Local organizations develops its own media response for cyberterrorism | - UN suggests guidelines to its members on how to comment on cyberterrorism<br>- UN regulate its members media to respond to cyberterrorism based on its media response strategy for cyberterrorism |
| **Engage in counter cyberterrorism activities** | - Government gathers information about cyber activities of all servers in the nation<br>- Government uses attacks on severs in the nation to launch cyber-attacks on attackers | - Local organizations gather its own information about cyberterrorism without governmental supervision<br>- Local organizations launch their own cyber-attacks on attackers without consulting with the government | - UN gathers information about cyberterrorism<br>- UN launches its own cyber-attacks on countries and local organizations in retaliation of their cyber-attacks based on UN voting |
| **Develop competencies for dealing with cyber terrorism activities** | - Government supervises the readiness of technical staff in all the nation<br>- Government handles cyber protection on all servers in the nation<br>- Government supervises activities of employees in all the nation | - Local organizations supervise the readiness of their employees without governmental supervision<br>- Local organizations handle their cyber protection without governmental supervision | - UN rates the cybersecurity readiness of each country<br>- UN handles cyber protection of its members |

Public value forum (PVF) uses scenarios to evaluate different decision alternatives. This study uses five scenarios that value-focused thinking (VFT) bares. It is taking VFT to add reliability to the input of PVF since otherwise it is based on a researcher's preference. The scenarios are best, worst, governmental, organizational, and global. Scenario A: Governmental outlines attributes that governments should implement to avert cyberterrorism and guard private and public sectors against cyberterrorism. Next, attributes outline Scenario B: Organizational are outlines how private and public organizations should implement independently from governmental interference to prevent cyberterrorism and guard their assets against cyberterrorism. Additionally, subjects outlined attributes of Scenario C: Global to outline how countries should work together to prevent cyberterrorism and guard their countries against cyberterrorism.

### 3.2.2.3. Public Policy Framework:

The paper develops public policy framework consequential to analyzing swing rank and weight, and importance rank and weight of fundamental objectives and scenarios attributes (table 3.2.2.3.1) the weight offers the rank of an objective. The two concepts this survey uses are importance and swing. Definition of the two concepts in detail are at different sections of the survey.

**Table 3.2.2.3.1. Example on Swing Weighing and Importance Weighing Objectives and Attributes**

| Objective | Attributes Defining the Objective | Swing Weight (Between | Importance Weight (Between |
|---|---|---|---|

|  |  | **0% and 100%)** | **0% and 100%)** |
|---|---|---|---|
| **Ensure governance of technical infrastructure** | - Allocate clear roles and responsibilities for cyberterrorism governance | 70% | 100% |
| **Ensure critical infrastructure protection mechanisms are in place** | - Assure constant monitoring of threats | 77% | 87% |
| **Define a media response for cyberterrorist actions** | - Ensure there is learning from past events | 100% | 56% |
| **Engage in counter cyberterrorism activities** | - Develop contingency plans for governmental data loss | 40% | 0% |
| **Develop competencies for dealing with cyber terrorism activities** | - Treat backup locations as a national security issue | 0% | 10% |

Importance rank and swing rank are ranks a decision maker faces. If she has five problems that she can decide to resolve all of them or several of them based on her prospective of problems priority, she is doing importance rank. On the other hand, if she should resolve all the problems in the order of their priority, she is doing swing rank.

This study wants to look at each objective in comparison with other objectives. However, no more than one objective can get a rank or a weight, e.g., no more than one objective can get #2 rank. Starting with finding the most important objective (#1) and the least important objective (#5) will make ranking the rest easier.

The importance weight is to stand for the level of importance between rankings so, rank #1 is 100% and rank #5 is 0%. Starting with weighting rank #1 as 100% and weighting rank #5 as 0% will make weighing the rest easier.

Note: The highest item always weigh 100%, the lowest always weigh 0%, and other items weigh less than 100% and greater than 0%, but do not have to add to 100%

The difference between swing weight and importance weight:

*.* Scenario: swing weigh and importance weigh items crucial for human survival of water, safety, and shelter

*.* Swing weight:

Swing assumes that the person has all three items so, compare the three items

For example, weigh safety as 100%, water as 70%, and shelter as 0%

- Explanation: the human in the scenario has all three items since swing weighing. Feeling safe is the highest swing among other three items since using water and shelter needs safety first; since safety is the highest swing, weigh it as 100%. Next, useful shelter is the one that has access to water otherwise human will have to move from the shelter to get water. Therefore, shelter swing weigh among other three items is 70%; the weighs do not add to 100%. Finally, shelter is the least swing among other three items so, weigh it as 0%.

*.* Importance weight:

Importance assumes that the person has one of the three items at a time so, individually weigh the items

For example, weigh water as 100%, shelter as 40%, and safety as 0%

- Explanation: the human in the scenario has one item at a time since importance weighing. Having water by itself is the most important item for human to survive; since water has the highest importance, weigh it as 100%. Next, weigh shelter low as 40% since shelter by itself is not very important to human survival; the weighs do not add to 100%. However, shelter by itself is more important than safety since shelter may help human to survive whether she feels safe or not. Finally, safety is the least importance item by itself among the three so, weigh it as 0%.

*.* May think about importance weight this way: the highest three donors in the world are United States of America, France, and Japan respectively. However, France donates around twice what Japan donates, thus, the importance weight of the donations can be as below:

- United States of America donation importance weight = 100%
- France's donation importance weight = 93%
- Japan's donation importance weight = 50%

Swing rank and weight do not have to match importance rank and weight. Subjects offered the following:

1) For the five fundamental objectives and their attributes, researchers asked subjects to offer swing rank, swing weight, importance rank, and importance weight. Besides, researchers informed participants the swing weight does not have to equal importance weight and swing rank does not have to equal importance rank;

2) Researchers asked subjects to examine an objective that attributes should ensure when offering importance rank and importance weight for attributes of Scenario A: Governmental, Scenario B: Organizational, and Scenario C: Global (table 3.2.2.3.2);

**Table 3.2.2.3.2. Objective to satisfy: Ensure critical infrastructure protection mechanisms are in place**

| Scenarios | Attributes | Importance Weight (100%-0%) |
|---|---|---|
| **Best Scenario** | - Governmental organizations cooperate in developing contingency plans for data loss<br>- Governmental organizations ensure the secrecy of governmental data backup locations<br>- Governmental organizations develop spam prevention policy<br>- Governmental organizations use SCADA | 100% |
| **Scenario A: Governmental** | - Government develops a plan for data loss<br>- Government owns backup servers and do not outsource their maintenance<br>- Government implements spam prevention on all servers in the nation<br>- Government demands organizations to use SCADA | (Participant Fills Out This Part) |
| **Scenario B: Organizational** | - Organizations develop their own data loss plan<br>- Organizations own their own backup servers<br>- Organizations implement their own spam prevention<br>- Organizations decide to use SCADA or not without governmental supervision | (Participant Fills Out This Part) |
| **Scenario C: Global** | - UN develops guidelines for data loss plan<br>- UN supply its members with backup servers<br>- UN suggests spam prevention guidelines<br>- UN offers guidelines and suggests using SCADA | (Participant Fills Out This Part) |
| **Worst Scenario** | - Governmental organizations do not develop contingency plans for data loss<br>- Governmental organizations publicly share governmental data backup locations<br>- Governmental organizations do not prevent spam<br>- Governmental organizations do not use SCADA | 0% |

3) Researchers asked participants to offer swing weight and importance weight of the all attributes of scenarios A, B, and C in the context of all objectives (table 3.2.2.3.3);

## Table 3.2.2.3.3. Table Participants Filled Out to Swing Weigh and Importance Weigh

| Objectives | Attributes | | | |
|---|---|---|---|---|
| **Ensure governance of technical infrastructure** | **- Allocate clear roles and responsibilities for cyberterrorism governance<br>- Assure constant monitoring of threats<br>- Ensure there is learning from past events** | **- Government supervises cyberterrorism governance<br>- Government analyzes and exchanges information about cyberterrorist attacks** | **- Local organizations handle their own infrastructure without supervision of the government<br>- Local organizations check their information systems for threats<br>- Local organizations analyze information about cyberterrorist attacks** | **- UN suggests guidelines to handle cyberterrorism governance<br>- UN analyzes and exchanges information about cyberterrorism attacks among its members** |
| **Ensure critical infrastructure protection mechanisms are in place** | - Develop contingency plans for governmental data loss<br>- Treat backup locations as a national security issue<br>- Prevent spam<br>- Increase use of Supervisory Control and Data Acquisition (SCADA) systems | - Government develops a plan for data loss<br>- Government owns backup servers and do not outsource their maintenance<br>- Government implements spam prevention on all servers in the nation<br>- Government demands local organizations to use SCADA | - Local organizations develop their own data loss plan<br>- Local organizations own their own backup servers<br>- Local organizations implement their own spam prevention<br>- Local organizations decide to use SCADA or not without governmental supervision | - UN develops guidelines for data loss plan<br>- UN supply its members with backup servers<br>- UN suggests spam prevention guidelines<br>- UN offers guidelines and suggests using SCADA |
| **Define a media response for cyberterrorist actions** | - Increase media coverage to match the danger of cyberterrorism<br>- Develop a media response strategy for cyberterrorism | - Government supervises the comments related to cyberterrorism of all employees in the nation<br>- Government controls the media response for cyberterrorism | - Local organizations supervises the comments related to cyberterrorism of all their employees<br>- Local organizations develops its own media response for cyberterrorism | - UN suggests guidelines to its members on how to comment on cyberterrorism<br>- UN regulate its members media to respond to cyberterrorism based on its media response strategy for cyberterrorism |
| **Engage in counter cyberterrorism activities** | - Engage in intelligence gathering for cyberterrorism detection and prevention<br>- Counter cyberterrorists attacks proactively | - Government gathers information about cyber activities of all servers in the nation<br>- Government uses attacks on severs in the nation to launch cyber-attacks on attackers | - Local organizations gather its own information about cyberterrorism without governmental supervision<br>- Local organizations launch their own cyber-attacks on attackers without consulting with the government | - UN gathers information about cyberterrorism<br>- UN launches its own cyber-attacks on countries and local organizations in retaliation of their cyber-attacks based on UN voting |
| **Develop competencies for dealing with cyber terrorism activities** | - Ensure technical staff have up to date knowledge<br>- Engage in strategically thinking | - Government supervises the readiness of technical staff in all the nation | - Local organizations supervise the readiness of their employees without governmental supervision | - UN rates the cybersecurity readiness of each country<br>- UN handles cyber protection of its members |

|  |  |  |  |  |
|---|---|---|---|---|
|  | about cyberterrorism protection<br>- Define mechanisms to get security feedback from individuals<br>- Train individuals on modern technologies | - Government handles cyber protection on all servers in the nation<br>- Government supervises activities of employees in all the nation | - Local organizations handle their cyber protection without governmental supervision |  |
| **Swing Weight**<br>**(less than 100% and greater than 0%)** |  | (Participant Fills Out This Part) | (Participant Fills Out This Part) | (Participant Fills Out This Part) |
| **Importance Weight**<br>**(less than 100% and greater than 0%)** |  | (Participant Fills Out This Part) | (Participant Fills Out This Part) | (Participant Fills Out This Part) |

4) Subjects offered importance rank and importance weight for attributes of Scenario A: Governmental, Scenario B: Organizational, and Scenario C: Global based on how much these attributes assure fundamental objectives. Besides, researchers asked participants to swing rank, swing weigh, importance rank, and importance weigh the attributes of the five scenarios without labeling the scenarios (table 3.2.2.3.4).

**Table 3.2.2.3.2. Table Participants filled out of Attributes that Do Not Have Labels**

|  |  |  | Attributes |  |  |
|---|---|---|---|---|---|
|  | - UN suggests guidelines to handle cyberterrorism governance<br>- UN analyzes and exchanges information about cyberterrorism attacks among its members | -Allocate clear roles and responsibilities of different local governmental local organizations (e.g. NSA & CIA) for cyberterrorism governance<br>- Local governmental local organizations cooperate in monitoring of cyber threats<br>- Local governmental local organizations exchange knowledge about past cyber attacks | - Local organizations handle their own infrastructure without supervision of the government<br>- Local organizations check their information systems for threats<br>- Local organizations analyze information about cyberterrorist attacks | - Government supervises cyberterrorism governance<br>- Government analyzes and exchanges information about cyberterrorist attacks | - No roles and responsibilities are allocated among different local governmental local organizations (e.g. NSA & CIA) for cyberterrorism governance<br>- Local governmental local organizations do not monitor cyber threats<br>- Local governmental local organizations do not exchange knowledge about past cyber attacks |
|  | - UN develops guidelines for data loss plan<br>- UN supply its members with backup servers | - Local governmental local organizations cooperate in developing contingency plans for data loss | - Local organizations develop their own data loss plan<br>- Local organizations own | - Government develops a plan for data loss<br>- Government owns backup servers and do not | - Local governmental local organizations do not develop contingency plans for data loss<br>- Local governmental local organizations |

| | | | | | |
|---|---|---|---|---|---|
| | - UN suggests spam prevention guidelines<br>- UN offers guidelines and suggests using SCADA | - Local governmental local organizations ensure the secrecy of governmental data backup locations<br>- Local governmental local organizations develop spam prevention policy<br>- Local governmental local organizations use SCADA | their own backup servers<br>- Local organizations implement their own spam prevention<br>- Local organizations decide to use SCADA or not without governmental supervision | outsource their maintenance<br>- Government implements spam prevention on all servers in the nation<br>- Government demands local organizations to use SCADA | publicly share governmental data backup locations<br>- Local governmental local organizations do not prevent spam<br>- Local governmental local organizations do not use SCADA |
| | - UN suggests guidelines to its members on how to comment on cyberterrorism<br>- UN regulate its members media to respond to cyberterrorism based on its media response strategy for cyberterrorism | - Local governmental local organizations use media to inform people about the danger of cyberterrorism<br>- Local governmental local organizations develop a media response policy | - Local organizations supervises the comments related to cyberterrorism of all their employees<br>- Local organizations develops its own media response for cyberterrorism | - Government supervises the comments related to cyberterrorism of all employees in the nation<br>- Government controls the media response for cyberterrorism | - Local governmental local organizations do not use media to inform people about the danger of cyberterrorism<br>- Local governmental local organizations do not develop a media response policy |
| | - UN gathers information about cyberterrorism<br>- UN launches its own cyber-attacks on countries and local organizations in retaliation of their cyber-attacks based on UN voting | - Local governmental local organizations cooperate in intelligence gathering for cyberterrorism detection and prevention<br>- Local governmental local organizations plane a counter cyberterrorists attacks | - Local organizations gather its own information about cyberterrorism without governmental supervision<br>- Local organizations launch their own cyber-attacks on attackers without consulting with the government | - Government gathers information about cyber activities of all servers in the nation<br>- Government uses attacks on severs in the nation to launch cyber-attacks on attackers | - Local governmental local organizations do not engage in intelligence gathering for cyberterrorism detection and prevention<br>- Local governmental local organizations do not respond to cyberterrorists attacks |
| | - UN rates the cybersecurity readiness of each country<br>- UN handles cyber protection of its members | - Local governmental local organizations standardize national skill's level of technical staff<br>- Local governmental local organizations develop a strategy about cyberterrorism protection<br>- Local governmental local organizations get security feedback from citizens via online feedback<br>- Local governmental local organizations develop national technical training policy | - Local organizations supervise the readiness of their employees without governmental supervision<br>- Local organizations handle their cyber protection without governmental supervision | - Government supervises the readiness of technical staff in all the nation<br>- Government handles cyber protection on all servers in the nation<br>- Government supervises activities of employees in all the nation | - Local governmental local organizations do not standardize national skill's level of technical staff<br>- Local governmental local organizations do not develop a strategy about cyberterrorism protection<br>- Local governmental local organizations do not get security feedback from citizens via online feedback<br>- Local governmental local organizations do not develop national technical training policy |
| Swing Weight | (Participant Fills Out This Part) | (Participant Fills Out This Part) | (Participant Fills Out This Part) | (Participant Fills Out This Part) | (Participant Fills Out This Part) |

| | | | | | |
|---|---|---|---|---|---|
| (100% - 0%) | | | | | |
| Importance Weight (100%-0%) | (Participant Fills Out This Part) | (Participant Fills Out This Part) | (Participant Fills Out This Part) | (Participant Fills Out This Part) | (Participant Fills Out This Part) |

The participants based their values on thoroughly assessing the different objectives, attributes, and scenarios. Researchers briefly discussed with participants the objectives, attributes, and scenarios before participants started the public forum and during the public forum. Participants used their knowledge, experience, and preference.

# Chapter 4: Processing the Findings

This chapter analyzes the results from using the theory and methodology from chapter 3. Section 4.1 discuss the findings of value-focused thinking (VFT) and explains VFT fundamental objectives and means objectives. Additionally, it describes the process of choosing fundamental objectives and means objectives, and the process of baring the relationship between fundamental objectives and means objectives. Section 4.2 explains and analyzes the results that public value forum (PVF) revealed. It shows the evaluation of complex policy decision alternatives.

## 4.1. Value Focused Thinking Objectives for Cyberterrorism Prevention

In this section, discussion of means objectives (MO) and fundamental objectives (FO) for preventing cyberterrorism. Our study found eighteen objectives where five are fundamental objectives and thirteen are means objectives. This section also discusses the relationship between fundamental objectives and means objectives for Preventing Cyberterrorism. In addition, combination of the systematically elicited values with factual inputs from literature to imitate Keeney (1990) approach of value focused thinking.

### 4.1.1. Means Objectives for Preventing Cyberterrorism

**MO1 Increase Resilience Capability Following Cyberterrorist Attacks**

In the United States of America, 85% of American cyber operations are defensive. 50% of the country's IT budget is for securing its infrastructure. More than 10% of the IT budget is for cyber defense. 4.8% of Defense Department IT spending is for the Navy/Marine intranet. Government spending should count cybersecurity in its spending and the World Bank should help countries in this issue.

Participants emphasized the importance of increasing resilience capability following cyberterrorist attacks. Increasing the resilience capability following cyberterrorist attacks includes empowering organizations recovering from cyber-attack and encouraging organizations to recover without governmental support.

### MO2 Define Governance Structures for Cyberterrorism Prevention

In December 4, 2007, the Saudi security intelligence and technology experts urge to create new laws for cybercrime (Bowman, 2007). This urge came because of growing cyberterrorism threats and the radical ideology terrorists promote (Bowman, 2007). At the end of a conference in Riyadh and set up by Saudi Intelligence Services which chaired by the kingdom's defense mister and the heir to the throne, a joint announcement to the UN was announced to ask experts to advent their security measurements and for countries to legislate cybercrime laws (Bowman, 2007).

The kingdom’s Defense mister and the heir to the throne said on behave of Saudi security intelligence that more than 17,000 websites requite and advertise terrorism and terrorists create more than 9,000 websites each year. The conference included about 3,000 security intelligent personal and information technology expertise and took three days (Writer, 2006). Kingdom’s defense mister and the heir to the throne said that communication and advertisement are important for terrorists’ military operation as it is for any sovereign country and that terrorists are using their websites for this task (Bowman, 2007). It is good to mention that terrorists attacked Kingdom of Saudi Arabia in which most of these attacks were claimed responsibility from Al-Qaeda.

Subjects found that defining governance structures is important for cyberterrorism prevention. The definition of governance structures includes implementation of governance structure specialized in counter cyberterrorism, define roles for information accessibility, and share accountability among individuals.

### MO3 Ensure Existence of Technical Security Measures

Companies all around the world only detect 10% of all intrusions. Adding to this weakness is the fact that cyberterrorism is getting more sophisticated (Hansen et al., 2007). Intrusion is “any intentional event where an intruder gains access that compromises the confidentiality, integrity, or availability of computers, networks, or the data residing on them” (Mohay, Andeson, Collie, Vel, & McKemmish, 2003). Intrusion detection is a responsive system that reacts to unwanted behaviors and learns from these behaviors to increase security controls (MCrosbie & Spafford, 1995). Advanced intrusion detection should be able to immediately identify intruders and appropriate defenses against them (Hansen et al., 2007). Furthermore, advanced intrusion detection should have the ability to prevent future intrusion (Stallings, 2003). In other words, a strong intrusion detection system should be able to learn patterns and predict future patterns according to previous intrusions (MCrosbie & Spafford, 1995).

Subjects recommended to ensure existence of technical security measures for preventing cyberterrorism. Technical security measures include increase use of strong encryption, define firewalls to watch traffic, and implement sophisticated intrusion detection system. Ferguson, Schneier, and Kohno (Ferguson et al., 2011) said That there are three challenges to consider when designing secure system performance, feature, and evolvement. First, secure system uses resources to keep its security and that may affect the performance and availability of the system. Second, several features may have security vulnerability so, security designers should plan which features to include and where to include them. Third, systems evolve as the organization expands and their complexity increases. The issue occurs when systems expand without updating their security systems to match the systems' expansion.

According to (Ferguson et al., 2011), security is to allow access to authorized people and prevent unauthorized ones. Ferguson, Schneier, and Kohno said that the main goal of cryptography is to minimize the number of users must trust that other users are legit. This study assumes that security includes accessibility and other aspects like systems integration and availability and not only accessibility as Ferguson, Schneier, and Kohno said. Hackers may attack systems to cause denial of service, thus, cause a security breach that disturbs the availability of the systems or part of them and disturb integration since part of the systems are not approachable. Cryptography is “like a lock” (Ferguson et al., 2011), but information systems security is more than placing a lock and it involves the decision of the place to put the lock and the places where to place locks hard to break.

Kerckhoffs's principle after the Dutch cryptographer Auguste Kerckhoffs in the 19th century. The following conditions are Kerckhoffs’s six conditions to design secure system using encryption:

1) The system should be unbreakable;

2) The design of the system does not have to be a secret;

3) The decryption key should be memoizable and easy to change;

4) Encrypted information should be transferable;

5) One person should be able to run and transfer the information and machines that use encryption;

6) The cryptographic system should have usability.

Nonetheless, this dissertation and (Ferguson et al., 2011) assume that every system may be vulnerable. Kerckhoffs's first principle does not seem to be applicable in real world since no system can be safe from any attacks and no system is fully free from vulnerabilities. This dissertation agrees with (Ferguson et al., 2011) that systems are vulnerable, but security level depends on how much work it takes to breech the systems.

Information systems have human and machine users and there should be a procedure to grant trust to these users to access the system. The socio-technical engineering is a main aspect of creating secure system and this dissertation uses internet users to offer the values of cyberterrorism prevention.

### MO4 Ensure Adequacy of Cyber Security Policy

Nowadays, critical infrastructures receive not only traditional security measurements but also new measurements, like cybersecurity (Fovinoa, Guidib, Maseraa, & Stefaninia, 2011). For example, most security procedures conducted by power plants are through the internet or from a distance (Fovinoa et al., 2011). Usually, the communication platform of a power plant is integrated into the company network (Fovinoa et al., 2011). The problem with those platforms is that some of them were meant to be in a disconnected or isolated networks years before the internet (Fovinoa et al., 2011). Threats toward power plants should not be ignored, because when power plants must shut down, they present severe cost both for the environment and power users (Fovinoa et al., 2011), especially hospitals and other humanitarian organizations that depend on energy to support life and people. The security application of power plants should include (Fovinoa et al., 2011):

- The ability to know and prioritize which information is to receive protection;
- Tell the requirements for confidentiality, integrity, and availability; and
- Outdate security policies.

Participants encourage the existence of adequate cyber security policy or preventing cyberterrorism. Ensure currency of cyber security policies. Per the participants, insurance of adequate cyber security policy includes ensure currency of cyber security policies, increase alignment of cyber security policies with security standards, and ensure cyber security policy links to organizational practices.

### MO5 Increase Cross Agency Coordination

On March 10, 2009, In the United States of America, the White House released a document stating that Mary Ann Davidson made testimony to the Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology (House, 2009). The government changed the Monroe Doctrine. The Americans made a Cyber Monroe Doctrine that will include any cyber space attack from a sovereign country as an act of war and should retaliate (House, 2009). Monroe Doctrine is meant to show that the United States of America will response to any intrusion or/and attack and cyber intrusion and/or attack is no different and should be in Monroe Doctrine (House, 2009). "The United States would have concerns about ensuring the safety of the 85% of US critical (cyber) infrastructure that is in private hands given that much of this critical infrastructure (if attacked or brought down) has a direct link to the economic well-being of the United States in addition to other damage that might result" (House, 2009).

President Barack Obama's budget proposal for the 2017 fiscal year included strengthening the partnerships with the private sector to "deter, detect and disrupt threats, including to the nation's critical infrastructure" (Obama, 2016). The partnership included a new cybersecurity Center of Excellence that encourage research collaboration among government and industry experts. The budget proposal also included setting up a national testing lab that tests the cybersecurity capabilities of companies under simulated attacks. The collaboration between nations' law enforcement agencies should fill the intelligence gaps (Fuentes, 2016).

Data analysis reveals that participants ask to increase cross agency coordination. They said that a proper increment in cross agency coordination includes engagement of public and private sectors to prepare for cyberterrorism prevention, and engagement of the global community (like the UN) to prevent cyberterrorism.

### MO6 Increase Awareness of Cyberterrorist Actions

Governments will not know what they are dealing with unless research names the threat. Although websites in the "dark web" have gained a lot of government and media attention, there are not enough studies about them (Qina et al., 2007). More research should be done to inform governments of the basics of cyberterrorism ideologies and the way they conduct their missions. Information systems security scholars and practitioners should analyze terrorists' websites and methods of attack. The UN should take the lead in this study and encourage members and research centers to take part.

Law enforcement should have awareness and intelligence to prevent the threats of radicalization through social networking (Fuentes, 2016). Terrorists websites are for fundraising and recruiting. Some of those websites are very dynamic and change overnight (Weimann, 2004), which is an invaluable quality, because any assassin terrorist should be able to adapt to situations quickly enough to survive prosecution. Websites are on free web servers by "internet savvy" people to provide these websites with propaganda and other materials that the group needs (Armstrong & Forde, 2003). These needs are primarily psychological and then social and economic. Cyberterrorism is a kind of politically motivated use of networks, computers, and websites to support terrorism ("Terrorism: Questions and Answers," 2004; Webster et al., 1998). Jarvis and Macdonald found that "the production of fear constitute[s] important elements of cyberterrorism" (Jarvis & Macdonald, 2015). In other words, cyberterrorists are terrorists who use cybernetics to carry out their missions.

Over 1.4 million small businesses and their workers get cybersecurity training via Small Business Administration under president Barack Obama's budget proposal for the 2017 fiscal year (Obama, 2016). The president stated the launch of new national awareness campaign to raise awareness of cyber threats.

Based on interviews conducted in this research, participants name increasing awareness of cyberterrorist actions as a crucial strategy for prevention of cyberterrorism attacks. They said that increasing awareness of cyberterrorist actions includes emphasize the seriousness of cyberterrorism to the global community, increase cyberterrorism prevention education, develop training for cyberterrorism detection and prevention, and increase awareness of consequences of cyberterrorist attacks.

### MO7 Increase Use of Hacker and Cracker Ability

Some hacktivists claim that they are "freedom fighters" (Kovacich, 1999), and some people become hacktivists to prove that they are more concerned about different issues and more skilled than their followers. In addition, some activists may hire hackers to do certain things at the certain times for certain organizations (Papadimiyriou, 2009), especially cyberterrorist groups. These groups do not hire hackers to damage property or steal; they want their hired hackers to send a message to enemy organizations or to potential allies (Papadimiyriou, 2009). In the terrorists' case, they usually hack for both goals.

On 31 May 2011, the Pentagon declared that it will respond to computer attacks with military operations in a realized document (Gorman & Barnes, 2011). The Pentagon is concerned about hackers that may damage the US Nuclear generators, subways, communications, or any other infrastructure, especially the ones that are critical (Gorman & Barnes, 2011). "The Pentagon's document runs about 30 pages in its classified version and 12 pages in the unclassified one" (Gorman & Barnes, 2011). The document also conations Laws of Armed Conflict and proportionality of response (Gorman & Barnes, 2011). The new strategy will also include allies of the United States of America maintain security in these countries (Gorman & Barnes, 2011). Therefore, American intelligence should prevent cyberterrorism attacks.

Based on the values from the subjects, they suggest increasing the use of hacker and cracker ability to be an effective way for preventing cyberterrorism attacks. They said that prevention should include recruiting ethical cyberterrorist for preventive purposes and finding geolocation of the cyberterrorist groups.

### MO8 Encourage Citizen Involvement for Cyberterrorism Prevention

Individuals are the core element of security. Security policies are crucial to assure systems security. However, security policies are not effective without compliance. Security compliance is unlikable without a security culture (Dhillon, 2015). Citizens might ignore embracing the enacted security policies without security culture. Dhillon (Dhillon, 2015) cited nine of Organisation for Economic Co-operation and Development (OECD) security guidelines. Four of those nine guidelines are directly related to citizen involvement.

- Participants should be aware of their role to enhance security
- Participants should handle the security of information systems and networks
- Participants should prevent, detect, and respond to security incidents
- Participants should respect the legitimate interest of others

During his announcement of budget proposal for the 2017 fiscal year, president Barack Obama announced the launch of new national awareness campaign that will encourage Americans to add extra layer of security like fingerprint or codes sent to your cellphone (Obama, 2016).

Data analysis of the interviews conducted for this research reveals that encouraging citizen involvement is a proactive way for cyberterrorism prevention. Subjects said that citizens' involvement should include encouraging citizens to be involved in fighting cyberterrorism, empowering citizens with respect to cyberterrorism prevention, encouraging citizens to practice good cyber hygiene, and encouraging citizen to report suspicious cyber activity.

### MO9 Increase Spending to Prevent Cyber Terrorism

Most organizations need to spend more money on investigating false identities as well as events caused by terrorists (Hansen et al., 2007). This suggestion does imply that organizations ignore some false identities and that they think false identities are worth ignoring. In the past, they may have been able to afford to ignore them, but cyberterrorism poses a new threat. Though cyberterrorism uses traditional hacking techniques, cyberterrorism is different from traditional hackers in that it is a group of people with political motivation to do harm ("Terrorism: Questions and Answers," 2004) and/or send a message.

Cyberterrorism is becoming terrorists' preferred method, because it offers anonymity, can be lunched from a location that law enforcement would find difficult to reach, and can provide relatively easy and safe intrusion into critical infrastructure ("Terrorism: Questions and Answers," 2004). Furthermore, cyberterrorism is unique in that it involves modified and more advanced hacking techniques to make it harder for police to follow them by using logic bombs, false identities, viruses, etc.

("Terrorism: Questions and Answers," 2004), which are analogous to the gas bombs of a common battle zone that prevent tracking. Whereas hacking is an older technique, cyberterrorism is a newer field that has yet to receive adequate researched (Hansen et al., 2007). Therefore, there is a need to increase spending to prevent cyber terrorism.

According to report written by National Coordination Office for Information Technology Research and Development to the president of the United States of America (Benioff & Lazowska, 2005), the government should increase the spending on unclassified research that civilians can access and use to secure themselves. The report said that increasing the spending will help securing civilian and commercial IT infrastructures.

Based on the interviews conducted for this research, participants said increase spending to prevent cyber terrorism will go a long way in ensuring security and safety. Subjects suggested that increasing the spending should include distributing federal funds for cyberterrorism detection and prevention, strategizing measures for cyberterrorism detection and prevention, and encouraging research on digital defense.

### MO10 Encourage Behavioral Controls

Dhillon, Challa, and Smith (Dhillon, Challa, et al., 2016) found increase ability to control personal information users desire. In addition, they found personal accountability to be important to prevent security threats. Reckless human behaviors (like having predictable password) attack an organization instead of using technical means to break into the system (Dhillon, 2015). Therefore, encouraging users to use proper behavioral controls can lead to prevent cyberterrorism.

Data analysis of the interviews conducted for this research show that participants think encouraging behavioral controls to support the technical means of security. Participants encourage behavioral controls that include ensure confidential data is made available on a need to know basis, encourage use of good password use habits, increase individual accountability in cyberterrorism prevention, and make cyberterrorism training mandatory.

### MO11 Increase Surveillance of Suspect Groups

Another aspect of hacking is identity. The internet gives the hackers a chance to separate themselves from their physical identities, serving as a form of moonlighting (Wynn & Katz, 1997). Some hackers may steal information to access the information of organizations that may help them to achieve their goals (Barrett, 2003). There are three aspects of a hacker's identity (Papadimiyriou, 2009).

- Anonymity: hackers like to keep anonymity, even while working toward a worthy cause. Anonymity may entail difficulty in finding the hacker or total non-identity.
- Metonym: metonymies are the most commonly used technique by hackers. Metonymies confuse the server, which makes it hard to trace the actor.
- Fluid identity: most hackers often switch identities by creating new ones or altering their current identity.

Cyberterrorists use these aspects, which is clear in the story of a hacker named terrorists007, who was terrorizing while studying at the UK and hiding his identity.

The hackers must have the ability to hide their location and identity to carry on hacking (Papadimiyriou, 2009). Terrorists have recognized what the internet offers, such as a vast audience, ease of access, and the ability to be placeless and unidentifiable (Jenkins, 2004).

Data analysis of the interviewees suggest the importance of increase surveillance of suspect groups. Respondents said that increase surveillance of suspect groups should include defining mechanisms to find cyberterrorism activity, increasing surveillance of concerned individuals, tracking individuals suspected of illegal activity, perfecting privacy requirements of citizens, and encouraging citizens to self-check their activities.

### MO12 Define Regulatory Measure for Cyberterrorism Prevention

Governments should legislation laws to criminalize cybercrime and make it clear to everyone especially their residents that cybercrime is a crime and criminals will always be come after. For example, the legislation happened in Kingdom of Saudi Arabia, when 120 members of the Saudi Council passed all the sixteen sections of cybercrime laws in October 13, 2006 (Writer, 2006). The laws were designed by the Commission for Telecommunication and Information Technology (Writer, 2006). The laws are meant to protect individuals, companies, and organizations from any harm over the internet, said Abdul Rahman Al-Yami, the head of the Saudi Council's Communications and Information Technology (Writer, 2006).

The laws are as follows (Writer, 2006):

- For hacking into government networks, using the internet to support terrorism, or manipulating any information related to national security: prison sentence of ten years and a fine of SAR 4.8million.
- Creating websites or programs that may defame someone, advertise for drugs, having any porno contents, or violate Kingdom's general laws, Islamic values, or public ethics: prison sentence up to five years and/or a fine of SAR 4.8 million
- Any person who gains unauthorized access to any network or install a virus on networks that he/she does not own: prison sentence up to four years and/or a fine of SAR 2,999,625
- Obtaining unauthorized electronic documents: prison sentence of three years
- Hacking into websites and change, damage, or misusing their contents: prison sentence of one year

Date analysis of the interview conducted in this research shows that participants felt the urge of defining regulatory measure for cyberterrorism prevention.  The stated that defining regulatory measure for cyberterrorism prevention includes insuring the existence of cybercrime laws, preserving citizens' rights to use the internet through regulations, avoiding regulations that invade citizens' privacy, assuring the criminalization of cyberterrorism acts, and punishing cyberterrorists as criminals that threat the national security.

### MO13 Increase Investigation of Cyberterrorist Funding Sources

Terrorists capitalized on these capabilities to create thousands of websites and fill them with material that encourages warfare, propagandist videos, propagandist t-shirts, and terrorist recruitment (Weimann, 2004). It is important to find sources of cyberterrorist funding to handle it.

Our respondents said that it is important to prevent cyberterrorism by increasing investigation of cyberterrorist funding sources. They suggested that it should include finding the source of income for cyberterrorists and cutting off the source of cyberterrorism income.

### 4.1.2. Fundamental Objectives for Preventing Cyberterrorism

Five fundamental objectives elucidate the major goals individuals have for preventing cyberterrorism. They are found in this research including: Ensure governance of technical infrastructure, Ensure critical infrastructure protection mechanisms are in place, Define a media response for cyberterrorist actions, Engage in counter cyberterrorism activities, and Develop competencies for dealing with cyberterrorism activities. Literature supports the fundamental objectives and the main aspects for preventing cyberterrorism.

### FO1 Ensure Governance of Technical Infrastructure

In Kingdom of Saudi Arabia (KSA), a giant security system protects the entire Saudi network known as King Abdulaziz City for Science and Technology (KACST). This electronic gate of the Kingdom of Saudi Arabia works like a castle gate. It filters every entity that enters through it and prevents unwanted entities from entering. Prevention includes anything that may produce harm, including malwares and websites. All governments should imitate the idea of King Abdulaziz City for Science and Technology. This gate will protect citizens from malware and from entering websites with unclear or unfair privacy policies, infected websites, and websites that encourages behaviors that are against the general ethics of the citizens' religion and culture (e.g., Islam and Saudi ethics); thus, it will prevent terrorists and pornographic websites.

The idea of preventing is more efficient than tracking earlier attackers, watch their subsequent activities, and then pursue them. Prevention is crucial in Saudi society so terrorist cells do not compromise civilians' freedom. Security breaches are valuable resources to improve system security (Pham & Cid, 2012), thus, KACST analyzes potential attacks to improve its system security.

Other governments should imitate King Abdulaziz City for Science and Technology because of its system's resiliency. It is connected to satellites. The advantage of this system was clear when the internet supply cable connecting most of the Middle East was cut by a ship. All countries along the Red Sea went offline except for KSA. KACST is an example of ensuring governance of technical infrastructure.

Subjects suggested that ensuring governance of technical infrastructure to be a proactive objective for preventing cyberterrorism. Governance of technical infrastructure includes allocation of clear roles and responsibilities for cyberterrorism governance, assurance of constant monitoring of possible always, and insurance there is learning for past events.

### FO2 Ensure Critical Infrastructure Protection Mechanisms are in Place

Intrusion into critical infrastructure is crucial to cyberterrorism goals, which involve security threats. Therefore, having a good enough intrusion detection mechanism is essential for handling cyberterrorism (Hansen et al., 2007), since most organizations now perform critical operations through the internet (Hansen et al., 2007). The challenge in intrusion detection is balancing flexibility with security. In other words, an information system needs to be flexible enough to have remote control of different structures on the internet, but there is a chance that unauthorized person can access an open-ended platform, too. An open platform connects through public and private sectors and even across national borders, and the international nature of attacks makes it even harder for governments to assign responsibility for intrusion (Borchgrave, Cilluffo, Cardash, & Ledgerwood, 2001), since most internet connections are built upon old infrastructures and usually without good planning. Because of its potential range, some say that cyberterrorism is “more damaging” than traditional kinds of terrorism ("Terrorism: Questions and Answers," 2004).

Cyberterrorists can attack energy systems, dams, communications, etc. from a safe distance and at a cheap cost. Ever since cyberterrorism and other security threats have become growing concerns ("Terrorism: Questions and Answers," 2004), different organizations have been testing different methodologies to prevent cyberterrorism threats (Hansen et al., 2007). Some studies show that current security applications and measures are not efficient enough against new threats and cyberterrorism (Forrest, Somayaji, & Ackley, 1997). The normal race between evil and good will never give the latter the advantage.

Aiming at infrastructure is a common hacking practice for example hacker in China and Russia hack into systems belong to United States defense contractors (Obama, 2016). Another example is North Korea’s cyber-attack on Sony in 2014 destroyed data and other infrastructure.

Subjects said the insurance that critical infrastructure protection mechanisms are in place to serve as both precautionary and recovery objectives for preventing cyberterrorism. Availability of critical infrastructure protection mechanisms includes development of contingency plans for governmental data loss, treatment backup locations as a national security issue, prevention of spam, and increase use of Supervisory Control and Data

Acquisition (SCADA) systems.  Per their report (Internet Security Threat Report, 2018), Symantec say that Kingdom of Saudi Arabia was the fifth highest country in the rate of receiving email malware and the most in spam rate.

### FO3 Define a Media Response for Cyberterrorist Actions

Although terrorists are increasingly using the internet and websites to affect some parts of the world (Qina et al., 2007), no advanced analysis exists, because of the lack of tools that interpret the language the terrorists are using on their websites (Qina et al., 2007), mainly Arabic.  The terrorists are using the internet to spread their message through videos and letters.  The increased sophistication of terrorists' websites indicates that they are gaining more popularity (Qina et al., 2007).

By using the internet, terrorists can reach more audiences and the information they market can still be online all day long for any interested party to access.  Studies have categorized terrorists' websites into five categories: propaganda, recruitment and training, fundraising, communication, and targeting.  Since the 1990s, organizations such as SITE institute, the Anti-Terrorism Coalition, and Middle East Media Research Institute (MEMRI) started to search through terrorists' websites (Qina et al., 2007).

Respondents felt that defining a good media response for cyberterrorist actions will go along ensuring the safety of the society.  The definition of a good media response for cyberterrorist actions includes increase of media coverage to match the danger of cyberterrorism and development of a media response strategy for cyberterrorism.

### FO4 Engage in Counter Cyberterrorism Activities

Attacking terrorists’ websites and cyberspace may be useful to at least slow them down. The UN should lead the initiative to create a center for counter cyberterrorism. Plus, each country and assemblies of countries (i.e., Organization of Islamic Cooperation) should take part. For example, Al-Qaida lost four out of five of its main websites. The websites where attacked by different organizations. Al-Qaida attacks Shittes websites and they attack back (Knickmeyer, 2008). The American intelligence is struggling to define rules to legalize the use of cyber weapons (Graham, 1998). On the other hand, the problem with these weapons that they can be unpredictable (Graham, 1998). Cyber-attacks are more likely to miss its target than a physical missile and its circumstances can be destructive. Another thing to keep in mind before attacking is the fact that a group of terrorists can change (or mask) their real location for a country to attack “an instance” country.

Per the subjects, proactively countering cyberterrorism activities is crucial for preventing cyberterrorism. Countering cyberterrorism activities includes participants engage in intelligence gathering for cyberterrorism detection and prevention and counter cyberterrorists attacks proactively.

### FO5 Develop Competencies for Dealing with Cyber Terrorism Activities

Security management should implement security controls to maintain information security at an organization (Dhillon, 2015). Organizations share information that is critical to their success through distributed systems and networks. Therefore, they should ensure security management. Security management implements formal controls, informal controls, and technical controls (Dhillon, 2015). Formal controls state security rules and polices. Informal controls are to train employees and spread security awareness among employees. Technical controls are to have technical security measures of the information systems including intrusion detection and firewalls.

During his announcement of budget proposal for the 2017 fiscal year, president Barack Obama announced the establishment of bipartisan Commission on Enhancing National Cybersecurity to focus on long-term solutions of cyber threats (Obama, 2016).
Respondents Ensure technical staff have up to date knowledge, engage in strategically thinking about cyberterrorism protection, define mechanisms to get security feedback from individuals, train individuals on new technologies.

### 4.1.3. Relationship Between Fundamental Objectives and Mean Objectives

Per figure 4.1.3.1, if an organization wants to ensure critical infrastructure protection mechanisms are in place (fundamental objectives) the organization could increase resilience capability following cyber terrorist attacks by increasing cross agency coordination, ensuring adequacy of cyber security policy, increasing use of hacker and cracker ability, and ensure existence of technical security measures.

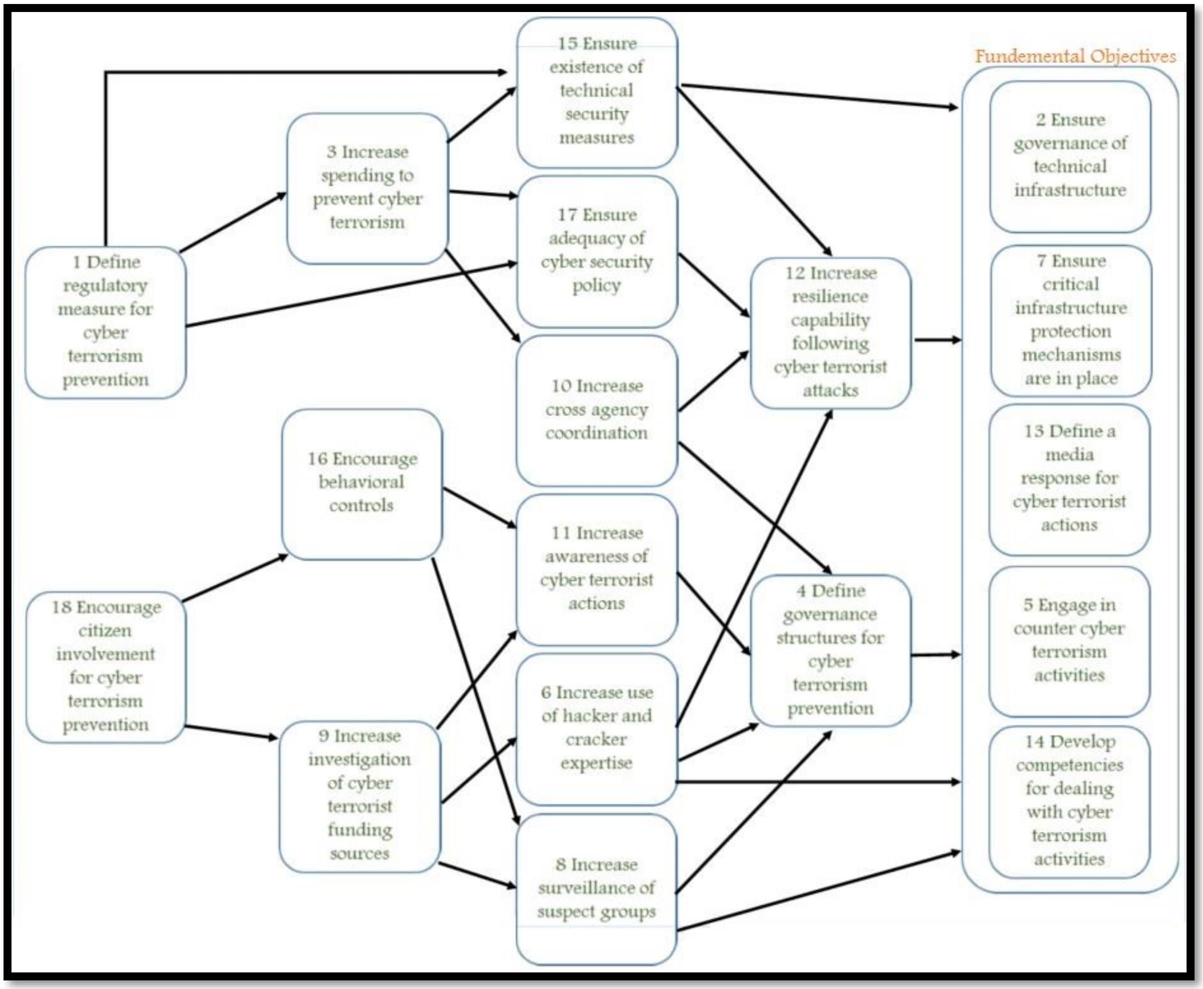
Fundemental Objectives
15 Ensure existence of technical security measures
3 Increase spending to prevent cyber terrorism
17 Ensure adequacy of cyber security policy
1 Define regulatory measure for cyber terrorism prevention
12 Increase resilience capability following cyber terrorist attacks
10 Increase cross agency coordination
16 Encourage behavioral controls
11 Increase awareness of cyber terrorist actions
18 Encourage citizen involvement for cyber terrorism prevention
4 Define governance structures for cyber terrorism prevention
6 Increase use of hacker and cracker expertise
9 Increase investigation of cyber terrorist funding sources
8 Increase surveillance of suspect groups
2 Ensure governance of technical infrastructure
7 Ensure critical infrastructure protection mechanisms are in place
13 Define a media response for cyber terrorist actions
5 Engage in counter cyber terrorism activities
14 Develop competencies for dealing with cyber terrorism activities

**Figure 4.1.3.1. Means Objectives and Fundamental Objectives for Preventing Cyberterrorism**

## 4.2. Public Value forum for Preventing Cyberterrorism

Using public values to derive policymaking decision process can lead to a comprehensive list of objectives and decision alternatives, where these values explain the concerns that individuals have about policy development and implementation (Keeney, 1999, 2013; Keeney et al., 1990; Siebert & Keeney, 2015; Smith & Dhillon, 2016). Alternatives are ranked based on their weight. Their weight is based on the input from the panel of experts (Smith & Dhillon, 2016). Figure 3.5 shows the third step of the proposed process. This step develops decision alternatives based on prioritizing objectives.

Hubbard and Seiersen (Hubbard & Seiersen, 2016) said that cybersecurity experts need to improve their understanding about how to measure observations that quantitively reduce uncertainty that includes inferences related to measuring subjective preferences and values subjects must reduce risk of cyberattacks. They said that measuring subjective preferences and values of the subjects can assess how much people are willing to pay for these subjective preferences and values. The paper use tables like Table 4.2.1 to swing rank and swing weight objectives for preventing cyberterrorism.

**Table 4.2.1. Swing Ranking and Weighting Objectives**

| Objective | Attributes Defining the Objective | Swing Weight0 (Between 0% and 100%) |
|---|---|---|
| **Ensure governance of technical infrastructure** | - Allocate clear roles and responsibilities for cyberterrorism governance<br>- Assure constant monitoring of threats<br>- Ensure there is learning from past events | |
| **Ensure critical infrastructure protection mechanisms are in place** | - Develop contingency plans for governmental data loss<br>- Treat backup locations as a national security issue<br>- Prevent spam<br>- Increase use of Supervisory Control and Data Acquisition (SCADA) systems | |
| **Define a media response for cyberterrorist actions** | - Increase media coverage to match the danger of cyberterrorism<br>- Develop a media response strategy for cyberterrorism | |
| **Engage in counter cyberterrorism activities** | - Engage in intelligence gathering for cyberterrorism detection and prevention<br>- Counter cyberterrorists attacks proactively | |
| **Develop competencies for dealing with cyber terrorism activities** | - Ensure technical staff have up to date knowledge<br>- Engage in strategically thinking about cyberterrorism protection<br>- Define mechanisms to get security feedback from individuals<br>- Train individuals on modern technologies | |

Per Keeney (Keeney, 2013), prioritizing objectives help decision-makers see through alternative decisions. Multiple objectives decision problem refers to decision problems with multiple fundamental objectives. Multiple objectives decision logically prioritizes the fundamental objectives to evaluate alternative solutions to the decision context. Those fundamental objectives are the ones related to decision. The logical prioritizing is to sort the multiple fundamental objectives based on the importance of achieving each one of them to a decision. However, prioritizing objectives should base on a logical foundation for prioritizing. Following logical foundation for prioritizing helps justifying the prioritizing task. Per (Youtie & Shapira, 2017), operationalizing public values can support the development of evolving technology.  The methods and technology terrorists use to in cyberattacks are evolving and becoming more sophisticated due to advancement in technology and learning from their earlier cyberattacks to improve cyberattacks. Therefore, preventing cyberterrorism is evolving to catch up with the improvement cyberterrorists have in cyberattacks methods and technology.  Taking the public value approach can link subject with a service that meets a need, solves a problem, or brings a benefit (Youtie & Shapira, 2017).

This study proposes developing public policy outline and decision alternative priority from subjects that are cybersecurity experts and internet users with basic acquaintance of cybersecurity.  Building on (Youtie & Shapira, 2017), this results in having public policy outline and decision alternative priority that (within the context of cyberterrorism prevention) meet a need, solve a problem, or bring a benefit to the subjects. Cyberterrorism prevention should become ahead of the methods and technology of cyberterrorism to be able to hold and prevent it.  This study contributes to the advancement of cyberterrorism prevention through helping decision makers understand and prioritize their decision alternatives for preventing cyberterrorism.

The study meets with members of the public and special interest group.  Special interest group is the group of information security experts.  Per (Keeney, 2013; Keeney et al., 1990; Smith & Dhillon, 2016) researchers using the approach of the public value forum meet with five to twenty-five participants from public, special interest groups or organizations that.  The participants use fundamental objectives, objective attributes, and scenario attributes to help decision makers choose decision alternatives for preventing cyberterrorism.  Participants give values to objectives, attributes, and scenarios to prioritize decision alternatives for preventing cyberterrorism.

Per (Keeney et al., 1990; Smith & Dhillon, 2016), there are two approaches for eliciting societal values for policy decisions.  First, researchers use stakeholders as participants to elicit societal values for policy decisions.  According to (Keeney et al., 1990; Smith & Dhillon, 2016), this approach is suitable for elicit societal values for policy decisions for topics that are contentious thus entail negotiation.  Second, select participants at random from the public.  Based on (Keeney, 1996, 2013; Keeney et al., 1990; Smith & Dhillon, 2016), this approach suitable for elicit societal values for policy decisions for topics that are new and "little to no knowledge exists about reasonable public values to drive policy decisions" (Smith & Dhillon, 2016) that includes relatively new topics.  Eliciting societal values for policy decisions is new and little to no knowledge exists about it.  Therefore, this study uses the second approach for eliciting societal values for policy decisions.

There are five methods to obtain public value that (Keeney et al., 1990; Smith & Dhillon, 2016) mentioned at their papers; survey, indirect public value elicitation, direct public value elicitation, focus groups, and engagement of the public.  Survey helps several participants feel comfortable when they offer public value.  Hence, it allows participants to feel less pressure than methods that have data collector looking at the participant waiting for her answer. However, participants may give noise instead of data if they:

a. Did not understand the topics, questions, and choices. This may happen in survey hence several participants may find it tedious to contact the data collectors every time they are confused about the meaning of a question or a choice;

b. Find the survey to be long may cause participants to fill out the survey with arbitrary or unthoughtful answers to be able to return the survey;

c. Do not feel the motive the fill out the survey since no one is watching them and waiting for their answers. This causes participants to leave out unrequired fields like short answer questions.

Indirect public value elicitation is to watch subjects in their natural environment to bare their behavior. This is useful because participants will act based on their values without the pressure of offering acceptable answers. Additionally, it allows data collectors to elicit public values based on their interpretation of participants behaviors. Hence, participants may interpret their actions differently than data collectors' interpretation. On one hand, it allows data collector to have the chance of eliciting more information than they initially wanted since participants behave without the structure of questions from data collectors. On the other hand, the freedom in behavior may cause the drawback of taking long time for participants to response to the behavior data collectors want to watch. In addition, drawbacks of indirect public value elicitation include data collector may misinterpret participant behavior.  For example, despite that her observation of the relationship between Kingdom of Saudi Arabia (KSA) and United States of America (USA) was thorough and made several thoughtful points, Bronson (Bronson, 2008) interpreted Saudi behavior based on her American (not Saudi) culture.  Additionally, she assumed the causation of the behavior.

Direct public value elicitation offers behavior interpretation that is based on the explanation of the public.  Hence, data collectors ask participants directly about their preferences and tradeoffs.  Additionally, it is an interactive process with individuals or groups to elicit values they prefer when evaluating policy options.  Moreover, the questions of direct value elicitation focus on the value side of the policy problem (Keeney et al., 1990).  Direct public value elicitation offers several rating and weighting methods for formal value elicitation which may contribute to enhancing the policy process. However, drawbacks of direct public value elicitation include it takes resources to conduct, e.g., finding time and place that is suitable for participants and arrange to meet at that time and place.  Additionally, non-experts may find it difficult to answer tradeoffs questions.  These questions are hypothetical in nature so, participants may act differently in reality than they answer they propose.

Focus groups is having a group of participants that are familiar with the topic that they are going to discuss where data collectors measure their reactions to solutions data collectors propose.  Therefore, the values data collectors elicit may be more informative than values from other elicitation styles. Additionally, the acquaintance of the participants may help data collectors by offering values that they were not aware about the way to elicit them. However, focus groups may be smaller than other groups since it may be hard to have many experts that are available. The small size of the focus group may produce data from a group that does not represent field experts. In addition, the small size of the focus group may result in having values of a small number of experts thus personal data instead of representative data.

Contribution of the Public combines the concepts of focus group and direct public value elicitation. It consists of a series of meetings between the data collectors and a group of experts and policy makers in addition to interest group where members are from the public that data collectors select. These groups solve a specific problem that concerns the participants. However, these problems tend to be specific and concise or oblige decision making for groups to solve within a period that they may be able to work on, e.g., less than two hours.

Table 4.2.2 shows comparison between different approaches to provoke public value the table is based on (Keeney et al., 1990; Smith & Dhillon, 2016) with modification.

**Table 4.2.2. Methods of Public Value Elicitation (Keeney et al., 1990; Smith & Dhillon, 2016)**

| Elicitation Style | Benefit | Drawback |
|---|---|---|

| | | |
|---|---|---|
| **Survey** | - Participants may have enough time to offer informative answers since they may think about their answer;<br>- Survey offers values, objective, and alternatives to participants to read and use them as basis for their answers;<br>- Participants may feel more comfortable in answering than they may feel by other methods. | - The design of the survey may influence the attitude of answers;<br>- Hard to design;<br>- Hard to find informative participants;<br>- May include noise and not data for anonymous and long surveys. |
| **Indirect Public Value Elicitation** | - Participants behave the way they usually do without the pressure of data collectors asking to watch their behavior for certain situation<br>- Data collectors may elicit more information than they initially wanted | - Data collectors may misinterpret the behavior of participants<br>- It may take long time to get data about behavior data collectors study<br>- Potential different behavior interpretation between participants and observers |
| **Direct Public Value Elicitation** | - Offers behavior interpretation that is based on the explanation of the public<br>- Focuses on the value side<br>- Has several rating and weighting methods | - May need intensive resources to conduct<br>- May get noise (not data) from non-experts<br>- Participants evaluate hypothetical tradeoffs |
| **Focus Group** | - Data collectors elicit values from participants familiar with the field of interest<br>- Participants expertise may help in eliciting informative values | - The group may have a small number of participants<br>- Small number of the focus group may result in eliciting personal data instead of representative data |
| **Contribution of the Public** | - Participants solve a specific problem of interest | - Problems are small or affect the decision making |

This study elicits values through public forum using a combination of survey, indirect public value elicitation, direct public value elicitation, focus groups, and engagement of the public.

- Survey: This study asks experts and non-experts to quantitatively offer quantitative weights to objectives, attributes, and scenarios that are derived from the results of value focused thinking in chapter 4;
- Indirect public value elicitation: This study asks experts and non-experts to offer weights to attributes that do not have a label (table 5.2.4);

- Direct public value elicitation: This study asks experts to offer scenarios that have different themes of preventing cyberterrorism;
- Focus group: This study asks experts and non-experts to offer weights that are their reactions for objectives, attributes, and scenarios that are derived from the results of value focused thinking;
- Contribution of the Public: This study asks non-experts, whom are a group of the public that share an interest and data collectors selected at random, to use value focused thinking to develop fundamental objectives and means objectives for preventing cyberterrorism. Subsequently, experts use the fundamental objectives and means objectives to develop attributes and scenarios. Afterward, experts and non-experts offer weights that helps decision makers in evaluating the objectives, attributes, and scenarios.

After the use of the second approach, the study uses the outcome of the approach to define the objectives and attributes then creates scenarios that are aptly contrasting. The study has five scenarios Best Scenario, Worst Scenario, Scenario A: Governmental, Scenario B: Organizational, and Scenario C: Global. Lastly, the study analyzes the results from the value forum for policy decision making for prevention cyberterrorism.

The study derives the steps of structuring the value forum from (Keeney et al., 1990; Smith & Dhillon, 2016) (check figure 4.2.1):

1) Researchers informed participants about the policy problem of preventing cyberterrorism specifically the importance of cyberterrorism prevention, the importance

of decision making for cyberterrorism prevention, and the importance of public policy to prevent cyberterrorism;

2) Researchers define the objectives and attributes to participants and answer any questions they have about the definition of objectives and attributes. Participants should have objectives that are not like offer them with distinct choices of objectives. Therefore, researchers should differentiate between objectives using attributes that distinguish the objectives that allows researchers to brace the accuracy of the utility function (Anderson et al., 2010). These objectives and attributes are from value focused thinking. The first two steps are to ensure that researchers elicit the wanted information that will generate right utility function;

3) Participants offer their single-attribute utility functions for objectives, attributes, scenarios, scenarios per objective. Researchers use the rank and weight participants gave to generate utility function. The utility function elicits favorability of an objective or a scenario;

4) Researchers elicit the tradeoffs among attributes defining objectives. This step elicits the favorability of attributes that can support policy decision makers in prioritizing their decision alternatives for preventing cyberterrorism, which is the purpose of the value forum.

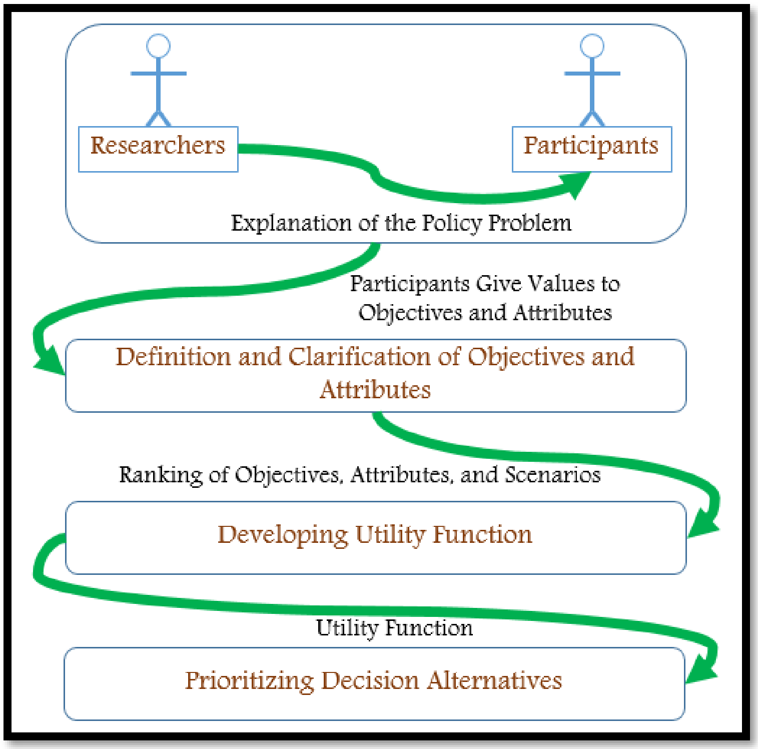
Researchers
Participants
Explanation of the Policy Problem
Participants Give Values to Objectives and Attributes
Definition and Clarification of Objectives and Attributes
Ranking of Objectives, Attributes, and Scenarios
Developing Utility Function
Utility Function
Prioritizing Decision Alternatives

**Figure 4.2.1. Structure of the Public Value Forum**

The study uses participants that work at security firms and have important level of expertise in information systems security. Additionally, the study uses a random sample of volunteers that are common internet users with little to no work experience in the field of information systems security. Per (Keeney, 2013; Keeney et al., 1990; Smith & Dhillon, 2016) the public value forum approach may meet with five to twenty-five participants to get representative sample of the population. The study uses twenty-four participants where eight are experts in information systems security and eighteen have little to no work experience in the field of information systems security. Most of the sample have educational background in information systems security and born at the state of Virginia in the United States of America. The age of participants rang is between twenty-four and sixty and participants were predominantly men. Afore starting the public value forum, researchers asked all participants to check their level of understanding about cyberterrorism and all participants have thorough or general understanding of cyberterrorism.

The study analyzes participants answers including positive and negative factors. Researchers asked participants to offer their input about which objectives and scenarios they think are least helpful in preventing cyberterrorism. The use of positive and negative factors that participants provides representation of the preference structure and braces predictive accuracy (Anderson et al., 2010).

### 4.2.3. Results of the Public Value Forum

Public value forum recommends having at least three experts and twenty non-experts. This study has eight experts and thirty non-experts and that gives the result of its public value forum more validity since it exceeds the minimal number of experts and non-experts to have valid values. The researchers did public forum of experts separately from the public forum of non-experts. Researchers collected the data from expert and non-expert participants and analyzed the findings. There are four parts of the results; first, researchers asked participants to use their preference to evaluate objectives and researchers registered initial overall and final importance rank, importance weight, swing rank, and swing weight. The initial overall is when participants started the public forum before they went through the rest of the survey and saw the different representations of relationships between objectives, attributes, and scenarios, i.e., before seeing each objective with its attributes then seeing it among other objectives and their attributes. Second, researchers asked participants to use their preference to importance rank and importance weigh scenarios assurance of satisfying each objective. Third, researchers asked participants to use their preference to importance rank, importance weigh, swing rank, and swing weigh scenarios. Fourth, researchers asked participants to use their preference to importance rank, importance weigh, swing rank, and swing weigh attributes of scenarios.

#### 4.2.3.1. Initial Overall and Final Importance Rank, Importance Weight, Swing Rank, and Swing Weight

Experts and non-experts had separate public forums and researchers analyzed the results of each group separately (table 4.2.3.1.1 and table 4.2.3.1.2). The values experts and non-experts offered when researchers asked them to use their preference the first round before they read all the objectives, attributes, and scenarios were the same values they offered afterwards as their final values. At the beginning of each public forum (one for experts group and one for non-experts group), researchers defined the five objectives and asked participants to use their preference to importance rank, importance weigh, swing rank, and swing weigh the five objectives.

Researchers use mean, median, and standard deviation to analyze the data. Researchers use standard deviation to measure the diversity of the dataset to show the diversity in the opinions of participants. Additionally, researchers use the mean and median to measure the central tendency of the dataset; researchers use mean to be able to predict any one value of the dataset with minimal error and they use median to show the middle score of the dataset. Mean Importance Weight, Coefficient of Variation Importance Weight, Mean Swing Weight, and Coefficient of Variation Swing Weight are important fields since they may tell the story of the data points. Mean Importance Weight and Mean Swing Weight show the difference in rank between different objectives. Additionally, Coefficient of Variation Importance Weight and Coefficient of Variation Swing Weight signposts if the data points distance to the mean are close or not. Therefore, Coefficient of Variation Importance Weight and Coefficient of Variation Swing Weight bare if the participants give close weights; that shows the level of agreement among participants.

**Table 4.2.3.1.1. Eight Experts Initial Overall Importance Rank, Importance Weight, Swing Rank, and Swing Weight**

| Objective | Ensure governance of technical infrastructure | Ensure critical infrastructure protection mechanisms are in place | Define a media response for cyberterrorist actions | Engage in counter cyberterrorism activities | Develop competencies for dealing with cyber terrorism activities |
|---|---|---|---|---|---|
| Mean Importance Rank | 3.13 | 1.75 | 4.75 | 3.5 | 1.88 |

| | | | | | |
|---|---|---|---|---|---|
| Median Importance Rank | 3 | 2 | 5 | 3.5 | 1.5 |
| Standard Deviation Importance Rank | 0.83 | 0.71 | 0.46 | 1.31 | 1.13 |
| Coefficient of Variation Importance Rank | 0.27 | 0.40 | 0.1 | 0.37 | 0.6 |
| *Mean Importance Weight* | *74.29* | *87.14* | *7.14* | *67* | *87* |
| Median Importance Weight | 84 | 95 | 0 | 85 | 99.5 |
| Standard Deviation Importance Weight | 28.94 | 23.43 | 18.9 | 41.72 | 28.12 |
| *Coefficient of Variation Importance Weight* | *0.4* | *0.27* | *2.65* | *0.62* | *0.32* |
| Mean Swing Rank | 3.63 | 2.13 | 4.5 | 3.33 | 1.75 |
| Median Swing Rank | 4 | 2 | 5 | 3.5 | 1.5 |
| Standard Deviation Swing Rank | 0.74 | 0.83 | 1.07 | 1.41 | 0.9 |
| Coefficient of Variation Swing Rank | 0.21 | 0.4 | 0.24 | 0.4 | 0.51 |
| *Mean Swing Weight* | *71.14* | *83.43* | *8.57* | *67.75* | *81.75* |
| Median Swing Weight | 80 | 90 | 0 | 85 | 99.5 |
| Standard Deviation Swing Weight | 34.46 | 24.27 | 22.7 | 42.26 | 30.85 |
| *Coefficient of Variation Swing Weight* | *0.48* | *0.291* | *2.65* | *0.62* | *0.4* |

Per table 4.2.3.1.1, experts appointed the highest importance weight mean and swing weight mean to the objective Ensure critical infrastructure protection mechanisms are in place. They say that cyberterrorists target critical infrastructure, e.g., oil and oil products production. Therefore, ensuring the protection of these critical infrastructure and employing backup systems may ensure that cyberterrorist attack will not achieve the damage level cyberterrorists want. Coefficient of Variation Importance Weight and Coefficient of Variation Swing Weight for the objective Ensure critical infrastructure protection mechanisms are in place are 0.2688308 and 0.29088765 respectively that is less than one and the least coefficient of variation among objectives. Therefore, they bare that experts agree on the weight and rank of this objectives more than they agree on the weight and rank of other objectives.

The experts have the highest swing weight standard deviation and importance weight standard deviation for the objective Engage in counter cyberterrorism activities. The experts are in different between counter attacking cyberterrorists and focus on defending information systems. On one hand, several of them say that counter attacking cyberterrorists will become cautious to cyberattack their information systems knowing that retribution will happen. On the other hand, several of them say that counter attacking cyberterrorists may have moral issues since it is hard to know the cyber attacker. Additionally, they say that counter attack consumes resources and it is more important to defend information systems rather than causing disorder because of different entities engaging in cyberattacks and counter cyberattacks.

The experts have the highest swing weight median, importance weight median, swing rank median, and importance rank median for the objective Develop competencies for dealing with cyber terrorism activities and it is close second to have the highest importance weight mean and swing weight mean. They say that preventing cyberterrorism consists of having trained people who have cyberterrorism awareness and tools capable of preventing cyberterrorism that they may use.

The experts have the lowest swing weight median and importance weight median for the objective Define a media response for cyberterrorist actions. The experts said that media response is the least important objective. They say it is more important to prepare people and infrastructure rather than spending resources on media response. However, they say defining media response for cyberterrorist actions is an important objective. Coefficient of Variation Importance Weight and Coefficient of Variation Swing Weight for the objective Define a media response for cyberterrorist actions are 2.645751311 which is greater than one. Therefore, they bare that experts give different weights and ranks for this objective and they think its weight and rank among objectives is contentious.

**Table 4.2.3.1.2. Thirty Non-Experts Initial Overall Importance Rank, Importance Weight, Swing Rank, and Swing Weight**

| Objective | Ensure governance of technical infrastructure | Ensure critical infrastructure protection mechanisms are in place | Define a media response for cyberterrorist actions | Engage in counter cyberterrorism activities | Develop competencies for dealing with cyber terrorism activities |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Mean Importance Rank | 1.93 | 2.26 | 4.63 | 2.92 | 3.15 |
| Median Importance Rank | 2 | 2 | 5 | 3 | 3 |
| Standard Deviation Importance Rank | 0.96 | 1.1 | 0.69 | 1.38 | 1.12 |
| Coefficient of Variation Importance Rank | 0.5 | 0.48 | 0.15 | 0.47 | 0.36 |
| *Mean Importance Weight* | *87.67* | *77.54* | *14.46* | *71* | *64.88* |
| Median Importance Weight | 95 | 90 | 0 | 85 | 80 |
| Standard Deviation Importance Weight | 20.89 | 27.9 | 29.65 | 34.18 | 32.85 |
| *Coefficient of Variation Importance Weight* | *0.23* | *0.34* | *2.02* | *0.5* | *0.5* |
| Mean Swing Rank | 2 | 2.41 | 4.5 | 2.73 | 3.36 |
| Median Swing Rank | 2 | 2 | 5 | 3 | 3.5 |
| Standard Deviation Swing Rank | 0.93 | 1.26 | 0.96 | 1.3 | 1.22 |
| Coefficient of Variation Swing Rank | 0.46 | 0.52 | 0.3 | 0.46 | 0.36 |
| *Mean Swing Weight* | *82.7* | *69.9* | *16.8* | *70.23* | *59.5* |
| Median Swing Weight | 95 | 80 | 0 | 85 | 80 |
| Standard Deviation Swing Weight | 21.5 | 31.2 | 31.23 | 31.59 | 37.14 |
| *Coefficient of Variation Swing Weight* | *0.25* | *0.5* | *1.8* | *0.5* | *0.62* |

Per table 4.2.3.1.2, non-expert participants appointed the highest importance weight mean and median in addition to swing weight mean and median to the objective Ensure governance of technical infrastructure. However, the objective experts chose (i.e. Ensure critical infrastructure protection mechanisms are in place) is close second and that shows close vision of objectives in general between non-experts and experts. The non-experts and experts think that if cyberterrorists can access infrastructure, they put people in danger. Therefore, they say that it is important to secure infrastructure and prepare it with technology to prevent cyberterrorist attacks. However, the objective Engage in counter cyberterrorism activities is close second in importance weight standard deviation. Coefficient of Variation Importance Weight is 0.348943897 and Coefficient of Variation Swing Weight 0.426522474. Therefore, non-experts have more confidence in ranking the objective Engage in counter cyberterrorism activities second when it is by itself, i.e., importance, but they are more contentious when comparing it to other objectives, i.e., swing. The experts have it as the highest importance weight standard deviation that shows similarity in the values of participants and it be because the non-experts participants have knowledge about cyberterrorism.

The non-experts have the lowest swing weight median and importance weight median for the objective Define a media response for cyberterrorist actions. Although defining media response came up from value-focused thinking and participants agreement that defining media response for cyberterrorist actions is an important objective, they think that it is the least important among the objectives.

Experts and non-experts weigh the objective Define a media response for cyberterrorist actions low among fundamental objectives (table 5.3.1.1 and table 5.3.1.2). Nonetheless, they say that it is an important objective thus analysis of data points bares that they are not confident about where they should rank it. Therefore, Coefficient of Variation Importance Weight and Coefficient of Variation Swing Weight are greater than one.

### 4.2.3.2. Initial Overall and Final Importance Rank, Importance Weight, Swing Rank, and Swing Weight

Researchers used attributes from scenarios A, B, and C to asked participants to evaluate how much these attributes ensure the implementation of an objective (e.g. table 4.2.3.2.1.1). Researchers think that evaluating the importance of scenarios A, B, and C becomes easier if the participants can evaluate within the context of the best attributes that satisfy the objective and the worst attributes that satisfy the objective. Researchers gave the highest importance to the attributes of Best Scenario and the least importance to the attributes of the Worst Scenario.

### 4.2.3.2.1. First Objective: Ensure Governance of Technical Infrastructure

**Table 4.2.3.2.1.1. Eight Experts Values on How Much Attributes of Scenarios A, B, and C Satisfy the First Fundamental Objective**

| **Objective: Ensure governance of technical infrastructure** | | | | |
|---|---|---|---|---|
| **Attributes** | Importance Weight | | | |
| | ***Mean*** | Median | Standard Deviation | ***Coefficient of Variation*** |
| Scenario A: Governmental<br>- Government supervises cyberterrorism governance<br>- Government analyzes and exchanges information about cyberterrorist attacks | ***64.75*** | 65 | 31.2 | ***0.5*** |
| Scenario B: Organizational<br>- Organizations handle their own infrastructure without supervision of the government<br>- Organizations check their information systems for threats<br>- Organizations analyze information about cyberterrorist attacks | ***68*** | 78.5 | 28.55 | ***0.5*** |
| Scenario C: Global<br>- UN suggests guidelines to handle cyberterrorism governance<br>- UN analyzes and exchanges information about cyberterrorism attacks among its members | ***41.13*** | 25 | 32.18 | ***0.78*** |

Experts weigh the objective Ensure governance of technical infrastructure as second among other fundamental objectives (table 4.2.3.1.1). At table 4.2.3.2.1.1, they offer coefficient of variation that is less than one so, data points are close to the mean. Experts gave the highest mean and median to attributes of Scenario B: Organizational (table 4.2.3.2.1.1) that define its approach of satisfying the objective of Ensure governance of technical infrastructure. Additionally, analysis of data points bares that attributes of Scenario B: Organizational have the lowest coefficient of variation and the closest data points to the mean among scenarios at table 4.2.3.2.1.1. They say the number of information systems to check and govern is huge for centralization, e.g., become the responsibility of the government of the United Nations, to fruitfully ensure governance of technical infrastructure. Hence, it is more utilitarian to ask organizations to govern their own technical infrastructure. Moreover, they say that organizations tendency to cut cost and outsourcing may affect the effectiveness of governing technical infrastructure.

The small value of standard deviations in addition to ranking scenarios as Scenario B: Organizational, Scenario A: Governmental, and then Scenario C: Global shows that experts agree that it is fruitful to hand governance of technical infrastructure to government the process of ensuring the governance of technical infrastructure. Although, its coefficient of variation is less than one, the coefficient of variation of Scenario C: Global is the highest among coefficient of variation at table 4.2.3.2.1.1. Therefore, analysis of data points bares that experts are in different of how much to weigh Scenario C: Global.

**Table 4.2.3.2.1.2. Thirty Non-Experts Values on How Much Attributes of Scenarios A, B, and C Satisfy the First Fundamental Objective**

| **Objective: Ensure governance of technical infrastructure** | | | | |
|---|---|---|---|---|
| **Attributes** | Importance Weight | | | |
| | ***Mean*** | Median | Standard Deviation | ***Coefficient of Variation*** |
| Scenario A: Governmental<br>- Government supervises cyberterrorism governance<br>- Government analyzes and exchanges information about cyberterrorist attacks | ***79.57*** | 90 | 19.48 | ***0.24*** |

|  |  |  |  |  |
|---|---|---|---|---|
| Scenario B: Organizational<br>- Organizations handle their own infrastructure without supervision of the government<br>- Organizations check their information systems for threats<br>- Organizations analyze information about cyberterrorist attacks | ***66.1*** | 75 | 25.38 | ***0.38*** |
| Scenario C: Global<br>- UN suggests guidelines to handle cyberterrorism governance<br>- UN analyzes and exchanges information about cyberterrorism attacks among its members | ***41.56*** | 45 | 28.21 | ***0.7*** |

Non-experts weigh the objective Ensure governance of technical infrastructure as the highest among other fundamental objectives (table 4.2.3.1.1.2). The values of coefficient of variation for the three scenarios are less than one so, analysis of data points bares that data points are close to the mean. Non-experts offer the highest mean and median to attributes of Scenario A: Governmental (table 4.2.3.2.2) that define its approach of satisfying the objective of Ensure governance of technical infrastructure. Non-experts say that they trust the government to govern technical infrastructure than organizations. They additionally think that having United Nations to govern technical infrastructure is centralization that disrupts the effectiveness of governing technical infrastructure at UN member states.

Both experts and non-experts are say that centralization messes up ensuring governance of technical infrastructure (table 4.2.3.2.1.1 and table 4.23.2.1.2). Yet, non-experts have trust factor in addition to competency. Non-experts say they trust government over organizations to ensure governance of technical structure. Therefore, trust factor urged non-experts to prefer attributes of Scenario A: Governmental that define its approach of satisfying the objective of Ensure governance of technical infrastructure.

#### 4.2.3.2.2. Second Objective: Ensure Critical Infrastructure Protection Mechanisms are in Place

**Table 4.2.3.2.2.1. Eight Experts Values on How Much Attributes of Scenarios A, B, and C Satisfy the Second Fundamental Objective**

| **Objective: Ensure critical infrastructure protection mechanisms are in place** | | | | |
|---|---|---|---|---|
| **Attributes** | Importance Weight | | | |
| | ***Mean*** | Median | Standard Deviation | ***Coefficient of Variation*** |
| Scenario A: Governmental<br>- Government develops a plan for data loss<br>- Government owns backup servers and do not outsource their maintenance<br>- Government implements spam prevention on all servers in the nation<br>- Government demands organizations to use SCADA | ***67.38*** | 62.5 | 18.65 | ***0.3*** |
| Scenario B: Organizational<br>- Organizations develop their own data loss plan<br>- Organizations own their own backup servers<br>- Organizations implement their own spam prevention<br>- Organizations decide to use SCADA or not without governmental supervision | ***77.13*** | 90 | 30.1256 | ***0.4*** |
| Scenario C: Global<br>- UN develops guidelines for data loss plan<br>- UN supply its members with backup servers<br>- UN suggests spam prevention guidelines<br>- UN offers guidelines and suggests using SCADA | ***33.75*** | 30 | 24.0401 | ***0.71*** |

Experts weigh the objective Ensure critical infrastructure protection mechanisms are in place as the highest among other fundamental objectives (table 4.2.3.1.1). Experts gave the highest mean and median to attributes of Scenario B: Organizational (table 4.2.3.2.2.1) that define its approach of satisfying the objective of Ensure critical infrastructure protection mechanisms are in place. They say that the usefulness of using Supervisory Control And Data Acquisition (SCADA) depends on the operational team and resource. Therefore, they recommend that organizations choose how to want to use SCADA. They think decentralization is easier when it comes to using SCADA and deploying it.

**Table 4.2.3.2.2.2. Thirty Non-Experts Values on How Much Attributes of Scenarios A, B, and C Satisfy the Second Fundamental Objective**

| **Objective: Ensure critical infrastructure protection mechanisms are in place** | | | | |
|---|---|---|---|---|
| Attributes | Importance Weight | | | |
| | ***Mean*** | Median | Standard Deviation | ***Coefficient of Variation*** |
| Scenario A: Governmental<br>- Government develops a plan for data loss<br>- Government owns backup servers and do not outsource their maintenance<br>- Government implements spam prevention on all servers in the nation<br>- Government demands organizations to use SCADA | ***76.5*** | 90 | 24.88 | ***0.33*** |
| Scenario B: Organizational<br>- Organizations develop their own data loss plan<br>- Organizations own their own backup servers<br>- Organizations implement their own spam prevention | ***70.9*** | 80 | 21.2512 | ***0.3*** |

| | | | | |
|---|---|---|---|---|
| - Organizations decide to use SCADA or not without governmental supervision | | | | |
| Scenario C: Global<br>- UN develops guidelines for data loss plan<br>- UN supply its members with backup servers<br>- UN suggests spam prevention guidelines<br>- UN offers guidelines and suggests using SCADA | ***38.96*** | 35 | 28.4813 | ***0.73*** |

Non-experts weigh the objective Define a Ensure critical infrastructure protection mechanisms are in place as second among other fundamental objectives (table 4.2.3.2.2.2). Non-experts say that government should control data backups to keep data backups within the borders of the country and they think outsourcing data backups may create a national threat. Therefore, they had scenario B second concerned with organizational outsourcing and scenario C third concerned with having other countries control the data backup policy.

### 4.2.3.2.3. Third Objective: Define a Media Response for Cyberterrorist Actions

**Table 4.2.3.2.3.1. Eight Experts Values on How Much Attributes of Scenarios A, B, and C Satisfy the Third Fundamental Objective**

| **Objective: Define a media response for cyberterrorist actions** | | | | |
|---|---|---|---|---|
| **Attributes** | Importance Weight | | | |
| | ***Mean*** | Median | Standard Deviation | ***Coefficient of Variation*** |
| Scenario A: Governmental | ***44.75*** | 35 | 28.96 | ***0.65*** |

| | | | | |
|---|---|---|---|---|
| - Government develops a plan for data loss<br>- Government owns backup servers and do not outsource their maintenance<br>- Government implements spam prevention on all servers in the nation<br>- Government demands organizations to use SCADA | | | | |
| Scenario B: Organizational<br>- Organizations develop their own data loss plan<br>- Organizations own their own backup servers<br>- Organizations implement their own spam prevention<br>- Organizations decide to use SCADA or not without governmental supervision | ***73*** | 87 | 28.43 | ***0.4*** |
| Scenario C: Global<br>- UN develops guidelines for data loss plan<br>- UN supply its members with backup servers<br>- UN suggests spam prevention guidelines<br>- UN offers guidelines and suggests using SCADA | ***40.88*** | 35 | 28.23 | ***0.7*** |

Experts and non-experts think the objective Define a media response for cyberterrorist actions to be the least important fundamental objective (table 4.2.3.1.1). Nonetheless, experts say that organizational media response is better than centralizing the response for cyberterrorist actions. The three coefficients of variations At table 4.2.3.2.3.1 are 0.64708077, 0.38938823, and 0.690663539, i.e., each less than one. The mean of importance weight experts offer bares that they favor Scenario B: Organizational. Additionally, the coefficient of variation for scenario B is the least among scenarios at table 4.2.3.2.3.1. Therefore, analysis of data points bares that data points are closer to the mean than data points of scenarios A and C. They say having different organizations responding for cyberterrorist actions may prevent governmental intervention and gives the government more room to and time to decide on what may be the proper response to the cyberterrorist action.

Experts weigh governmental and international media response around 28.25 mean lower than organizational with small standard deviation (table 4.2.3.2.3.1). Hence, experts are confident that organizational definition of media response for cyberterrorist actions is better than governmental and international.

**Table 4.2.3.2.3.2. Thirty Non-Experts Values on How Much Attributes of Scenarios A, B, and C Satisfy the Third Fundamental Objective**

| **Objective: Define a media response for cyberterrorist actions** | | | | |
|---|---|---|---|---|
| **Attributes** | Importance Weight | | | |
| | ***Mean*** | Median | Standard Deviation | ***Coefficient of Variation*** |
| Scenario A: Governmental<br>- Government develops a plan for data loss<br>- Government owns backup servers and do not outsource their maintenance<br>- Government implements spam prevention on all servers in the nation<br>- Government demands organizations to use SCADA | ***63.11*** | 77 | 28.74 | ***0.46*** |
| Scenario B: Organizational<br>- Organizations develop their own data loss plan<br>- Organizations own their own backup servers<br>- Organizations implement their own spam prevention<br>- Organizations decide to use SCADA or not without governmental supervision | ***67.7*** | 75.5 | 25.73 | ***0.38*** |
| Scenario C: Global<br>- UN develops guidelines for data loss plan<br>- UN supply its members with backup servers<br>- UN suggests spam prevention guidelines<br>- UN offers guidelines and suggests using SCADA | ***37.35*** | 27.5 | 29.7 | ***0.8*** |

Non-experts weigh the objective Define a media response for cyberterrorist actions as fifth among other objectives (table 4.2.3.1.2). The coefficients of variations among scenarios at table 4.2.3.2.3.2 are each less than one, i.e., analysis of data points bares that data points are close to the mean. The mean difference of the weight from non-experts between scenario B and A are less than the one of the experts. Nonetheless, non-experts think by more than 12 mean and small standard deviation that having organizational definition of media response for cyberterrorist actions is more important than governmental and international (table 4.2.3.2.3.2). Additionally, scenario B has the least coefficient of variation among scenarios at table 4.2.3.2.3.2, i.e., analysis of data points bares that data points are closer to the mean than the data point of scenarios A and C. Moreover, the small standard deviation may show that there is small variation in the answers non-experts offered.

Experts and non-experts think the objective Define a media response for cyberterrorist actions to be the least important fundamental objective. Additionally, they both think with confidence that it is better to have an organizational definition of media response for cyberterrorist actions rather than governmental and international.

#### 4.2.3.2.4. Fourth Objective: Engage in Counter Cyberterrorism Activities

**Table 4.2.3.2.4.1. Eight Experts Values on How Much Attributes of Scenarios A, B, and C Satisfy the Fourth Fundamental Objective**

| Objective: Engage in counter cyberterrorism activities | |
|---|---|
| **Attributes** | Importance Weight |

| | ***Mean*** | Median | Standard Deviation | ***Coefficient of Variation*** |
|---|---|---|---|---|
| Scenario A: Governmental<br>- Government gathers information about cyber activities of all servers in the nation<br>- Government uses attacks on severs in the nation to launch cyber-attacks on attackers | ***71.25*** | 70 | 26.5 | ***0.37*** |
| Scenario B: Organizational<br>- Organizations gather its own information about cyberterrorism without governmental supervision<br>- Organizations launch their own cyber-attacks on attackers without consulting with the government | ***57.63*** | 62.5 | 30.98 | ***0.54*** |
| Scenario C: Global<br>- UN gathers information about cyberterrorism<br>- UN launches its own cyber-attacks on countries and organizations in retaliation of their cyber-attacks based on UN voting | ***37.75*** | 26 | 34.85 | ***0.92*** |

Experts weigh the objective Engage in counter cyberterrorism activities as fourth among other objectives (table 4.2.3.1.1). The coefficient of variation of table 4.2.3.2.4.1 are each less than one, i.e., analysis of data points bares that data points are close to the mean. Additionally, the coefficient of variation for scenario A is the least among scenarios at table 4.2.3.2.4.1.

Per table 4.2.3.2.4.1, experts appointed the highest importance weight mean and median to attributes of Scenario A: Governmental that define its approach of satisfying the objective of Engage in counter cyberterrorism activities. They say that the attributes defining scenario A are the most suitable for countering cyberterrorism activities because centralization works better for such cases. Hence, it is more utilitarian to ask government to govern counter cyberterrorism activities. And for the same reason experts say that scenario B is the second most important among the three followed by scenario C;

international governing is the least centralize among the three scenarios in table 4.2.3.2.4.1.

Per table 4.2.3.2.4.1, coefficients of variations are less than one. Therefore, experts offer data points that are close to the mean. Moreover, it bares that experts offer close weights when weighting the scenarios at table 4.2.3.2.4.1. However, experts offer closest weights for scenario A and least close weights for scenario C. Experts say that government should rheostat the engagement in counter cyberterrorism activities, but they were hesitant about the weight of engaging UN in countering cyberterrorism. On one hand, they say that scenario C may be insufficient given that it is hard for one government to agree among itself on activities to counter cyberterrorism so, having more than one country deciding may be deficient. On the other hand, they say that having the UN regulate these activities may prevent hostile between different nations and add legitimacy to these activities.

**Table 4.2.3.2.4.2. Thirty Non-Experts Values on How Much Attributes of Scenarios A, B, and C Satisfy the Fourth Fundamental Objective**

| **Objective: Engage in counter cyberterrorism activities** | | | | |
|---|---|---|---|---|
| **Attributes** | Importance Weight | | | |
| | ***Mean*** | Median | Standard Deviation | ***Coefficient of Variation*** |
| **Scenario A: Governmental**<br>**- Government gathers information about cyber activities of all servers in the nation**<br>**- Government uses attacks on severs in the nation to launch cyber-attacks on attackers** | ***72.11*** | 87.5 | 28.88 | ***0.4*** |
| **Scenario B: Organizational** | ***53.85*** | 60 | 31.55 | ***0.6*** |

| | | | | |
|---|---|---|---|---|
| **- Organizations gather its own information about cyberterrorism without governmental supervision**<br>**- Organizations launch their own cyber-attacks on attackers without consulting with the government** | | | | |
| **Scenario C: Global**<br>**- UN gathers information about cyberterrorism**<br>**- UN launches its own cyber-attacks on countries and organizations in retaliation of their cyber-attacks based on UN voting** | ***46.52*** | 50 | 32.211 | ***0.7*** |

Non-experts weigh the objective Engage in counter cyberterrorism activities as third among other objectives (table 4.2.3.1.2). Per table 4.2.3.2.4.2, non-experts appointed the highest importance weight mean and median to attributes of Scenario A: Governmental that define its approach of satisfying the objective of Engage in counter cyberterrorism activities.

They say that the attributes defining scenario A are the most suitable for countering cyberterrorism activities because centralization works better for such cases. Hence, it is more utilitarian to ask government to govern counter cyberterrorism activities. And for the same reason experts and non-experts say that scenario B is the second most important among the three followed by scenario C; international governing is the least centralize among the three scenarios in table 4.2.3.2.7.

Per table 4.2.3.2.4.2, non-experts offer data points that are close to the mean. Hence, their coefficients of variations are less than one. Grippingly, they offer close coefficients of variations for scenarios B and C 0.603127089 and 0.69686649 respectively.

Additionally, their means are around ten points difference where experts offer around twenty points difference in the mean of scenarios B and C. Hence, non-experts consider the engagement in counter cyberterrorism activities as an internal matter and that centralization makes it operative. On the other hand, experts are hesitant about how low they should weigh scenario C for the fourth objective.

### 4.2.3.2.5. Fifth Objective: Develop Competencies for Dealing with Cyberterrorism Activities

**Table 4.2.3.2.5.1. Eight Experts Values on How Much Attributes of Scenarios A, B, and C Satisfy the Fifth Fundamental Objective**

| Objective: Develop competencies for dealing with cyberterrorism activities | | | | |
|---|---|---|---|---|
| Attributes | Importance Weight | | | |
| | *Mean* | Median | Standard Deviation | *Coefficient of Variation* |
| Scenario A: Governmental<br>- Government supervises the readiness of technical staff in all the nation<br>- Government handles cyber protection on all servers in the nation<br>- Government supervises activities of employees in all the nation | *73.75* | 89 | 27.63 | *0.38* |
| Scenario B: Organizational<br>- Organizations supervise the readiness of their employees without governmental supervision<br>- Organizations handle their cyber protection without governmental supervision | *63.38* | 80 | 36.304 | *0.58* |
| Scenario C: Global<br>- UN rates the cybersecurity readiness of each country<br>- UN handles cyber protection of its members | *38.63* | 37.5 | 29.83 | *0.78* |

The eight experts ranked the fifth objective of Develop competencies for dealing with cyber terrorism activities as the second among other fundamental objectives (table 4.2.3.1.1). Experts public value forum did not have a high standard deviation showing that experts data points are close to the mean. They say that dealing with cyberterrorism via developing technical competencies is governmental responsibility since the government should oversee the readiness of technical staff in all the nation.

Per table 4.2.3.2.5.1, data points non-experts offer have coefficients of variations that are less than one. Hence, they are close to their means. Therefore, experts offer close weights for scenarios at table 4.2.3.2.5.1.

**Table 4.2.3.2.5.2. Thirty Non-Experts Values on How Much Attributes of Scenarios A, B, and C Satisfy the Fifth Fundamental Objective**

| Objective: Develop competencies for dealing with cyberterrorism activities | | | | |
|---|---|---|---|---|
| Attributes | Importance Weight | | | |
| | *Mean* | Median | Standard Deviation | *Coefficient of Variation* |
| Scenario A: Governmental<br>- Government supervises the readiness of technical staff in all the nation<br>- Government handles cyber protection on all servers in the nation<br>- Government supervises activities of employees in all the nation | *71.78* | 80 | 26.39 | *0.36* |
| Scenario B: Organizational<br>- Organizations supervise the readiness of their employees without governmental supervision<br>- Organizations handle their cyber protection without governmental supervision | *61.85* | 70 | 27.79 | *0.48* |
| Scenario C: Global<br>- UN rates the cybersecurity readiness of each country<br>- UN handles cyber protection of its members | *43.11* | 42.5 | 31.44 | *0.72* |

Non-experts rank the fifth objective of Develop competencies for dealing with cyberterrorism activities as fourth among objectives (table 4.25.3.1.2). Hence, they say that the competencies for dealing with cyberterrorism develops after securing infrastructures and facilities in addition to countering cyberterrorism activities.

Per table 4.2.3.2.5.2, the coefficients of variations for data points from non-experts are less than one. Hence, non-experts offer data points that are close to the mean. Therefore, data analysis bares that many of them offer close importance weights.

# Chapter 5: Discussion

This study incorporates value focused thinking and public value forum offering an innovative approach to discover strategic measures and alternatives for complex policy decisions for preventing cyberterrorism. This socio-organizational study reconnoiters a newfangled area of cyberterrorism in the field of information systems. For example, it uses the output of a qualitative methodology as an input to a quantitative methodology. Hence, employs the methodologies of value focused thinking and public value forum to reveal the policy values of decision alternatives for complex policy decisions. Using one the methodologies are capable to bare alternative for policy decision making. Moreover, this study uses the befits of both methodologies to discover the decision alternatives for policy decision making. Hence, it uses the output of value focused thinking and plugs it to serve as an input for public value forum.

This study uses several decision-making theories, e.g., evidential decision making, normative decision-making theory, and utility theory. In addition, it uses several statistical analysis techniques, e.g., conjoint analysis and multidimensional scaling. The study uses techniques from normative decision theory to analyze and explain participants input and the rational of their decisions when offering weights in chapter 5. Utility theory explains the connection between decision and preference and the influence of preference on decision-maker. The study shows that when explaining the different decisions experts and non-experts made. Hence, utility shows the uniqueness of subject's preference and judgment. The statistical technique of conjoint analysis's fundamental concept is utility. Utility definition requires conjoint task. Conjoint task defines attributes to construct hypothetical choice situations. Conjoint task includes four aspects:

1) Attributes that are the more important than others;

2) How subjects can understand the level of each attribute, e.g., understating the difference between price and quality;

3) Prediction of subject's evaluated aspects of attributes;

4) The number of profiles that are subjects evaluate.

This study combines two methodologies that scholars use for eliciting values that helps in policy decision making; value focused thinking and public value forum (see figure 5.1). Although scholars may use one of the methods to aid policy decision making, this study offers the reliability of using two methodologies. Hence, it implements value focused thinking and converts its output, i.e., fundamental objectives and means objectives, to objectives and attributes that are the input of public value forum.

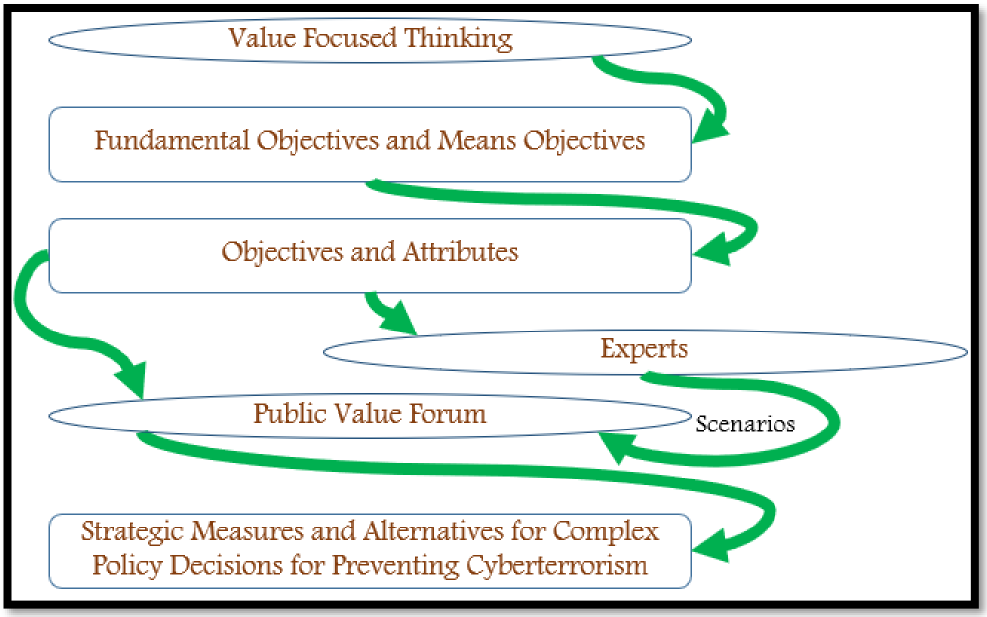
Value Focused Thinking
Fundamental Objectives and Means Objectives
Objectives and Attributes
Experts
Public Value Forum
Scenarios
Strategic Measures and Alternatives for Complex Policy Decisions for Preventing Cyberterrorism

**Figure 5.1. The Combination between Value Focused Thinking and Public Value Forum**

Combining these two methodologies offers input to public value forum. Hence, value focused thinking systematically derives the fundamental objectives and means objectives. The combination offers a combination between qualitative methodology, i.e., value focused thinking, and quantitative methodology, i.e., public value forum. Per the definition of the relationship between fundamental objectives and means objectives for value focused thinking, means objectives are the means to reach the fundamental objectives. Similarly, public value forum says that attributes are means to satisfy the objectives. Therefore, this study converts fundamental objectives to objectives and attributes.

Although few may say that there were not enough data to measure the decision alternatives and objectives because the number of experts that evaluated the decision alternatives and the number of subjects created that objectives, Hubbard & Seiersen (Hubbard & Seiersen, 2016) said that such claim is does not have an actual math to support it. They said that using small samples can offer informative inferences. This dissertation says that increasing the size of the sample does not increase generalizability. Generalizability is the abstraction of instances to make a general notion predicts the behavior of similar instances (Lee & Baskerville, 2003). Increasing the size of the sample can simply mean more variation within a population. Moreover, increasing the sample size does not mean that the inductive general statement is correct.

Scientific theory can use rational abstraction for prediction and replication of the behavior of certain instances thus generalize based on Lee and Baskerville definition of generalization (Lee & Baskerville, 2003) (p. 221). "Scientific theory employs hypothetico-deductive logic" (pp. 229) thus hypothetico-deductive logic is more generalizable over inductive logic. Increasing sample size of a random sample increases reliability of that sample-based estimates and does not give more generalizability to any population characteristics (Lee & Baskerville, 2003) (p. 226). This research employs hypothetico-deductive logic to generalize. It uses valid theories per experts and literature and combine them with input of the subjects to use in the objectives emerged.

Hypothetico-deductive logic uses deductive reasoning and makes research more generalizable. Deductive reasoning is the process of logical reasoning from theoretical statements (major and minor premises) to empirical or conclusion statements. It can lead a scientist to craft logically consist and empirical theory’s propositions (Lee & Baskerville, 2003) (p. 229). Performing controlled deduction is harder than in mathematical analysis since qualitative analysis does not have the “corresponding body of rules as succinct or easily applies as the rules of algebra" (Lee, 1989) (p. 40). However, using proper qualitative analysis, i.e., deduction with verbal propositions, "does not deprive itself of the rules of formal logic, to which it may therefore still turn when carrying out the task of making controlled deductions" (p. 40). Hypothetico-deductive logic starts with a theory and "employs the deductive logic of the syllogism, in contrast to inductive logic" (Lee & Baskerville, 2003) (p. 229).

## 5.1. Exploring Cyberterrorism Prevention Objectives

This study uses value focused thinking which elicits the values of participants to form fundamental objectives and means objectives. This study qualitatively investigates and reveals thirty-five actionable objectives where five of them are fundamental objectives and thirty are means objectives (figure 4.1.3). Institutions and governments may use fundamental objectives and means objectives to allocate resources for preventing cyberterrorism. These objectives are for introducing measures and protections for preventing cyberterrorism.

These objectives are the essence for measures to use in policy making and decision.

## 5.2. Decision Making

This study elicits values through public forum using a combination of survey, indirect public value elicitation, direct public value elicitation, focus groups, and engagement of the public. The value-focused thinking shows that the objective Define a media response for cyberterrorist actions is important fundamental objective. However, public forum shows that it is an important objective, but it is the least important objective when it comes to weighing decision alternatives and implementing the objectives. Analysis of data points bares that highest weights have the least coefficient of variation among other items, i.e., data points of highest items are closer to the mean than other items and many participants weigh it as the highest.

Although experts and non-experts have different rank of fundamental objectives (tables 4.2.3.1.1 and 4.2.3.1.2), they offer the same ranking of scenario attributes of fundamental objectives (tables 4.2.3.2.5 and 4.2.3.2.6, and 4.2.3.2.4.1 and 4.2.3.2.4.2). Experts and non-experts weigh the objectives based on their value of the objective importance among objectives. Hence, the objective with 100% weight is the one that they think is foundational for the rest of objectives like the importance weight of entities of a building (see figure 5.1).

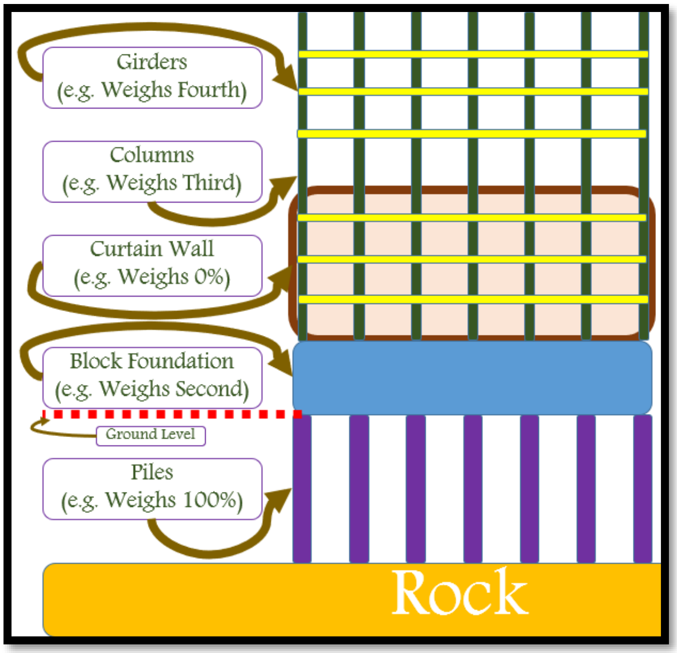

**Figure 5.2.1. Cross Section of a Building Showing Its Foundational Parts and The Importance Weight of Each Foundational Entity**

### 5.2.1. Objectives

Experts think that securing infrastructure is important via protection mechanisms, i.e., second objective Ensure critical infrastructure protection mechanisms are in place, thus they weigh the first objective as 100%. They think that securing the infrastructure through protection mechanisms helps implementing the rest of the objectives. Hence, they say infrastructure is the most sensitive entity that cyberterrorist may get a great revenge if they successfully debilitate. Besides, experts say that securing the infrastructure through automating the steps that governments, organizations, and UN members should take is assurance of safety that is important for any activity. Next, experts say that after the second objective it is time to be ready through securing other facilities that are less important than infrastructure. Therefore, they weigh the fifth objective Develop competencies for dealing with cyberterrorism activities as second among objectives. After securing infrastructures and other facilities, experts say it is time for having policy compliance for information systems security. They say that the policy should build on supporting the security of infrastructures and other facilities. Ensuing, creating activities to counter cyberterrorism, i.e., the fourth objective. Experts say that after managing internal affairs, it is time to go after cyberterrorists and retaliate to debilitate their cyber attacking competencies. After protecting and attacking, experts say that it is time to publicly address cyberterrorism activities and inform the public about cyberterrorists actions.

**Table 5.2.1.1. Shows the Experts Rank and Non-Experts Rank of Objectives for Preventing Cyberterrorism**

| Objective | Experts Rank | Non-Experts Rank |
|---|---|---|
| **Ensure governance of technical infrastructure** | 3 | 1 |
| **Ensure critical infrastructure protection mechanisms are in place** | 1 | 2 |
| **Define a media response for cyberterrorist actions** | 5 | 5 |
| **Engage in counter cyberterrorism activities** | 4 | 3 |
| **Develop competencies for dealing with cyber terrorism activities** | 2 | 4 |

### 5.2.2. Attributes

Statistical analysis bares a trend in the trend of expert and non-expert participants that they tend to respectively prefer securing infrastructure, improving the ability to respond to cyberterrorist attacks, and communicating about the cyberterrorist attacks. Correspondingly, participants prefer governmental regulations instead of organizational. However, experts (and unlike non-experts) tend to prefer domestic regulations over international. Hence, experts trust in decentralizing the process of preventing cyberterrorism to suit different country needs and reduce centralization overhead. Therefore, experts rank Scenario C: Global lower than scenarios A and B. On the other hand, non-experts tend to believe that organizations may cut corners and outsource sensitive national information. Therefore, they prefer international governmental control over organizational.

**Table 5.2.2.1. Swing Ranks Per Scenarios and Groups**

| **Attributes of Scenarios** | **Experts** | | **Non-Experts** | |
|---|---|---|---|---|
| | **Mean** | **Median** | **Mean** | **Median** |
| **Best Scenario** | ***1.6*** | ***2*** | ***1.5*** | ***1*** |
| **Scenario A: Governmental** | 2.6 | 3 | 2.625 | 2.5 |
| **Scenario B: Organizational** | 3.4 | 3 | ***4.375*** | ***5*** |
| **Scenario C: Global** | 3.2 | 4 | 3.5 | 3.5 |
| **Worst Scenario** | ***4.2*** | ***5*** | 3 | 3 |

Per table 5.2.2.1, non-experts prefer the attributes of worst scenario over allowing organizational control of preventing cyberterrorism. On the other hand, experts rank attributes of the worst scenario the lowest. Table 6.2.1 and interviews with participants bare that experts prefer decentralization in developing robust competencies to prevent cyberterrorism.

### 5.2.3. Scenarios

Participants prefer Scenario B: Organizational to satisfy the objectives Ensure critical infrastructure protection mechanisms are in place and Define a media response for cyberterrorist actions. In addition, they prefer Scenario A: Governmental for objectives Engage in counter cyberterrorism activities and Develop competencies for dealing with cyber terrorism activities. However, experts prefer Scenario B: Organizational for objective Ensure governance of technical infrastructure where non-experts prefer Scenario A: Governmental.

**Table 5.2.3.1. Scenario Type Experts Group and Non-Experts Group Prefer for Each Objective**

| Objective | Scenario Experts Prefer | Scenario Non-Experts Prefer |
|---|---|---|
| Ensure governance of technical infrastructure | Organizational | Governmental |
| Ensure critical infrastructure protection mechanisms are in place | Organizational | Organizational |
| Define a media response for cyberterrorist actions | Organizational | Organizational |
| Engage in counter cyberterrorism activities | Governmental | Governmental |
| Develop competencies for dealing with cyber terrorism activities | Governmental | Governmental |

The findings suggest that participants prefer preventing cyberterrorism using domestic means. Per table 5.2.3.1, participants do not prefer international interference in preventing cyberterrorism over domestic. Correspondingly, non-experts think that organizations may outsource controls and information they use for preventing cyberterrorism. However, non-experts think that may lead to security breach either by the local government where the outsource is taking a place or by intercepting the communications between outsourcing organization and organization where outsourcing is taking place. On the other hand, experts think that they like to govern their own organizational technical infrastructure while collaborate with government.

### 5.2.4. In Case of Different Ranking

Sections 5.3.2. Initial Overall and Final Importance Rank, Importance Weight, Swing Rank, and Swing Weight, 5.2.1. Objectives, 5.2.2. Attributes, and 5.2.3. Scenarios show that experts ranking of values may be different than non-experts. The methodology of public value forum does a good at implementing the objectives. In addition, it does not need condensing. However, this study considers the rank of the group that influence a value. Therefore, expert participants rank of objectives Ensure governance of technical infrastructure, Ensure critical infrastructure protection mechanisms are in place, and Engage in counter cyberterrorism activities is more important than non-expert participants rank of these objectives (see table 5.2.4.1). Hence, information security experts have more authority over values that ensures the governance of technical infrastructure to maintain their security, e.g., monitoring cyberterrorist threats, learning from past cyberterrorist attacks, and allocating responsibilities and accountability for preventing cyberterrorism. In addition, they control values that employ protection mechanism to recover from cyberterrorist attacks on infrastructure, e.g., the use of Supervisory Control and Data Acquisition (SCADA) systems, spam prevention, and plans for governmental data loss. Finally, expert participants control the readiness of countering cyberterrorism activities, e.g., intelligence gathering for cyberterrorism detection and prevention and response to cyberterrorists attacks proactively.

**Table 5.2.4.1. Attributes of Objectives that Expert Participants Have Influence on More Than Non-Expert**

| Objectives | Attributes |
|---|---|
| **Ensure governance of technical infrastructure** | Ensure there is learning from past events |
| | Assure constant monitoring of threats |
| | Allocate clear roles and responsibilities for cyberterrorism governance |
| **Ensure critical infrastructure protection mechanisms are in place** | Increase use of Supervisory Control and Data Acquisition (SCADA) systems |
| | Prevent spam |
| | Treat backup locations as a national security issue |
| | Develop contingency plans for governmental data loss |
| **Engage in counter cyberterrorism activities** | Engage in intelligence gathering for cyberterrorism detection and prevention |
| | Counter cyberterrorists attacks proactively |

On the other hand, non-expert participants rank of objectives Define a media response for cyberterrorist actions and Develop competencies for dealing with cyber terrorism activities is more important than expert participants rank of these objectives (see table 5.2.4.2). Hence, the public common internet users have more control over these objectives than information security expert participants. Educating the public about cyberterrorism prevention involves understanding the values of the public and non-expert participants are influencing these objectives and their attributes, e.g., educating about the danger of cyberterrorism, developing an appropriate media response, training staff about cyberterrorism, and engaging and sharing about practices to prevent cyberterrorism.

**Table 5.2.4.2. Attributes of Objectives that Non-Expert Participants Have Influence on More Than Expert**

| Objectives | Attributes |
|---|---|
| **Define a media response for cyberterrorist actions** | Increase media coverage to match the danger of cyberterrorism |
| | Develop a media response strategy for cyberterrorism |
| **Develop competencies for dealing with cyber terrorism activities** | Ensure technical staff have up to date knowledge |
| | Engage in strategically thinking about cyberterrorism protection |
| | Define mechanisms to get security feedback from individuals |
| | Train individuals on modern technologies |

Per tables 5.2.4.2 and 5.2.4.1, the best scenario for objective Ensure governance of technical infrastructure is Scenario B: Organizational. Hence, information security experts have authority over ensuring the maintaining of cybersecurity of infrastructure against cyberterrorist attacks. The expert and non-expert participants have different scenario preference of fundamental objective Ensure governance of technical infrastructure because of experts' trust in organizational governance of technical infrastructure and non-experts' trust in governmental. However, expert and non-expert participants have similar scenario preference of fundamental objectives Ensure critical infrastructure protection mechanisms are in place, Define a media response for cyberterrorist actions, Engage in counter cyberterrorism activities, and Develop competencies for dealing with cyber terrorism activities.

**Table 5.2.4.3. This Study Suggests These Scenarios for Objectives**

| Objective | Scenario Experts Prefer |
|---|---|
| Ensure governance of technical infrastructure | Organizational |
| Ensure critical infrastructure protection mechanisms are in place | Organizational |
| Define a media response for cyberterrorist actions | Organizational |
| Engage in counter cyberterrorism activities | Governmental |
| Develop competencies for dealing with cyber terrorism activities | Governmental |

This study enhances the public value forum and proposes solution for the case of groups offering different ranks. The proposal is using the rank of the group that influences and controls the values the most. Per literature review, no other study propose a way to solve the challenge of having groups offer different ranks for the public value forum especially for cyberterrorism prevention.

# Chapter 6: Conclusions

This study involves the socio-technical prospective to ensure the implementation of security measures through creating objectives that are based on the input of common internet users and trusted cybersecurity exports for preventing cyberterrorism. The study also creates a decision framework to reveal how cybersecurity experts encounter cyberterrorism attacks. Robert Tapan Morris developed the Morris worm in 1988. The Morris worm is the first recognized worm to attack the world's cyber infrastructure. Cyberterrorism is a growing threat that needs the attention of individuals, organizations, and governments. There are over 31,300 magazine and journal articles written on cyberterrorism. However, there is not enough literature and practices about what to do in the case of cyberterrorism. Experts suggest that wars are going to include cyberattacks along with conventional military attacks.

The internet is for several types of communication, thus, developing public policy for preventing cyberterrorism is an effective solution to its challenges. It is important to understand the values offered by individuals to prevent cyberterrorism in the context of cybersecurity. This empirical study conducted interviews of individuals about their belief on how to prevent cyberterrorism at personal, organizational, and governmental levels. The results categorized in objectives and logically classified by means and fundamental goals. These results explain the concerns that individuals have about cyberterrorism. These objectives apply to designing security policy and its measures. This study develops objectives to prevent cyberterrorism. The development of the objectives consists of three steps: finding values, structuring values, and organizing objectives. Policy makers can use revealed fundamental objectives and mean objectives to create a policy for preventing cyberterrorism.

Cyberterrorists use cyber-attacks to cause harm and influence governments, organizations, and individuals is growing at a threating rate. However, many studies focus on developing new encryption algorithms and new security apps which is important, but it is not the only aspect to maintain security. These studies do not take into consideration the socio-technical structure and influence that decides the implementation of security measures like security software. Armies use cyber-attacks as the first wave of attack in several recent wars. A special cyber-attack is the one used by terrorist organizations and groups to achieve and help their goals.

This study involves the socio-technical prospective to ensure the implementation of security measures through creating objectives based on the input of common internet users and trusted cybersecurity exports for preventing cyberterrorism. The study also creates a decision framework to reveal how cybersecurity experts lever cyberterrorism attacks.

Cyberterrorism is a growing threat that needs individuals, organizations, and governments to pay attention to. Internet is for several types of communication, thus, developing public policy for preventing cyberterrorism is effective solution to the challenge of cyberterrorism.  It is important to understand the values offered by individuals to prevent cyberterrorism in the context of cybersecurity.  This empirical study elicits these public values and develop objectives that provide alternatives for decision making process in preventing cyberterrorism.  Knowing which alternative to use depends on expertise of the field.  Therefore, field experts ranked and weighted alternatives.  In addition, this paper offers scenarios for the implementation of these objectives to prevent cyberterrorism at individual, organizational, and governmental levels.

This study incorporates value focused thinking and public value forum offering an innovative approach to discover strategic measures and alternatives for complex policy decisions for preventing cyberterrorism.  The study develops Effective policies are based on understanding "how people think about and respond to risk" (Slovic, 1987).  Per their March 2018 report, Symantec found that in 2017 ninety percent of the ten percent increment of targeted cyber-attacks motivated by intelligence gathering and the other ten percent were a form of disruptive activity (Internet Security Threat Report, 2018). Moreover, the report say that internet of things attacks is up by 600% in 2017.  Therefore, it is important to employee the combination of the two methodologies for prevention cyberterrorism.  The combination offers grounded socio-organizationally qualitative and quantitative methodology to develop measures and alternatives for complex policy decisions for preventing cyberterrorism.

In conclusion, this paper offers a new combination of methodologies for preventing cyberterrorism. It offers an overview of cyberterrorism and some of the techniques that terrorists are now using to carry out their missions. The dissertation explains several counter measurements that a few governments are following to prevent cyberterrorism. This paper presents empirical study of participants. Data analysis shows the need to improve security policies. In addition, participants understand that preventing cyberterrorism needs privacy and secrecy of information. Hence, they prefer governmental and organizational control over international.

Additional contribution of this study is enhancing public value forum and proposes solution for the case of groups offering different ranks. Per literature review, no other study proposes a way to solve the challenge of having groups offer different ranks for the public value forum especially for cyberterrorism prevention. The proposal is using the rank of the group that influences and controls the values the most.

Per facts this study presents, policy makers, government officials, organizations administrators, and security researchers should incorporate socio-technical aspects that help preventing cyberterrorism, e.g., defending infrastructures' cyberspace, making legislation of laws to criminalize cybercrime, and attack terrorists' websites in cyberspace. Thereby using the study's innovative approach to discover strategic measures and alternatives for complex policy decisions for preventing cyberterrorism and incorporating value focused thinking and public value forum.

### 6.1. Contributions and Innovations

The study offers an innovative approach to elucidate strategic measures and alternatives for complex policy decisions for preventing cyberterrorism that concludes incorporating value focused thinking (VFT) and public value forum (PVF). The approach and its finding have several contributions from several prospectives. This section discovers theoretical, methodological, and practical contributions of this study. VFT and PVF systematically bares the model of values. The model of values offers relevant decision values and their classification.

#### 6.1.1. Theoretical Contributions

Cyber users are using Cyber-attacks to cause harm and influence governments, organizations, and individuals, and it is growing at an alarming rate. However, many studies focus on developing new encryption algorithms and new security apps which is important, but they are not the only aspect needed to support security. These studies do not take into consideration the socio-technical structure and influence that decides the implementation of security measures like security software. Military commanders used cyber-attacks as the first wave of attack in several recent wars. A special cyber-attack is the one used by terrorist organizations and groups to achieve and help their goals.

Using value-focused thinking (VFT) focuses on individuals' values and preferences. Therefore, VFT detects decision opportunities and forms decision alternatives (Ralph L. Keeney, 2009c). The study's innovative approach incorporates VFT and PVF. It discovers strategic measures and alternatives for complex policy decisions for preventing cyberterrorism. These measures and alternatives are per the values and preferences of individuals addressing the aims of complex policy decisions for preventing cyberterrorism.

The results show that knowing the objective and scenario with the highest weight and rank helps decision making in prioritizing the alternatives. In addition, knowing the order of objectives, attributes, and scenarios helps decision maker in evaluating her decision alternative. Moreover, it helps decision maker in evaluating the current situation by knowing the weight of her current situation. For example, if an organization wants to satisfy objective **Ensure governance of technical infrastructure**. If it implements governmental scenario, it ranks 2nd to employing the best scenario. The organization want to invest in improving its scenario for that objective since it weighs high among objectives. On the other hand, if an organization employ Global scenario for objective **Define a media response for cyberterrorist actions**, it may consider not improving the scenario it uses since it is a low weigh objective. Therefore, the decision model this study presents maximizes value in the following ways:

1) Improve: Prioritizing between decision alternatives by using the gap of values between decision alternatives as a guideline;

2) Resources management: Choosing which to improve based on available resources;

3) Understand the value of current implementation: Evaluating the current situation of an organization based on the rank and weight of current situation.

Table 6.1.1.1. Prioritizing of Objectives and Scenarios Without Attributes Consideration

| Influencer | Objectives Order | | Second Scenario | Third Scenario | Fourth Scenario | |
|---|---|---|---|---|---|---|
| Expert Participants | Ensure critical infrastructure protection mechanisms are in place | Best Scenario | Organizational | Governmental | Global | Worst Scenario |
| | Ensure governance of technical infrastructure | | Organizational | Governmental | Global | |
| | Engage in counter cyberterrorism activities | | Governmental | Organizational | Global | |
| Non-Expert Participants | Develop competencies for dealing with cyber terrorism activities | | Governmental | Organizational | Global | |
| | Define a media response for cyberterrorist actions | | Organizational | Governmental | Global | |

At a scenario level, expert participants prefer Scenario B: Organizational, Scenario A: Governmental, and Scenario C: Global respectively. They think that decentralization adds flexibility and reduces overhead. In addition, it allows organizations to take decisions faster.

Table 6.1.1.2. Prioritizing of Objectives and Scenarios with Attributes Value

| Influencer | Objectives Order | Best Scenario | Second Scenario | Third Scenario | Fourth Scenario | Worst Scenario |
|---|---|---|---|---|---|---|
| Expert Participants | Ensure critical infrastructure protection mechanisms are in place | Best | Organizational | Governmental | Global | Worst |
| | Ensure governance of technical infrastructure | Best | Organizational | Governmental | Global | Worst |
| | Engage in counter cyberterrorism activities | Best | Governmental | Organizational | Global | Worst |
| Non-Expert Participants | Develop competencies for dealing with cyber terrorism activities | Best | Governmental | Global | Worst | Organizational |
| | Define a media response for cyberterrorist actions | Best | Governmental | Global | Organizational | Worst |

Per facts this study presents, Cyberterrorism is now a real and pressing problem. Hence, terrorists are using everything they can to complete their missions, including the web. The web gives the terrorist the ability to hide identity and real location as well as attack and harm from a distance, to communicate among other terrorists and in a cheap way.

When the need to solve a decision problem arises, decision-makers need to elucidate decision opportunities that help in reaching the decision. Value-focused thinking (VFT) forms decision alternatives per individual values and preferences. Thus, the decision alternatives address goals and aims of decision making. Other decision-making approaches list decision alternatives before understanding the values and preferences that base the goal of decision making.

Incorporating value-focused thinking (VFT) and public value forum (PVF) for solving the complex policy decisions for preventing cyberterrorism in this study discovers strategic measures and alternatives.  It offers theoretical contribution that offers the decision model for preventing cyberterrorism.  The model is per individuals' values and preferences that address the goals of the policy for preventing cyberterrorism.  Per (Ralph L. Keeney, 2009c), VFT combines hard, e.g., number of cyberterrorism activities to watch, and soft, e.g., the quality of watching cyberterrorism activities, data for decision-making.  VFT values guides the decision making process to get better decision for preventing cyberterrorism.

### 6.1.2.  Methodological Contributions

This study combines the methodologies of value-focused thinking (VFT) and public value forum (PVF) (see figure 6.2.1).  Keeney (1990 and 2009) proposed the methodologies of VFT and PVF.  He proposed them as independent methodologies. This study increases the trustworthiness of their results by combining them to create one methodology.

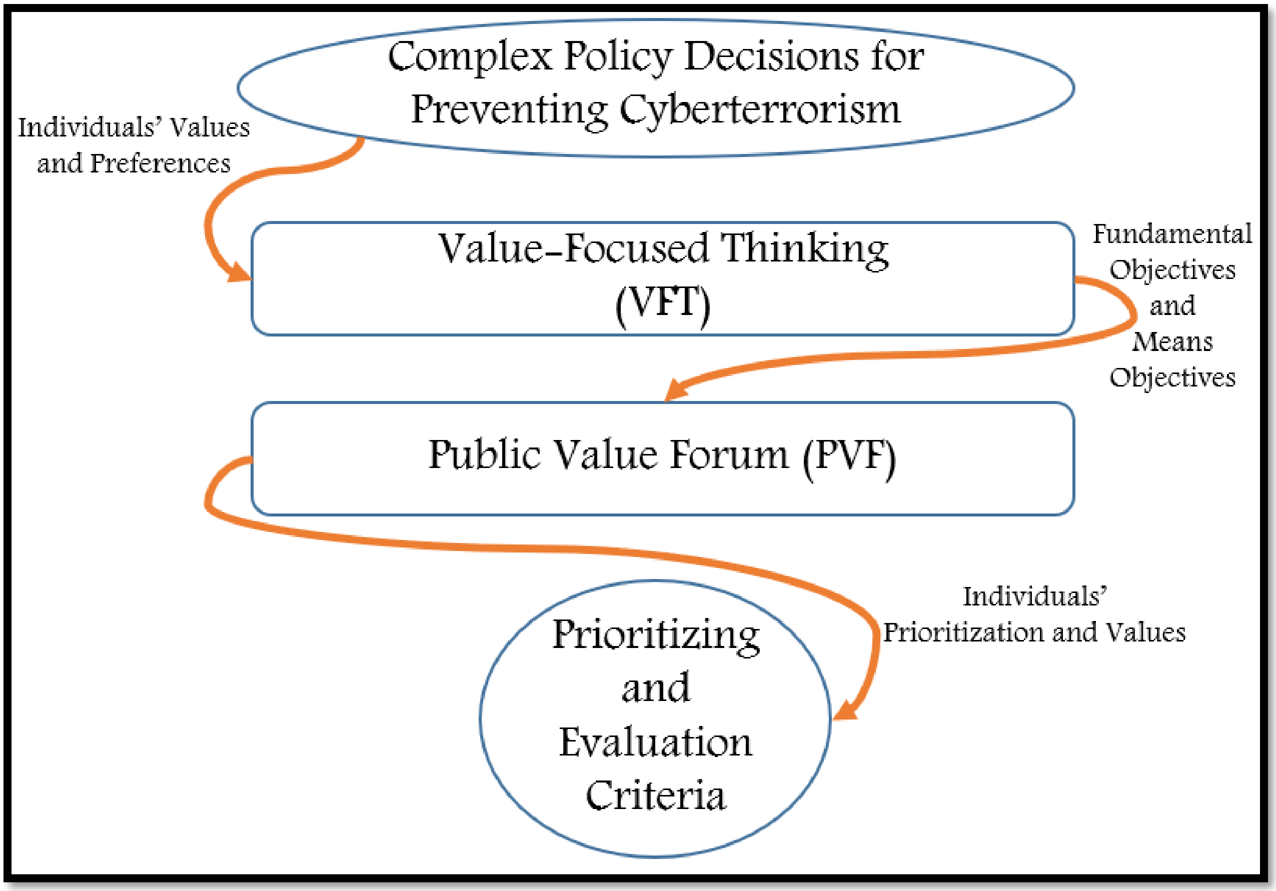
Complex Policy Decisions for Preventing Cyberterrorism
Individuals' Values and Preferences
Value-Focused Thinking (VFT)
Fundamental Objectives and Means Objectives
Public Value Forum (PVF)
Individuals' Prioritization and Values
Prioritizing and Evaluation Criteria

Figure 6.1.2.1. The combination of the Methodology of Value-Focused Thinking (VFT) and the Methodology of Public Value Forum

Keeney (1992) suggested that public value forum (PVF) methodology gets its values from experts or researchers. However, it may cause validity of the process to get the values questionable. This study uses the fundamental objectives from value-focused thinking (VFT) to supply the PVF with its values. It adds dependability to the values VFT enters in PVF. The innovative approach that incorporates VFT and PVF discovers strategic measures and alternatives for complex policy decisions.

### 6.1.3. Practical Contributions

The study offers the process to elucidate strategic measures and alternatives for complex policy decisions for preventing cyberterrorism that concludes incorporating value focused thinking (VFT) and public value forum (PVF). Practitioners can use the approach that study offers to elucidate strategic measures and alternatives for complex policy decisions for any policy problem.

Keeney published studies of policies that practitioners needed and value focused thinking (VFT) or public value forum (PVF) were able to develop the policy. Table 6.1.3.1 concludes several of them.

Table 6.1.3.1. Shows Practical Examples of Using Value-Focused Thinking (VFT) and Public Value Forum (PVF); (Ralph L. Keeney, 2009b, 2009d)

| Case | Methodology |
|---|---|
| Choosing future space missions that the U.S. civilian space program should pursue | PVF |
| Evaluating the transportation of nuclear waste | VFT |
| Planning actions for nations to do towards global warming | PVF |
| Deciding on how to manage the air pollution in Los Angeles | PVF |
| Deciding on a product design | PVF |
| Choosing how to make book revisions | VFT |
| The British Columbia Hydro and Power Authority (B.C. Hydro) planning | PVF |

Per table 6.1.3.1, value focused thinking (VFT) or public value forum (PVF) can help in policy decision-making. Nonetheless, the study incorporates VFT and PVF to increase the trustworthiness of its strategic measures and alternatives for complex policy decisions.

## 6.2. Limitations

This study uses qualitative and quantitative methods aiming to reduce the limitations that they may have when researchers apply them individually. Per on evidential decision-making theory, there is a probability that using decision process to choose a decision alternative does not lead to get the consequence theory predicted (Ahmed, 2005; Peterson, 1992c). Hence, if decision process predicts that conducting action O leads to consequence 0, conducting action O may lead to consequence 0, consequence 0 and other consequences, consequences other than consequence 0, or no clear consequences. Another limitation is that the cyberterrorism concepts discussed before beginning the interviews might influenced the answer of participants. Few subjects might answer in a way to impress the researcher or to help her (Mark L. Mitchell, 2009). This can question the validity of their answers. However, it can be overcome by having a decent sample-size (Mitchell & Jolley, 2009). The interviewee wanted to ensure that subjects knew the topic they are interviewed about. The validity of answers is less threatened by the influence of the answers of a few subjects.

Additionally, qualitative research interpretations can be subjective. Interpretive science is the science that studies phenomena by using procedures associated with techniques such as "ethnography, hermeneutics, phenomenology, and case studies" (Lee, 1991)(p. 342). The interpretive science deals with knowledge as a subjective truth. For many interpretivists, there can be many acceptable interpretations for a phenomenon. In interpretive science, different readers can have different interpretations of the same text (Lee, 1991)(p. 348). Interpretivists use their background to interpret phenomena (Van Maanen, 1979)(p. 548). There can be several interpretations based on the Interpretivist's background and reflection. Nonetheless, Value-focused thinking (VFT) and public value forum (PVF) systematically create the model of values that bares the classification of relevant decision values and decision model. Per (Ralph L. Keeney), the systematic development of a model of values is objective and scientific.

### 6.3. Future Work:

Per on facts this study presents, cyberterrorism is a pressing threat that is concerning all humanity. It is an oversimplification to think that cyberterrorism harm is limited to the people it directly affects.

*"The first day or so we all pointed to our country. The third or fourth day we were pointing to our continent. By the fifth day, we were aware of only one Earth," Sultan bin Salman Al Saud.*

The having of knowledge and using it give one competitive advantage over others. Hubbard and Seiersen (2016) said that it is critical to ensure cybersecurity, thus, reducing the uncertainty related to cybersecurity can be extremely valuable and cybersecurity experts can use small sample size to make informative inferences. It is important to have the culture of unity when handling safety concerns. There are several research directions that may emerge from facts this study presented and may produce several papers. The future publications use the study’s innovative approach to discover strategic measures and alternatives for complex policy decisions for preventing cyberterrorism and incorporating value focused thinking and public value forum.  There are namely seven publications that the main researcher and committee members may work on after the approval of the dissertation.

1) The next step for this study is to incorporate the means objectives in decision making.  Public value forum will include attributes from fundamental objectives and means objectives.  This study is at policy level and offering multi-attribute utility model will offer cyberterrorism prevention at organizational and governmental levels;

2) Explain the interaction between the identified list of means objectives and fundamental objectives;

3) Compare identified list of means objectives and fundamental objectives with other suggested measures used for cyberterrorism prevention;

4) Per (Dhillon, Oliveira, Susarapu, & Caldeira, 2016), managers and academics struggle with having the right balance between requirements of information security and usability.  It is hard to prevent unauthorized access which is to make access difficult for unauthorized users while making access convenient for

authorized users since it is hard to distinguish between users. Therefore, Dhillon, Oliveira, Susarapu, & Caldeira proposed two instruments to assess the balance between information security and usability. Their two instruments were built by using value-focused thinking approach and interviews with 35 experts. This study uses the two instruments to evaluate the balance between information security and usability of proposed objectives to prevent cyberterrorism;

5) Develop a public policy for preventing cyberterrorism for each category of cyberterrorism;

6) Investigate the level of cyberterrorism prevention related to the implementation of the identified list of means objectives and fundamental objectives;

7) Develop a computer game that adopts the policy created and the case study for training. The game will simulate the hacking case of an American research university.

## References:

Abed, J., & Weistroffer, H. R. (2016, March 18th–19th, 2016 ). Understanding Deterrence Theory in Security Compliance Behavior: A Quantitative Meta-Analysis Approach. Paper presented at the Proceedings of the Southern Association for Information Systems Conference, St. Augustine, FL, USA.

Adam, A., & Ofori-Amanfo, J. (2000). Does gender matter in computer ethics? Ethics and Information Technology, 2(1), 37-47.

Mishra, S., & Dhillon, G. (2007). A Theoretical Basis for Defining Internal Control Objectives for Information Systems Security. AMCIS 2007 Proceedings, 347.

Najjar, F. M. (1964). Al-Fārābī's The Political Regime: Al-Siyāsa al-Madaniyya Also Known as The Treatise on the Principles of Beings.

Aiken, P. (2010). Practical Considerations for Rapidly Improving Quality in Large Data Collections, 1-11. Retrieved from

Anderson, R. E., Black, W. C., Babin, B. J., & Hair, J. F. (2009). Multivariate Data Analysis (7th Edition - Kindle Edition ed.). Upper Saddle River, NJ 07458, USA: Prentice Hall.

Anderson, R. E., Black, W. C., Babin, B. J., & Hair, J. F. (2010). Conjoint Analysis. In J. Heine (Ed.), Multivariate Data Analysis (Seventh Edition (February 23, 2009) ed., pp. 408 - 480): Prentice Hall.

Armstrong, H. L., & Forde, P. J. (2003). Internet anonymity practices in computer crime. Information management & computer security, 11(5), 209-215.

Bainbridge. (1997). Cannot employees also be hackers? Computer Law and Security Report, 13(5), 352–354.

Barrett. (2003). Penetration testing and social engineering – hacking the weakest link. Information Security Technical Report., 8(4), 56–64.

Benioff, M. R., & Lazowska, E. D. (2005). Cyber Security: A Crisis of Prioritization. Retrieved from

Boell, S. K. (2017). Information: Fundamental positions and their implications for information systems research, education and practice. Information and Organization, 27(1), 1-16.

Borchgrave, Cilluffo, Cardash, & Ledgerwood. (2001). Cyber Threats and Information Security: Meeting the 21st Century Challenge. Center for Strategic and International Studies (CSIS), Washington, DC, May 2001.

Bowman. (2007). Saudi urges action on escalating cyber-terrorism. Arabian Business(December 5, 2007).

Bronson, R. (2008). Thicker than oil: America's uneasy partnership with Saudi Arabia (1 edition (June 25, 2008) ed.): Oxford University Press.

Catton Jr, W. R. (1959). A Theory of Value. American Sociological Review, 24(3), 310-317.

Conley-Ware, L. D. (2010). Medical Differential Diagnosis (MDD) as the Architectural Framework for a Knowledge Model: A Vulnerability Detection and Threat Identification Methodology for Cyber-Crime and Cyber-Terrorism. ERIC, Coss, D. L. (2013). Cloud privacy audit framework: A value-based design. (Doctor of Philosophy in Business at Virginia Commonwealth University), Virginia Commonwealth University, VCU Scholars Compass. Retrieved from http://scholarscompass.vcu.edu/etd/3106 Available from Graduate School at VCU Scholars Compass (3106)

Civantos, C. (2017). The Afterlife of Al-Andalus: Muslim Iberia in Contemporary Arab and Hispanic Narratives: SUNY Press.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In Networks and netwars: The future of terror, crime, and militancy (pp. 239-288): National Defense Research Institute (RAND).

Dhillon, G. (2015). Enterprise Cyber Security (2nd edition ed.): CreateSpace Independent Publishing Platform.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153.

Dhillon, G., Challa, C., & Smith, K. (2016). Defining Objectives for Preventing Cyberstalking. Paper presented at the IFIP International Information Security and Privacy Conference.

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. Computers in Human Behavior, 61, 656-666.

Dhillon, G., Syed, R., & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. Information & Management, 54(4), 452-464.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314.

Embar-Seddon, A. (2002). Cyberterrorism Are We Under Siege? American Behavioral Scientist, 45(6), 1033-1043.

Ferguson, N., Schneier, B., & Kohno, T. (2011). Cryptography engineering: design principles and practical applications (1st ed.). Indianapolis, Indiana: Wiley Publishing, Inc.

Filiol, & Richard. (2006). Cyber-criminalite. Paris: Dunod.

Fishburn, P. C. (1970). Utility theory for decision making: Research Analysis Corp Mclean va.

Forrest, Somayaji, & Ackley. (1997). Building diverse computer systems. Paper presented at the Proceedings of the Sixth Workshop on Hot Topics in Operating Systems, Los Alamitos, CA.

Fovinoa, Guidib, Maseraa, & Stefaninia. (2011). Cyber Security Assessment of a Power Plant. Electric Power Systems Research, 81, 518–526.

Fuentes, K. M. (2016). Cyberterrorism: The Use of Social Networking to Recruit Westerners an Informational Guide for Law Enforcement Agencies. (Master of Science in Cybersecurity Capstone), Utica College

Furnell, Chiliarchaki, & Dowland. (2001). Security analyzers: Administrator assistants or hacker helpers? Information management & computer security, 9(2), 93–101.

Gilsinan, K., & Calamur, K. (2017, January 6, 2017). Did Putin Direct Russian Hacking? And Other Big Questions
Did Moscow influence the U.S. election? Who else has been hacked? Could the CIA be wrong? The Atlantic. Retrieved from https://www.theatlantic.com/international/archive/2017/01/russian-hacking-trump/510689/

Gordon, S., & Ford, R. (2002). Cyberterrorism? computers & security, 21(7), 636-647.

Gorman, & Barnes. (2011). Cyber Combat: Act of War, Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force. The Wall Street Journal(MAY 31, 2011).

Graham. (1998). Cyberwar: a New Weapon Awaits a Set of Rules; Military, Spy Agencies Struggle to Define Computers' Place in U.S. Arsenal. The Washington Post(Jul 8, 1998), A.01

Gregory, R., & Keeney, R. L. (2017). A Practical Approach to Address Uncertainty in Stakeholder Deliberations. Risk Analysis, 37(3), 487-501. doi:10.1111/risa.12638

Habboush, M., Ackerman, G., & Riley, M. (2016, December 12, 2016 3:27 AM EST ). Hack of Saudi Arabia Exposes Middle East Cybersecurity Flaws, Opinion Article. Bloomberg News. Retrieved from https://www.bloomberg.com/news/articles/2016-12-12/hack-of-saudi-arabia-exposes-middle-east-cyber-security-flaws

Hansen, Lowry, Meservy, & McDonald. (2007). Genetic Programming for Prevention of Cyberterrorism Through Dynamic and Evolving Intrusion Detection. Decision Support Systems, 43 1362-1374.

Hardy, K., & Williams, G. (2014). What is ‘cyberterrorism’? Computer and internet technology in legal definitions of terrorism. In Cyberterrorism: Understanding, Assessment, and Response (pp. 1-23): Springer.

House, W. (2009). The Monroe Doctrine in Cyberspace. (March 10, 2009).

Hubbard, D. W., & Seiersen, R. (2016). How to Measure Anything in Cybersecurity Risk (First Edition ed.): John Wiley & Sons.

Internet Security Threat Report. (2018). Retrieved from

Jarvis, L., & Macdonald, S. (2015). What is cyberterrorism? Findings from a survey of researchers. Terrorism and Political Violence, 27(4), 657-678.

Jarvis, L., Nouri, L., & Whiting, A. (2014). Understanding, locating and constructing cyberterrorism. In Cyberterrorism (pp. 25-41): Springer.

Jenkins. (2004). World Becomes the Hostage of Media-Savvy Terrorists: Commentary. USA Today(August 22, 2004).

Jones, B. H., Chin, A. G., & Aiken, P. (2014). Risky business: Students and smartphones. TechTrends, 58(6), 73-83.

Keeney, R. L. (1992a). 2. The Framework of Value-Focused Thinking. In Value-Focused Thinking: A Path to Creative Decisionmaking (pp. 53-154). Cambridge, Massachusetts, UNITED STATES: Harvard University Press.

Keeney, R. L. (1992b). Selected Applications. In Value-Focused Thinking: A Path to Creative Decisionmaking (2009-07-31 Edition ed., pp. 289-341). Cambridge, Massachusetts, UNITED STATES: Harvard University Press.

Keeney, R. L. (1992c). The Framework of Value-Focused Thinking. In Value-Focused Thinking: A Path to Creative Decisionmaking (pp. 53-154). Cambridge, Massachusetts, UNITED STATES: Harvard University Press.

Keeney, R. L. (1992d). Value-Focused Thinking at British Columbia Hydro. In Value-Focused Thinking: A Path to Creative Decisionmaking (2009-07-31 Edition ed., pp. 342-371). Cambridge, Massachusetts, UNITED STATES: Harvard University Press.

Keeney, R. L. (1996). Value-focused thinking: Identifying decision opportunities and creating alternatives. European Journal of operational research, 92(3), 537-549.

Keeney, R. L. (1999). The value of Internet commerce to the customer. Management science, 45(4), 533-542.

Keeney, R. L. (2009). 6. Uncovering Hidden Objectives. In Value-Focused Thinking (2009-07-31 Edition ed., pp. 157-197). Cambridge, UNITED STATES: Harvard University Press.

Keeney, R. L. (2009). Value-Focused Thinking: A Path to Creative Decisionmaking: Harvard University Press.

Keeney, R. L. (2013). Identifying, prioritizing, and using multiple objectives. EURO Journal on Decision Processes, 1(1-2), 45-67.

Keeney, R. L., Von Winterfeldt, D., & Eppel, T. (1990). Eliciting public values for complex policy decisions. Management science, 36(9), 1011-1030.

Kerstetter, J. (2016, DEC. 2, 2016). Daily Report: Malware Damages Aviation Systems in Saudi Arabia. The New York Times.

Knickmeyer. (2008). Al-Qaida Web Forums Abruptly Taken Offline, Separately, Sunnis and Shittes Wage Online War. The Washington Post.

Kovacich. (1999). Hackers: Freedom fighters of the 21st century. 18(7), 573–576.

Kramer, R. (2002). Internet use by terrorists and content analysis of terrorist Websites. (MA in Electronic Communication and Publishing Master's thesis), University College, London, (UMI Number: 1421948)

Lee, A. S. (1989). A scientific methodology for MIS case studies. MIS quarterly, 33-50.

Lee, A. S. (1991). Integrating positivist and interpretive approaches to organizational research. Organization science, 2(4), 342-365.

Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. Information Systems Research, 14(3), 221-243.

Lipton, E., Sanger, D., & Shane, S. (2016, December 14, 2016). The Perfect Weapon: How Russian Cyberpower Invaded the U.S. The New York Times, p. A1. Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=1

Mark L. Mitchell, J. M. J. (2009). Internal Validity. In Research Design Explained (7 ed., pp. 304-333): Wadsworth Publishing.

MCrosbie, & Spafford. (1995). Applying genetic programming to intrusion detection. Paper presented at the Proceedings of the Working Notes for the AAAI Symposium on Genetic Programming, Cambridge, MA, Cambridge, MA.

Mitchell, M. L., & Jolley, J. M. (2009). Research Design Explained (7th ed.): Wadsworth Publishing.

Mohay, Andeson, Collie, Vel, d., & McKemmish. (2003). Computer and Intrusion Forensics. Artech House, Boston, MA.

Mishra, S., & Dhillon, G. (2007). A Theoretical Basis for Defining Internal Control Objectives for Information Systems Security. AMCIS 2007 Proceedings, 347.

Najjar, F. M. (1964). Al-Fārābī's The Political Regime: Al-Siyāsa al-Madaniyya Also Known as The Treatise on the Principles of Beings.

Obama, B. (2016). Protecting U.S. Innovation From Cyberthreats. Opinio|Commentary. U.S. Edition. Retrieved from http://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003

Papadimiyriou. (2009). A nexus of Cyber-Geography and Cyber-Psychology: Topos/"Notopia" and identity in hacking. Computers in Human Behavior, 25, 1331-1334.

Pham, V., & Cid, C. (2012, 2012//). Are We Compromised? Modelling Security Assessment Games. Paper presented at the Decision and Game Theory for Security, Berlin, Heidelberg.

Protection, C. I. (2004). Challenges and Efforts to Secure Control Systems. United States Government Accountability Office, GAO-04-628T.

Qina, Zhoub, Reidc, Laid, & Chenc. (2007). Analyzing terror campaigns on the internet: Technical sophistication, content richness, and Web interactivity. Int. J. Human-Computer Studies, 65, 71–84.

Reuters. (2012, December 10, 2012). Aramco Says Cyberattack Was Aimed at Production. The New York Times. Retrieved from http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html

Reuters. (2016). Obama Budget Proposal Includes $19 Billion for Cybersecurity. TECH, Changing Face of Security. Retrieved from http://fortune.com/2016/02/09/obama-budget-cybersecurity/

Sanger, D., & Shane, S. (2016, December 10, 2016). Russian Hackers Acted to Aid Trump in Election, U.S. Says. The New York Times, p. A1. Retrieved from https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html

Siebert, J., & Keeney, R. L. (2015). Creating More and Better Alternatives for Decisions Using Objectives. Operations Research, 63(5), 1144-1158.

Slovic, P. (1987). Perception of Risk. Science, 236(4799), 280-285.

Smith, K., & Dhillon, G. (2016, 2016). Eliciting Societal Values About Cyberstalking Policy Decisions. Paper presented at the Thirty Seventh International Conference on Information Systems, Dublin, Ireland.

Stallings. (2003). Cryptography and Network Security (3rd ed.): Prentice Hall.

Terrorism: Questions and Answers. (2004). Cyberterrorism, 2004.

Van Hoogenstyn, A. J. (2007). Knowledge and Perception of "Cyberterrorism". (Master of Arts in Justice Studies Master of Art Thesis), University of New Hampshire, (UMI Number: 1449587)

Van Maanen, J. (1979). The fact of fiction in organizational ethnography. Administrative science quarterly, 24(4), 539-550.

Wark. (2004). A hacker manifesto. Cambridge, Mass: Harvard College.

Webster, Borchgrave, Gallagher, Cilluffo, Berkowitz, & Lanz. (1998). Cybercrime…Cyberterrorism…Cyberwarfare...: Averting an Electronic Waterloo. Center for Strategic and International Studies (CSIS), Washington, DC(November 1998).

Weimann. (2004). www.terror.net: How Modern Terrorism Use the Internet. Special Report, US Institute of Peace.

Weimann, G. (2005). Cyberterrorism: The sum of all fears? Studies in Conflict & Terrorism, 28(2), 129-149. doi:10.1080/10576100590905110

Williams, C. (2017, January 27, 2017). Hackers hit D.C. police closed-circuit camera network, city officials disclose. The Washington Post.

Writer. (2006). Saudi passes cybercrime laws. Arabian Business(13 October 2006).

Wynn, & Katz. (1997). Hyperbole over cyberspace: Self-presentation and social boundaries in internet home pages and discourse. The Information Society, 13(4), 297–327.

Yar. (2005). Computer hacking: Just another case of juvenile delinquency? Howard Journal of Criminal Justice, 44(4), 387–399.

Youtie, J., & Shapira, P. J. (2017). Exploring public values implications of the I-Corps program. The Journal of Technology Transfer, 42(6), pp 1362–1376. doi:https://doi.org/10.1007/s10961-016-9518-z

## Appendix 1: List of objectives and values for preventing cyberterrorism

1 Define regulatory measure for cyberterrorism prevention

Ensure the existence of cybercrime laws

Preserve citizens’ rights to use the internet through regulations

Avoid regulations that invade citizens' privacy

Assure criminalization of cyberterrorism acts

Punish cyberterrorists as criminals that threat the national security

2 Ensure governance of technical infrastructure

Allocate clear roles and responsibilities for cyberterrorism governance

Assure constant monitoring of threats

Ensure there is learning from past events

3 Increase spending to prevent cyberterrorism

Allocate federal funds for cyberterrorism detection and prevention

Strategize measures for cyberterrorism detection and prevention

Encourage research on digital defense

4 Define governance structures for cyberterrorism prevention

Implement governance structure specialized in counter cyberterrorism

Define roles for information accessibility

Share accountability among individuals

5 Engage in counter cyberterrorism activities

Engage in intelligence gathering for cyberterrorism detection and prevention

Counter cyberterrorists attacks proactively

6 Increase use of hacker and cracker ability

Recruit ethical cyberterrorist for preventive purposes

Find geolocation of the cyberterrorist groups

7 Ensure critical infrastructure protection mechanisms are in place

Develop contingency plans for governmental data loss

Treat backup locations as a national security issue

Prevent spam

Increase use of Supervisory Control and Data Acquisition (SCADA) systems

8 Increase surveillance of suspect groups

Define mechanisms to find cyberterrorism activity

Increase surveillance of concerned individuals

Track individuals suspected of illegal activity

Perfect privacy requirements of citizens

Encourage citizens to self-check their activities

9 Increase investigation of cyberterrorist funding sources

Find the source of income for cyberterrorists

Cut off the source of cyberterrorism income

10 Increase cross agency coordination

Engage public and private sectors to prepare for cyberterrorism prevention

Engage the global community (like the UN) to prevent cyberterrorism

11 Increase awareness of cyberterrorist actions

Emphasize the seriousness of cyberterrorism to the global community

Increase cyberterrorism prevention education

Develop training for cyberterrorism detection and prevention

Increase awareness of consequences of cyberterrorist attacks

12 Increase resilience capability following cyberterrorist attacks

Empower organizations recovering from cyber attack

Encourage organizations to recover without governmental support

13 Define a media response for cyberterrorist actions

Increase media coverage to match the danger of cyberterrorism

Develop a media response strategy for cyberterrorism

14 Develop competencies for dealing with cyberterrorism activities

Ensure technical staff have up to date knowledge

Engage in strategically thinking about cyberterrorism protection

Define mechanisms to get security feedback from individuals

Train individuals on modern technologies

15 Ensure existence of technical security measures

Increase use of strong encryption

Define firewalls to watch traffic

Implement sophisticated intrusion detection system

16 Encourage behavioral controls

Ensure confidential data is made available on a need to know basis

Encourage use of good password use habits

Increase individual accountability in cyberterrorism prevention

Make cyberterrorism training mandatory

Prevent citizens from sharing their personal information over social media

17 Ensure adequacy of cyber security policy

Ensure currency of cyber security policies

Increase alignment of cyber security policies with security standards

Ensure cyber security policy links to organizational practices

18 Encourage citizen involvement for cyberterrorism prevention

Encourage citizens to be involved in fighting cyberterrorism

Empower citizens with respect to cyberterrorism prevention

Encourage citizens to practice good cyber hygiene

Encourage citizen to report suspicious cyber activity

## Appendix 2: Expert Participants

The study uses eight information security experts:

1) Chief Information Security Officer at an American Public Research University;

2) Systems Security Architect at Public Research University;

3) Navy Engineer at United States Navy and Ph.D. Candidate of Systems Engineering at George Washington University;

4) Data Analyst at a contractor with National Security Agency (NSA);

5) Political Scientist that graduated from Virginia Commonwealth University with Bachelor of Arts in Political Science;

6) Information security administrative assistant at a small retail business;

7) Retired (April 2017) vice president of multinational corporation provides solutions for risk management, health insurance, and outsourcing services;

8) Director of professional services at an organization that develops applications to designs security for information systems.

## Appendix 3: Non-Expert Participants

The study uses thirty non-expert participants:

1) Participant did not disclose her information;
2) Assistant Manager, Dominos Pizza, inc;
3) Finance Administrator, World Horizons USA;
4) Research Associate 2, Abbott Laboratories;
5) Ten students of Master of Science in information systems at Virginia;
6) Student at Bachelor of Science in Mechanical Engineering with a Nuclear Engineering Concentration at Public Research University at Virginia;
7) Math Teacher Middle School at Seattle;
8) Chick Fil A Employee;
9) Graduate Assistant at Public Research University at Virginia;
10) Accountant at Car Dealership;
11) Director of Richmond Campus Ministries;
12) Undergraduate Research Assistant at Public Research University at Maryland;
13) Nations Within staff, The Navigators;
14) Event Services supervisor, Bandimere Speedway;
15) Principal, Texas City Independent School District;
16) Special Education Teacher, North Side Independent School District San Antonio TX;
17) Financial Manager and Team Leader, Christian service organization;
18) Credit Specialist, University of Colorado Medicine;

19) Physician, Health care;

20) Estimator, Electrical Contractor;

21) Senior Trip Leader, Ministry Organization;

Civantos, C. (2017). *The Afterlife of Al-Andalus: Muslim Iberia in Contemporary Arab and Hispanic Narratives*: SUNY Press.

Keeney, R. L. FOUNDATIONS. In.

Keeney, R. L. (1996). Value-focused thinking: Identifying decision opportunities and creating alternatives. *European Journal of operational research, 92*(3), 537-549.

Keeney, R. L. (2009a). 2. The Framework of Value-Focused Thinking. In *Value-Focused Thinking: A Path to Creative Decisionmaking* (pp. 53-154). Cambridge, Massachusetts

London, England: Harvard University Press.

Keeney, R. L. (2009b). Selected Applications. In *Value-Focused Thinking: A Path to Creative Decisionmaking* (2009-07-31 Edition ed., pp. 289-341). Cambridge, UNITED STATES: Harvard University Press.

Keeney, R. L. (2009c). The Framework of Value-Focused Thinking. In *Value-Focused Thinking: A Path to Creative Decisionmaking* (pp. 53-154). Cambridge, Massachusetts

London, England: Harvard University Press.

Keeney, R. L. (2009d). Value-Focused Thinking at British Columbia Hydro. In *Value-Focused Thinking: A Path to Creative Decisionmaking* (2009-07-31 Edition ed., pp. 342-371). Cambridge, UNITED STATES: Harvard University Press.

Mishra, S., & Dhillon, G. (2007). A Theoretical Basis for Defining Internal Control Objectives for Information Systems Security. *AMCIS 2007 Proceedings*, 347.

Najjar, F. M. (1964). Al-Fārābī's The Political Regime: Al-Siyāsa al-Madaniyya Also Known as The Treatise on the Principles of Beings.

## Vita

Osama Bassam J. Rabie was born on 26/Rabi al-Thani/1406 (January 7, 1986), in Jeddah, Kingdom of Saudi Arabia (KSA), and is a Saudi citizen. He graduated from Al-Fisal High School, Jeddah, KSA in 2002. He received his Bachelor of Science in Computer Science from King Abdulaziz University (KAU), Jeddah, KSA in 2008 and worked as a web developer and taught at KAU. He received his Master of Science in Information Systems from University of Maryland, Baltimore County (UMBC) in 2012.

Important Elements to include in a Vita for accurate Cataloging:

Osama Bassam J. Rabie

January 7, 1986 in Jeddah, Kingdom of Saudi Arabia

Adjunct professor at Virginia Commonwealth University Summer 2017 and Spring 2018