RISK ASSESSMENT AND DECISION MAKING OF SECURITY IN CONTAINER PORT FACILITIES

WAN MUHD ZULHILMI BIN ABDUL HALIM

(W. M. Z. Abdul Halim)

A Thesis Submitted to Liverpool John Moores University

For the Degree of Doctor of Philosophy

February 2020

Abstract

Ports are exposed to various risks, both in their internal operation as well as external business interactions with other maritime logistics companies. While traditional safety and security policies are able to deal with accidents, theft, and hazard-based risks in ports, a new risk assessment is urgently required to tackle those that are caused by threats, such as terrorist attacks. Terrorist attacks have always been classified as disruption risk because they pose a bigger risk of causing enormous damage, unlike that of a natural disaster. In contrast to natural disasters, terrorist attacks do not have a similar pattern among them and usually, terrorists will attack a port at its weakest point or where it can cause the highest impact values. Therefore, it is important for port stakeholders to identify and pinpoint which of the port facilities have the highest impact value as any terrorist attacks. This study starts with the classification types of port facilities and their risk of terrorist attacks based on a comprehensive literature review, and through interviewing academic and industrial port security experts relating to a particular port. The identified risks of port facilities under terrorist attack scenarios are then analysed to consider the impact of the terrorist attacks on port facilities and the resilience of the current port security system. Various approaches have been combined and applied in this process, which offer the chance of the birth of some novel and effective risk modelling techniques and assessment tools, such as, using a combination of ETA and BN to calculate the consequence of the attack, create new security function as a main criteria in ER model and showing full step by step calculation using four criteria in ER. The study is about risk assessment of security countermeasures which is important and beneficial not only to academics but also to seaport stakeholders especially port operators. The work is also able to predict the percentage of damage if the risk occurs and allows the practitioners to make decisions on investing security countermeasures based on complex analysis. Although the risk assessment methods are presented on the basis of specific security countermeasures, it is believed that, with domain-specific knowledge and data, they can also be tailored for a wide range of applications to evaluate the safety of other logistics and transport domains, especially those where a high level of uncertainty is involved.

Acknowledgements

This thesis is the result of six years of work during which I have been accompanied and supported by many people and organisations. It is a pleasant aspect that I have now the opportunity to express my sincere gratitude to all of them.

The first person I would like to thank is my principal supervisor Professor Dr Zaili Yang. I thank Professor Yang for of his patience, encouragement, great direction and advice provided in completing this thesis. More importantly, his overt enthusiasm and integral view on research and his mission for providing 'only high-quality work and nothing less', have made a deep impression on me. I owe him lots of gratitude for having shown me this way of conducting research. He could not even realise how much I have learned from him and I am really glad that I have known Professor Yang in my life.

Besides that, not to forget my excellent tutor's Dr Trung Thanh Nguyen and Assc. Professor Dr Saiful Fitri who provided me great help in my study. I would like to express my gratitude to both of them who always monitored the progress of my work and were available when I needed their advice. My colleagues in the LOOM's group all gave me the feeling of being at home at work. They also substantially contributed to the development of this thesis. I thank them all.

This research has been supported and funded by University Malaysia Terengganu and I thank them for their confidence and assistance in me. I am also deeply grateful to the School of Engineering at LJMU for providing me an excellent working environment during the past six years.

I feel a deep sense of gratitude for my father and mother for their great material and spiritual support. I am very grateful for my wife, Nik Fatiha, for her love, trust and patience during the PhD period. Without their love, care and understanding I would not have delivered the thesis like this.

The chain of my gratitude would be definitely incomplete. Many persons have helped me and many good friends have shared experiences and thoughts with me throughout the past years. For all of them, if their names do not appear in the first course of the chain, I would like to express my heartfelt gratitude here.

Table of Contents

Abbreviation

Abbreviation	Descriptions of The Element State
ACD	: Access Control, Delay and Deterrence (ACD)
AHP	: Analytic Hierarchy Process
AS	: Administration Site
BN	: Bayesian Network
CB	: Container Bomb Attacks
CEA*	: Countermeasure Efficiency on the Terrorist Attack
CEE**	: Countermeasure Efficiency on the Explosion
CEO	: Chief of Executive Operation
DA	: Detection and Assessment (DA)
DMDNB	: Dimethyl and Dinitrobutane
DOD****	: Damage on Death
DOI***	: Damage on Injury
DTC	: Drill Training Cost (DTC)
ER	: Evidential Reasoning
ESS	: Experienced Staff Salary (ESS)
ETA	: Event tree Analysis
FLX	: Flexibility (FLX)
GB	: Gate and Barrier (GB)
H	: An Event Happening
HDA	: Hearing Detection and Assessment (HDA)
HES	: Hiring Experience Staff (HES)
HUV	: Hijacking Using Vessels
LL	: Landscaping and Layout (LL)
NH	:No Event Happening
NO (Damages)	: No Damages
NST	: Non-security Staff Training (NST)
ODA	: Other Detection and Assessment (ODA)
OIE	: Overcome the Identification of Employees
OIV	: Overcome the Identification of Visitors
OPUDA	: Overcome the Prevention of Unauthorised Document Access
OPUE	: Overcome the Prevention of Unauthorised Entry

OPUEArmy	: Armed Attackers Overcome the Prevention of Unauthorised Entry
OPUIIPF	: Overcome the Prevention of Unauthorised Introduction of Items in Port Facilities
ORI	: Overcome the Routine Security Inspections
PEC	: Procurement Equipment Cost (PEC)
PESC	: Personnel and Equipment Security Cost (PESC)
PG	: Port Gates
R1	: Expert Respondent 1
R2	: Expert Respondent 2
R3	: Expert Respondent 3
R4	: Expert Respondent 4
R5	: Expert Respondent 5
R6	: Expert Respondent 6
RCA	: Root Cause Analysis
RTT	: Response to the Threat (RTT)
SC	: Smuggling in of Unauthorised Containers (Bombs)
SCBT	: Suicide Collision by Trucks
SCBTV	: Suicide Collision by Trucks/Vessels
SCBV	: Suicide Collision by Vessels
SCM	: Successful Countermeasure
SCU	: Screening and Check-up (SCU)
SEMC	: Security Equipment Maintenance Cost (SEMC)
SL	: Security Level
SST	: Security Staff Training (SST)
USCM	: Unsuccessful Countermeasure
UTC	: Using Tampered Containers
UTT	: Using Tampered Truck(s)
VDA	: Visual Detection and Assessment (VDA)
WA	: Weapons Attack
WOS	: Wharf Operation Site
YES (Damages)	: There is Damage
YOS	: Yard Operation Site

List of Figures

List of Tables

Chapter 1: Introduction

Summary

This study describes the application of the decision-making tools that analyse security risks of container port facilities of being attacked by terrorists. The first part of this study covers research background, research objectives, research novelty, research scopes, research assumption and the structure of the study. The second part of this study present the literature review of the undertaken research. The third part of this study consists of the first technical chapter and this chapter highlights the development of a model to calculate the risk probability of terrorist attacks on container port facilities by using Bayesian Network (BN). The fourth part of this study includes the second technical chapter that describes the consequence or impact that may affect the port if there is an attack on the port facilities. The fifth part of this study ranks the available security countermeasure using Analytic Hierarchy Process (AHP) and Evidential Reasoning (ER) to enable the port management team to select the most effective countermeasure. The sixth part of this study states the recommendations, conclusion and future development of the research.

1.1 Background of the Research

The globalisation of trade and the containerisation replacing cargo process has given a significant advance to the world's economic development in last three decades. This genius invention, conducted by cramping every cargo into one uniform container and shipping it to the whole world, sets a new trend of fast and cheaper trade. It transforms the world economy, commercial and industrial activities especially in seaports. Nowadays, the numbers of ports entertaining cargo without containers are decreasing and seaports that only specialise in containers are increasing.

Globalisation also creates a lot of changes towards the transportation network, such as integrating the seaport and land transport which is the road and rail, making extended services such as door-to-door services. Such integration also attracts a lot of shipping companies to start relocating themselves near the seaport creating a one-stop-shop services chain. This progress is applauded, however, placing seaports as essential to a country's economic growth can render them vulnerable to many risks, specifically from terrorist attacks. The stakes of these risks are extremely high, as any attack on a seaport would cause enormous loss to the seaport operator and cripple the region or country economy.

Modern trade is at an international scale and complex, with planning and prediction in ensuring the cargo arrives at the right time, at the right place, in the right condition and at the right cost (Rushton *et al*., 2000). Any disruptions on that planned shipment will cost the port operator, the shipping lines and the end customer a significant loss. Therefore, shipping lines will choose seaports with a good track record of efficiency and high security countermeasures.

In this study, container terminals will be utilised as the test cases to identify which parts of seaports have a high impact compared to other places and in consequence high security criticality for disruption. By identifying which port places have a high risk of terrorist attacks, the governments will more effectively cooperate with port operators to invest in port logistics resilience plans. Port operators will also benefit from this study as they will be able to plan their emergency responses in advance. Consequently, the time taken for supply chain networks to recover will be significantly reduced with the development of cost-effective measures and emergency response.

1.2 Primary Objective and Subsidiary Objective of the Study:

The primary purpose of this study is to assess the risk of terrorist attacks on a seaport facility and its consequences, and then select the best security countermeasures to mitigate the attack risk and reduce damage inflicted on the port (provided the security countermeasures currently used are not effective). However, if the security countermeasures are sufficient to handle a physical terrorist attack, another study may be required to compare and propose a better security countermeasure which can benefit port operators in terms of security and financial aspects.

In order to achieve this aim, some subsidiary objectives need to be addressed. They are:

- To investigate the probability of terrorist attack and assess the security in sea port using Root Cause Analysis (RCA) and Bayesian Network (BN).
- To use test cases to validate the newly developed methodology and the supporting models/methods in the risk reduction in emergency response and preparation if a terrorist attack happens at a seaport.
- To identify which of the port facilities have the highest probability of an attack from terrorist.
- To analyse different types of possible terrorists, different types of attacks, security breaches and different type of port sites/facilities that may be targeted.
- To find the factors that have significant effects on the port facilities’ vulnerabilities.
- To suggest the corrective action(s) to prevent recurrence of each harmful event.
- To develop a model that is able to predict the terrorist’s first and second attacks and consider different possibilities of attacks (developing BN models to calculate the probability risk of terrorist attacks on port facilities).
- To identify the initiating event of a terrorist attack

- To test the level of damage caused by the terrorist attacks to the seaport using an Event Tree Analysis (ETA) combine with BN.
- To identify existing countermeasures and to group them into three big groups which counter fire, weapons and explosions.
- To identify the initiating event of terrorist attack and obtain event failure probabilities.
- To evaluate the outcome risk and recommend corrective action.
- To estimate the cost and benefits of port security by ranking up the security countermeasures listed by using the Analytic Hierarchy Process (AHP) approach and synthesising the outcome by using the Evidential Reasoning (ER) approach.

1.3 Justification of the Research and Research Novelty

The purpose of this study is to develop a new methodology to model and analyse security risk and to enhance security countermeasures toward combating terrorist attacks. The novelties of this study are 1) developing a generic model for security countermeasures risk assessment using RCA and BN, 2) providing a powerful risk based decision making tool for predicting which place has the highest risk of attack, 3) calculating the potential damage using ETA combine with BN and 4) addressing alternatives on security countermeasures for future improvement using AHP and ER.

For novelty 3, there has not been a study on terrorist attack on seaports using this event tree approach, because event tree cannot be used to predict the success and failure probabilities of such attacks. Therefore, BN approach is used to cover those weaknesses. In event tree, two important dimensions are used namely initiating event and the countermeasure. The initiating event for this study was the risk of terrorist attack to the wharf site and the countermeasures for the event were called security countermeasures or retaliation countermeasures.

In the end, this study ranks the security countermeasures listed by using an Analytic Hierarchy Process (AHP) approach and synthesising the outcome by using an Evidential Reasoning (ER) approach. This newly developed methodology and the supporting models/methods will contribute in developing effective emergency response and preparation in security countermeasures. This study is valuable to both academic and industrial communities such as port operators, manufacturer/shippers, government, and end buyers.

1.4 Structure of the Study

The structure of the research is laid out in Figure 1.1. There are six chapters and each individual chapter is described in brief as follows:

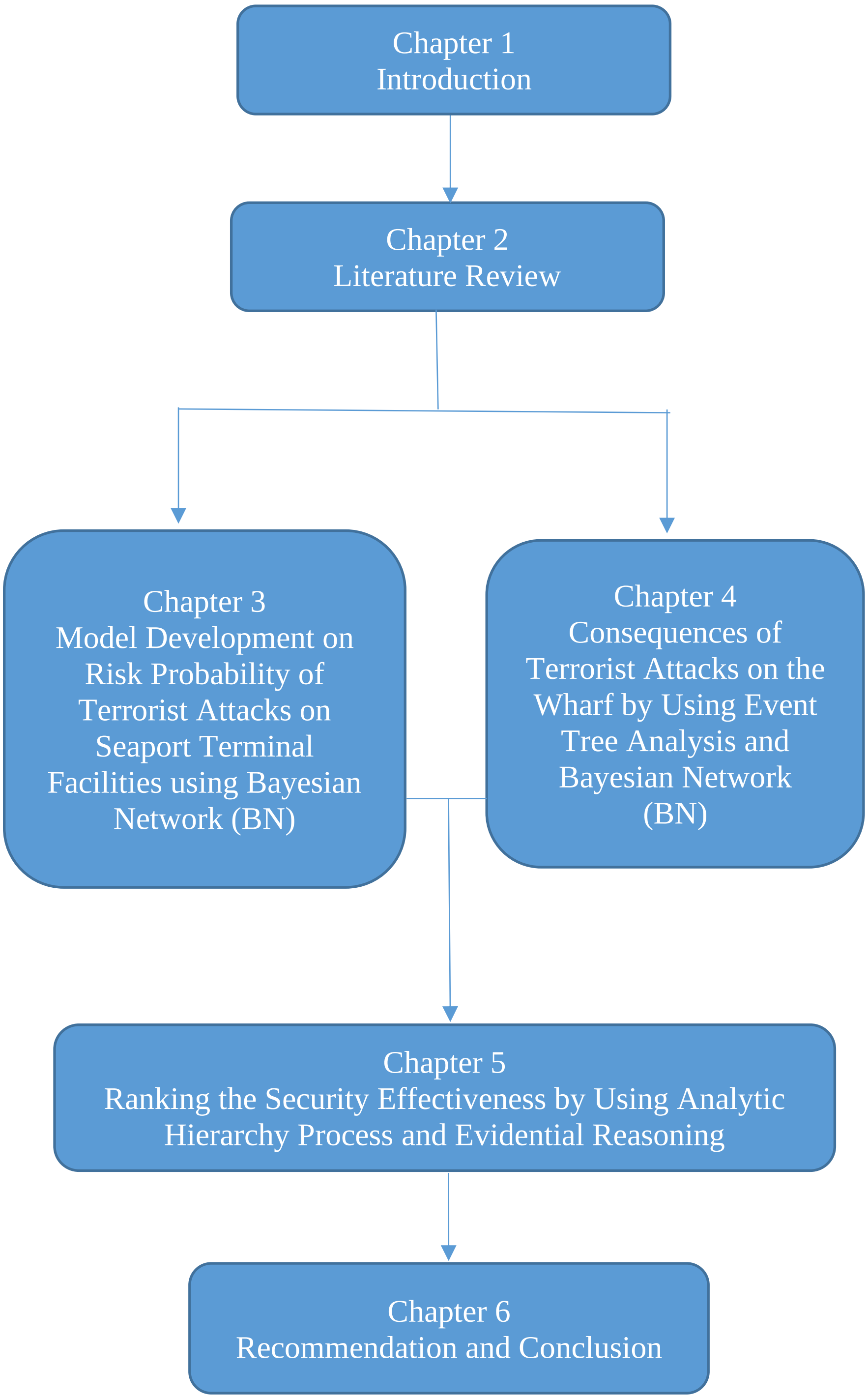

Chapter 1
Introduction
Chapter 2
Literature Review
Chapter 3
Model Development on Risk Probability of Terrorist Attacks on Seaport Terminal Facilities using Bayesian Network (BN)
Chapter 4
Consequences of Terrorist Attacks on the Wharf by Using Event Tree Analysis and Bayesian Network (BN)
Chapter 5
Ranking the Security Effectiveness by Using Analytic Hierarchy Process and Evidential Reasoning
Chapter 6
Recommendation and Conclusion

Figure 1.1: The Thesis Outline

Chapter One: Introduction

This chapter contains the background of the research and explanation necessary to justify the principal research objective and sub-objectives. The justification of the research study is also addressed to identify the importance of this study according to the industrial needs. A number of techniques and methods are highlighted in brief for consideration and links between them. Also, the research outline is addressed in brief. Finally, the limitation of this research is given to identify its boundaries.

Chapter Two: Literature Review

This chapter consist of four main topic which is 1) Definition of Sea Port, 2) Terrorism and Its Definition, 3) Definition of Risk Assessment and 4) Risk Assessment Methodologies. Definition of Sea Port explain about the Port Function, its categories, Port security and Risk in Port Facilities. Terrorism and Its Definition explain about Types of Terrorist, History of Terrorist, Terrorist Behaviour, Evolution of Terrorism, *et cetera.* Definition of Risk Assessment explain about Security Risk Assessment, Types of risk Assessment, Benefit conducting Risk Assessment, Weaknesses in Risk Assessment, *et cetera.* Risk Assessment Methodologies explain about method used in this study which is Bayesian Network, Event Tree Analysis, Analytic Hierarchy Process and Evidential Reasoning.

Chapter Three: Model Development on Risk Probability of Terrorist Attacks on Seaport Terminal Facilities by Using Bayesian Network (BN)

This chapter intends to identify which of the port facilities have the highest impact value in any terrorist attacks. This model development is motivated by security prioritisation and the risk reduction process of port facilities. This first technical chapter describes an advanced risk analysis methodology to identify and prioritise the port facilities under study in the element of uncertainties. The developed model is Bayesian Network (BN) Risk Assessment, which is used for uncertainty data combined with Root Cause Analysis (RCA).

Chapter Four: Consequences of Terrorist Attacks on the Wharf by Using Event Tree Analysis and Bayesian Network (BN)

This chapter focuses on the consequences of terrorist attacks at the wharf by using an event tree which is a standard technique in modelling accident systems. This chapter is a continuation from the previous chapter, where a further study was conducted on the subject of how effective the security countermeasures on wharf site are and the aftermath of the attack. Since the security countermeasures are complex and too big to be included in the event tree, a new approach was taken by combining Event Tree Analysis with a BN. In this chapter, three small Bayesian models were developed to predict the outcome of security countermeasures towards the probability of terrorist attacks on the seaport. These probability outcomes will then act as the countermeasures in the event tree analysis to calculate the consequence of the terrorist attacks on the wharf site port terminal.

Chapter Five: Ranking the Security Effectiveness by Using Analytic Hierarchy Process and Evidential Reasoning

This chapter focuses on the cost estimation and benefits of port security by ranking up the security countermeasures listed by using an analytic hierarchy process (AHP) approach and synthesising the outcome by using an evidential reasoning (ER) approach. This chapter is an extension from the previous chapter which estimates the consequences of a terrorist attack and the role of the existing security countermeasures. Since the previous results indicated the success of the existing countermeasures, this chapter further explores the security effectiveness as a whole including countermeasures on the terrorist attack at the wharf. The countermeasures will be listed in hierarchical order starting with the main criteria followed by the sub-criteria.

Chapter Six: Conclusions

In this chapter, the integration of the research model is discussed based on the security risk assessment on container port facilities. Also, how the principal objective and sub-objectives can be achieved and satisfied are addressed. The contribution of the research to knowledge is also discussed. Finally, this chapter recommends possible future research in this area.

1.5 The Limitation, Scope and Key Assumption

Although the study attempts to provide a comprehensive analysis related to the risk assessment and security countermeasures, due to the time constraints, the current study has some limitations in scope, which can be identified as:

A) The case study focuses on a seaport in a Southeast Asian country. The study is heavily related to the security system of the port and terrorist attack and normally port operators would refuse to even entertain such study, except for this one particular port where the researcher has previous employment history.

B) Limitation of Port Operator Requirement - Since the research is heavily related to security in port facilities and terrorism, it does have some constraints in terms of disclosing sensitive information. Port operators have agreed to allow a study to be done in their port and respond to the interview and questionnaire with some rules such as 1) study is not allowed to disclose the capability of security of that particular port in the thesis, 2) study is not allowed to disclose the amount of money invested into the security, and 3) security systems are only allowed to be discussed in terms of expert opinion rather than disclosing details.

C) It is impossible to predict where terrorist attacks will take place since the terrorists are intelligent and flexible (Ezell, 2010), and exploit weaknesses in defences to increase damage from their attacks (Brown, 2011). Therefore, to ensure a consistent feedback from different experts, an assumption was made. That assumption was that the terrorists have already set their target on the port to attack. Further explanation will be laid out in Chapter 3, Subtopic 3.3 under Step 5.

1.6 Conclusions

This chapter sets up the foundation for the study by introducing the background of research study, research problems and list of research objectives. Justification for the research is presented, the structure of the study is outlined and the limitations of the study are described. The detailed research proceeds on these foundations.

Chapter 2: Literature Review

Summary

This chapter begins with the definition of the Port and Port Development followed by Terrorism and Its Definition, Definition of Risk Assessment and Risk Assessment Methodologies.

2.1 Definition of Sea-Port

A port is important in terms of transportation and trade. It acts as a hub linking trading partners, the railroad and motorways. It supports a country's economy and acts as a gateway for trade, which consequently attracts the commercial infrastructure, such as industrial activities and banks (Alderton, 2008; Song & Panayides, 2008.) A port is also referred to as a town because it owns a harbour and facilities to cater for ships and customers (Alderton, 2008). Briefly the estimation that 90% of global trade is transported by using ships has proven that a port is significant in the world supply chain (Grzelakowski, A.S., 2014). A port is complex and it has roles in the logistic community (Bichou, 2004), such as supplying raw materials (e.g. oil and flour), and access to national industries and local supermarkets.

The placement of port usually at a strategic area where ships can load and unload their cargoes, such as at the coast, near estuaries, rivers or be artificially built. The geographical locations have different environments for each port, depending on whether it is perfect for building a port or not, for example, a tidal port would require more expense in land surveying operations and dredging than a traditional port (Alderton, 2008). Besides port locations, physical infrastructure ("hard") and various services ("soft") are in place to increase port functions. The physical infrastructure (a hard port), such as the amount of heavy-duty equipment and terminal size, is determined by location, region and port concentration. The soft port features include providing a wider selection for ship owners, specialisation in handling cargo (or container), shipping services, and integration of the global maritime network (Caldeirinha & Felício, 2014).

The main types of port asset are buildings, vertical infrastructure, warehouses, machinery for cargo handling, and information systems. Various services are available with these assets, whereby any attack that endangers these assets may affect port operational speed and efficiency (Boyes *et al*., 2016). However, if any physical attack was to happen at the port, it will not only damage a particular asset, for example, an attack on a building will also affect the information system since it is placed in the building. Therefore, it is important to categorise the assets based on location, such as assets on administrative sites and assets in wharfs.

A. Port Function and Its Category

A port function can be categorised into operational, administrative and engineering functions. Operational functions deal with cargo loading and unloading, storage and cargo distribution, pilotage, as well as tugging and mooring activities. Administrative functions are in charge of all paperwork that is needed when a ship arrives at the port, such as immigration, health inspections, customs, commercial documentary control and control of dangerous goods. Engineering functions include berth infrastructure, cargo network with roads and rail, industrial management and access to the sea and land (Alderton, 2008). It can be roughly divided into two categories, which are the bigger ports (main port that handles international trade) and smaller ports that cover the short marine and coastal transport. The bigger port not only has better performance, but also better economies of scale (Caldeirinha & Felício, 2014).

B. Port Security

Port security regulation was initiated when the United States decided to invest in the International Maritime Organisation in 1948, followed by a function of the Safety of Life at Sea (SOLAS) in 1974. Since then, a multitude of other international regulations sprouted concurrently (International Maritime Organization Conviction, EC regulation, US marine TPTN Security Act, Safety of Maritime Navigation, Australian MarSec Act, *et cetera*), reducing illegal activities, for example, human trafficking and international drug smuggling. Such regulations also facilitate flow of goods and people between countries worldwide (Eski, 2011). Over the years, a port has become the main focus for international and national security groups, who are trying to reduce, control, or even better, prevent any threats to the port. At first, their main interest was to provide a safe passage and anchorage, and the attention was moved to focus on containerisation since it is known that a container is an excellent way of transporting illegal immigrants and drugs because it is not regularly checked. In the United States, about 10 million containers passed through the ports annually and only 2% of them were examined (Eski, 2011).

In 2004, the International Maritime Organisation (IMO) adopted the *International Ship and Port Facilities Security* (ISPS) code that covers the confluence or meeting between ships and port facilities, port operators providing services to international ships, regulation on domestic ships and onshore operations, such as freight roads and rail transport companies and forwarders (Pinto & Talley, 2006; Thai & Grewal, 2007; Alderton, 2008). The ISPS code has set up three threat security levels, ranging from low to high in nature and scope of the incident or threat. It requires port operators to improve their port facility security plan (PFSP) for each threat level and nominate a port facility security officer (PFSO) (Bichou, 2004).

The standard framework for security and protection of maritime traffic and ports includes legal tools, (such as UNCLOS, SOLAS, MARPOL, the ISM and ISPS codes), and management measures (such as formal safety assessment and integrated coastal zone management) (Bichou, 2004). Maritime safety regulations are implemented differently at national and international levels, for example, individual nations need to set their own rules and norms in regard to different technical perspectives of ships and navigation to increase safety. A flag state is a country that regulates ships under its registrations and exercises its own jurisdiction and control over administrative, technical and social matters that relate to ships that operate under its flag to ensure safety at sea (Mansel, 2009).

C. Risk in Port Facilities

The ports industry is always considered as a silent industry since it operates by itself with little attention or involvement from the society, but it does not mean that it is immune from risks (Ahokas J, 2017). Risks at a port can affect the port, customers, stakeholders, and ultimately will affect the whole supply chain (Ho & Ho, 2006; Loh & Thai, 2015). The risk that may happen in the form of poor documentation, insufficient time or low budget allocation, for example, the implementation of port security regulations in safety planning has increased the importance of site design (Marsh & McLennan Companies, 2014.) Other risks that can cause supply chain disruption are port accidents, port equipment failures, mishandling of hazardous goods, financial losses, cargo or information theft, security breaches and labour strikes. These disruptions can have direct or indirect consequences (economic effect and the social well-being of the surrounding environment) on the operations and functions of the supply chain network, for example, an earthquake in 2011 caused serious disruption on port operations of a North Eastern Japanese port, and hence affected the warehouse and production facilities serving the port areas (Kurapati *et al*. 2015; Loh & Thai, 2015).

At the early stage of a port operation, it may be exposed to the risk of information clash, installation procurement of undemonstrated technologies and unreliable suppliers (Marsh & McLennan Companies, 2014). Even during the construction phase, it may have risks, such as design exposure (unable to complete the construction due to poor soil condition findings) or natural danger during port construction (earthquake, volcanic activity, flooding, tidal wave or wind storm) (Ministry of Defence of Finland, 2011; Marsh & McLennan Companies, 2014). Finally, during port operations, it is also exposed to risk in assets and equipment handling (damages or loss of assets, damage of sea walls, piers or wharf caused by natural disaster), turnover stream risk (strikes, transport accidents that affect the cargo handling movement), and liability risk (third parties operator injuries, causing damage to vessels or cargoes, fines and pollution risk) (Marsh & McLennan Companies, 2014).

Statistically, port incidents are usually unintentional and natural disaster risks, such as interrupted transport system due to an accident, damage to the machinery or personnel and environmental hazard. It was observed that almost 40% of port incidents happen at sea, 21% happen on land, which concerned warehousing, processes and transport, and 39% at a sea-land interface (Pinto & Talley, 2006). Nevertheless, the biggest unpredictable threat that may happen at sea and port is maritime terrorism. Maritime terrorism suggests that there is a potential of a group targeting the ships and port to achieve human casualties, economic losses, environmental damage, indoctrinate fear and other negative effects such as insecurities (Eski, 2011, Boyes *et al*., 2016).

2.2 Terrorism and Its Definition

Terrorism, as it is generally understood, involves the use of fear and violence against people, nations and their properties. It is used by political parties, societies and even organs of governments to instil fear among people or segments of the population to achieve group objectives. Usually terror is employed by rebels or non-state actors. However, there are instances where state or state-sponsored actors employ terror in their operations. Terrorism is not a new phenomenon. In fact, the Jacobins during the French Revolution in 1790s used terror and mass execution of its opponents by guillotine in order to stay in power. The era was called "the Reign of Terror". Throughout history, there are many examples of terrorism in use both by state and non-state actors.

Terrorism is not new and even though it has been used since the early times of recorded history, it can be relatively difficult to define terrorism. Terrorism has been variously described both as a tactic and strategy; crime and holy duty; justified reaction to oppression and an inexcusable abomination. Obviously, a lot depends on whose point of view is being represented. Terrorism has often been an effective tactic for the weaker side in a conflict. As an asymmetric form of conflict, it confers coercive power with many of the advantages of military force at a fraction of the cost. Due to the secretive nature and small size of terrorist organisations, they often offer opponents with no clear organisation to defend against or to deter. That is why pre-emption is being considered to be so important. In some cases, terrorism has been a means to carry on a conflict without the adversary realising the nature of the threat, mistaking terrorism for criminal activity. Because of these characteristics, terrorism has become increasingly common among those pursuing extreme goals throughout the world. But despite its popularity, terrorism can be a nebulous concept. Even within the U.S. Government, agencies responsible for different functions in the ongoing fight against terrorism and extremism use different definitions.

There are many definitions of "terrorism". Various parties generally have diverse definitions of terrorism. The samples of such definitions are given in table 2.1.

Table 2.1: Definition of Terrorism

Source	Definition of Terrorism
Laqeur (1977)	Terrorism is "the illegitimate use of force to achieve a political objective by targeting innocent people".
Bjorgo (2005)	Terrorism is a set of methods of combat rather than an identifiable ideology or movement, and involves premeditated use of violence primarily against non-combatants in order to achieve a psychological effect of fear on others than the immediate targets.
The United States Department of State (2002)	Define terrorism as "premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually to influence an audience"
United States Department of Defence	Defines terrorism as "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological." Note: Within this definition, there are three key elements– violence, fear, and intimidation and each element produce terror in its victims.
The US Federal Bureau of Investigations (FBI) (2005)	Terrorism is "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."
The United Nations	Definition of terrorism in 1992; "An anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or

	political reasons, whereby - in contrast to assassination - the direct targets of violence are not the main targets."
the British Government	Definition of terrorism (from 1974) is "...the use of violence for political ends, and includes any use of violence for the purpose of putting the public, or any section of the public, in fear."

In short, terrorism involves the use of illegitimate violence against non-combatant targets to intimidate and influence the people for the purpose of the perpetrators' political or social, including ideological or religious, objectives. So, terrorism is politically motivated, whereas crimes are financially or profit motivated. Terroristic acts aim to gain wide publicity from the violence and to inflict as much damage as possible. Prior to 9/11, terrorists generally aimed for wide publicity for their acts but after 9/11 the terrorists planned for as many casualties as possible (Desker, 2007).

Terrorism is a criminal act that influences an audience beyond the immediate victim. The strategy of terrorists is to commit acts of violence that draw the attention of the local populace, the government, and the world to their cause. The terrorists plan their attack to obtain the greatest publicity, choosing targets that symbolise what they oppose. The effectiveness of the terrorist act lies not in the act itself, but in the public's or government's reaction (fear) to the act. The introduction of this fear can be from the threat of physical harm or a grisly death, financial terrorism from the fear of losing money or negative effects on the economy, cyber terrorism harming the critical technological infrastructures of society and psychological terrorism designed to influence people's behaviour. Terrorism is designed to produce an overreaction and anecdotally, it succeeds at that almost all the time.

There are three perspectives of terrorism: the terrorist's, the victim's, and the general public. The phrase *"one man's terrorist is another man's freedom fighter"* is a view, terrorists themselves would gladly accept. Terrorists do not see themselves as evil. They believe they are legitimate combatants, fighting for what they believe in, by whatever means possible to attain their goals. A victim of a terrorist act sees the terrorist as a criminal with no regard for human life. The general public view though can be the most unstable. The terrorists take great pains to foster a "Robin Hood" image in hope of swaying the general public point of view towards their cause. This sympathetic view of terrorism has become an integral part of their psychological warfare and has been countered vigorously by governments, the media and other organisations.

A. Types of Terrorism

Over the past 20 years, terrorists have committed extremely violent acts for alleged political or religious reasons. Political ideology ranges from the far left to the far right. For example, the far left can consist of groups, such as the Marxists and Leninists who proposed a revolution of workers led by a revolutionary elite (Marxist-Leninist, 1990). On the far right, dictatorships that typically believe in a merging of state and business leadership are found. Nationalism is the devotion to the interests or culture of a group of people or a nation. Typically, nationalists share a common ethnic background and wish to establish or regain a homeland. Religious extremists often reject the authority of secular governments and view legal systems that are not based on their religious beliefs as illegitimate. They often view modernisation efforts as corrupting influences on the traditional culture. Special interest groups include people on the radical fringe of many legitimate causes, e.g. people who use terrorism and extremism to uphold anti-abortion views, animal rights, and radical environmentalism. These groups believe that violence is morally justifiable to achieve their goals. Terrorism campaigns vary according to their aims, resources, membership, beliefs, and contexts. Groups sometimes describe themselves as freedom fighters but may be branded by their enemies as terrorists. Generally, there are three types of terrorism, namely the revolutionary, sub-revolutionary and establishment terrorisms (Jenkins, 2017). This classification is inexhaustive and too simplistic.

Some researchers classify terrorism into six (NCJRS, 1976; Crime Museum, 2016) categories where the first is **civil disorder,** which is sometimes a violent form of protest held by a group of individuals, usually in opposition to a political policy or action. They are intended to send a message to a political group that “the people” are unhappy and demand change. The protests are intended to be non-violent, but they do sometimes result in large riots in which private property is destroyed and civilians are injured or killed. Second is **political terrorism,** which is used by one political faction to intimidate another. Although government leaders are the ones who are intended to receive the ultimate message, it is the citizens who are targeted with violent attacks. Third is **non-political terrorism,** which is a terrorist act perpetrated by a group for any other purpose, most often religious. The desired goal is something other than a political objective, but the tactics involved are the same. Fourth is **quasi terrorism,** which is a violent act that utilises the same methods as terrorists employ, but does not have the same motivating factors. Cases like these usually involve an armed criminal who is trying to escape from law enforcement utilising civilians as hostages to help them escape. The law breaker is acting in a similar manner to a terrorist, but terrorism is not the goal. Fifth is **limited political terrorism,** where the acts are generally one-time only plots to make a political or ideological statement. The goal is not to overthrow the government, but to protest a governmental policy or action. Sixth is **state terrorism,** which defines any violent actions initiated by an existing government to achieve a particular goal. Most often this goal involves a conflict with another country.

Martin (2017) classified terrorism into the following eight categories, starting from the **new terrorism** – this can be described as the new age terrorism characterised by its aim to cause mass casualties, different and creative organisational set-up, promotion of transnational religious solidarity and the exhortation of moral justification for its acts. Second is **state terrorism,** which is purely a state-sponsored terrorism against perceived enemies. Third is **dissident terrorism**, which are terrorist acts carried out by non-state rebels. Fourth is **religious terrorism**, which are terrorist acts carried out by groups based on religious beliefs or faiths. Fifth is **ideological terrorism**, which covers terrorist acts based on political ideologies. Sixth is **international terrorism**, which are terrorist acts that spread onto the international stage. Seventh is **criminal dissident terrorism**, which is motivated by profits, or in some instances, a combination of profit and ideological motives. Eighth is **gender-selective terrorism**, being terrorist acts targeted at males or females due to their perceived roles in certain issues.

B. History of Terrorism

Terrorist acts or the threats of such action were in existence for millennia. Despite having a history longer than the modern nation-state, the use of terror by governments and those that contest their power remains poorly understood. Meanwhile, the meaning of the word ‘terror’ itself is clear, but when it is applied to acts and actors in the real world it becomes confusing. Part of this is due to the use of terror tactics by actors at all levels in the social and political environment. For example, is the Unabomber, with his solo campaign of terror, a criminal, terrorist, or revolutionary (Chase, 2003, Chase, 2004)? Can he be compared to the French revolutionary governments who coined the word terrorism by instituting systematic state terror against the population of France in the 1790s, killing thousands? Are either the same as revolutionary terrorist groups, such as the Baader-Mienhof Gang of West Germany or the Weather Underground in the United States (Chitadze, 2014)?

Those distinctions of size and political legitimacy of the actors by using terror have raised questions as to what is and is not terrorism. The concept of moral equivalence is frequently used as an argument to broaden and blur the definition of terrorism as well. This concept argues that the outcome of an action is what matters, not the intent. Collateral or unintended damage to civilians from an attack by uniformed military forces on a legitimate military target is the same as a terrorist bomb directed deliberately at the civilian target with the intent of creating that damage. Simply, a car bomb on a city street and a jet fighter dropping a bomb on a tank are both acts of violence that produce death and terror. Therefore, at the extreme end of this argument, any military action is simply terrorism by a different name. This is the reason behind the famous phrase "One man's terrorist is another man's freedom fighter" (Vilde Skorpen Wikan, 2018, Here Begynneth, and Hood, 2018). It is also a legacy of legitimising the use of terror by successful revolutionary movements after the fact.

The flexibility and adaptability of terror throughout the years have contributed to the confusion. Those seeking to disrupt, reorder or destroy the status quo have continuously sought new and creative ways to achieve their goals. Changes in the tactics and techniques of terrorists have been significant, but the growth in the number of causes and social contexts where terrorism is used is even more significant.

Where It Began: 14th–18th Century - From the late 13th Century to the 1700s, terror and barbarism were widely used in warfare and conflict, but there was a lack of the key ingredients for terrorism. Until the rise of the modern nation state after the Treaty of Westphalia in 1648, the sort of central authority and cohesive society that terrorism attempts to influence barely existed (Gross, 1948). Communications were inadequate and controlled, and the causes that might inspire terrorism, such as religious schism, insurrection and ethnic strife, typically led to open warfare. By the time kingdoms and principalities became nations, they had sufficient means to enforce their authority and suppress activities such as terrorism.

The French Revolution provided the first uses of the word’s "terrorist" and "terrorism". "Terrorism" was first used in 1795 in reference to the Reign of Terror initiated by the revolutionary government (Linton, 2011). The agents of the Committee of Public Safety and the National Convention that enforced the policies of "The Terror" were referred to as terrorists. The French Revolution provided an example to future states in oppressing their populations. It also inspired a reaction by royalists and other opponents of the revolution who employed terrorist tactics, such as assassination and intimidation, in resistance to the revolutionary agents. The Parisian mobs played a critical role at key points before, during, and after the revolution. Such extra-legal activities, as killing prominent officials and aristocrats in gruesome spectacles started long before the guillotine was first used.

Entering the Modern Era: The 19th Century - During the late 19th Century, radical political theories and improvements in weapons technology spurred the formation of small groups of revolutionaries who effectively attacked nation-states. Anarchists espousing belief in the "propaganda of the deed" produced some striking successes, assassinating heads of state from Russia, France, Spain, Italy, and the United States. However, their lack of organisation and refusal to cooperate with other social movements in political efforts rendered the anarchists ineffective as a political movement. In contrast, Communism's role as an ideological basis for political terrorism was just beginning, and would become much more significant in the 20th Century. Another trend in the late 19th Century was the increasing tide of nationalism throughout the world, in which the nation, the identity of a people, and the political state were combined. The best-known nationalist conflict from this time is still unresolved are the multi-century struggle of Irish nationalism. Nationalism, like communism, became a much greater ideological force in the 20th Century. The terrorist group from this period that served as a model in many ways for what was to come was the Russian 'Narodnya Volya' (peoples will) (Hilbrenner, and Schenk, 2010). It differed in some ways from the modern terrorists, especially in that it would sometimes call off attacks that might endanger individuals other than its intended target. Other than this quirk, many of the traits of terrorism were seen here for the first time; clandestine, cellular organisation; impatience and inability for the task of organising the constituents they claim to represent; and a tendency to increase the level of violence as pressures on the group mount.

The Early 20th Century - The first half of the 20th Century saw two events that influenced the nature of conflict to the present day; the effects of two World Wars inflamed passions and hopes of nationalists throughout the world, and severely damaged the legitimacy of the international order and governments.

Nationalism on the Rise - Nationalism intensified during the early 20th Century throughout the world and it became a powerful force in the various colonial empires. Although dissent and resistance were common in many colonial possessions, and sometimes resulted in open warfare, nationalist identities became a focal point for these actions. Gradually, as nations became closely tied to concepts of race and ethnicity, international political developments began to support such concepts. Members of ethnic groups whose states had been absorbed by others or had ceased to exist as separate nations saw opportunities to realise nationalist ambitions. Several of these groups chose terror as a method to conduct their struggle and make their situation known to world powers, they hoped would be sympathetic. In Europe, both the Irish and the Macedonians had existing terrorist campaigns as part of their ongoing struggle for independence, but had to initiate bloody uprisings to further their cause. The Irish were partially successful, while the Macedonians failed.

Damaged Legitimacy - The “total war” practices of all combatants of World War II provided further justification for the “everybody does it” view of the use of terror and violations of the laws of war. The desensitisation of people and communities to violence that started in World War I accelerated during World War II. The intensity of the conflict between starkly opposed ideologies led to excesses on the part of all participants. New weapons and strategies that targeted the enemies’ civilian population to destroy their economic capacity for conflict exposed virtually every civilian to the combatant hazards. The major powers’ support of partisan and resistance organisations by using terrorist tactics was viewed as an acceptance of their legitimacy. It seemed that civilians had become legitimate targets, despite any rules forbidding it (Kiras, J.D., 2006).

Cold War Developments - The bi-polar world of the Cold War changed perception of global conflicts. Relatively minor confrontations took on significance as arenas where the superpowers could compete without risking escalation to full nuclear war. Warfare between the East and West took place on the peripheries, and was limited in scope to prevent escalation. During the immediate post-war period, terrorism was more of a tactical choice by leaders of nationalist insurgencies and revolutions. Successful campaigns for independence from colonial rule occurred throughout the world, and many employed terrorisms as a supporting tactic. When terrorism was used, it was used within the framework of larger movements, and coordinated with political, social, and military action. Even when terrorism came to dominate the other aspects of a nationalist struggle, such as the Palestinian campaign to reclaim their land against Israel, it was combined with other activities. Throughout the Cold War, the Soviet Union provided direct and indirect assistance to revolutionary movements around the world by giving free weapons and training. Many of these organisations and individuals utilised terrorism in support of their political and military objectives. The policy of the Soviet Union to support revolutionary struggles everywhere, and to export revolution to non-communist countries, provided extremists willing to employ violence and terror with the means to realise their ambitions (Kiras *et al.*, 2006).

The Internationalisation of Terror - The age of modern terrorism might be said to have begun in 1968 when the Popular Front for the Liberation of Palestine (PFLP) hijacked an El Al airliner *en route* from Tel Aviv to Rome (Jenkins, and Johnson, 1975). Meanwhile, even though hijackings of airliners had occurred before, this was the first time that the nationality of the carrier (Israeli) and its symbolic value was a specific operational aim. Also, a first was the deliberate use of the passengers as hostages for demands made publicly against the Israeli government. The combination of these unique events, added to the international scope of the operation and gained significant media attention. The founder of PFLP, Dr. George Habash, observed that the coverage level was a lot greater than battles with Israeli soldiers in their previous area of operations. Another aspect of this internationalisation is the cooperation between extremist organisations in conducting terrorist operations. Cooperative training between Palestinian groups and European radicals started as early as 1970, and joint operations between the PFLP and the Japanese Red Army (JRA) began in 1974. Since then, international terrorist cooperation in training, operations, and support has continued to grow, and continues to this day. Motives range from the ideological, such as the 1980s alliance of the Western European Marxist-oriented groups, to financial, as when the Irish Republican Army (IRA) exported its expertise in bomb making as far afield as Colombia (DTIC, 2003).

Current State of Terrorism - The largest act of international terrorism occurred on September 11 often referred as 9-11, 2001 in a set of co-ordinated attacks on the United States of America, where the terrorists hijacked civilian airliners and used them to attack the World Trade Centre (WTC) towers in New York City and the Pentagon in Washington, DC. The effects of 9/11 had a significant impact on the American psyche and led to global reverberations. Other major terrorist attacks have also occurred in New Delhi where the Indian Parliament was attacked (Sultan, 2001); Bali car bomb attack; London subway bombings; Madrid train station bombings; attacks in Mumbai (hotels, train station and a Jewish outreach centre, Nigeria, Pakistan, Paris, and more.

C. Terrorist Behaviour

There is clearly a wide choice of definitions for terrorism. Despite this, there are common elements among the majority of useful definitions. Common threads of various definitions identify terrorism as political, psychological, using force, dynamic, deliberate, media exploitation, illegality of methods and preparation, and support.

1) ‘Political’ is a terrorist act that is political or is committed with the intention to cause a political effect by merely eliminating the intermediate step of armies and warfare, and applied violence directly to the political contest. 2) ‘Psychological’ means the intended results of terrorist acts cause a psychological effect, which is “terror” by aiming at a target audience (other than the actual victims of the act) which may be the population as a whole, some specific

portions of a society, or decision-making elites in the society’s political, social, or military populace. 3) ‘Using force’ is where violence and destruction are used in the commission of the act to achieve the targeted result, even if the casualties are not the results of a terrorist operation intended, the potential of violence itself is what produces the intended effect. For example, a successful hostage taking operation may result in all hostages being freed unharmed after negotiations and bargaining. Regardless of the outcome, the terrorist bargaining chips were nothing less than the raw threat of applying violence to kill some or all of the hostages. When the threat of violence is not credible, or the terrorists are unable to implement violence effectively, then the terrorism fails (DTIC, 2003).

4) ‘Dynamic’ is when terrorist groups demand change, revolution, or political movement by justifying that terrorism mandates a drastic action to destroy or alter the status quo. 5) ‘Deliberate’ is when terrorism is an activity planned to achieve particular goals and it is a rationally employed, specifically selected tactic, and is not a random act (remember that the actual target of terrorism is not the victim of violence, but the psychological balance). Operations in permissive societies will make terrorists conduct more operations in societies where individual rights and civil legal protections prevail. While terrorists may base themselves in repressive regimes that are sympathetic to them, they usually avoid repressive governments when conducting operations wherever possible. An exception to this case is a repressive regime that does not have the means to enforce security measures. Governments with effective security forces and few guaranteed civil liberties have typically suffered much less from terrorism than liberal states with excellent security forces (DTIC, 2003).

6) ‘Media exploitation’ has terrorism’s effects that are not necessarily aimed at the victims but at a third party by sending information of the attack to the targeted audience. The next step in transmission will depend on what media is available, but it will be planned, and it will frequently be the responsibility of a specific organisation within the terrorist group to do nothing else but exploit and control the news cycle. News media can be manipulated by planning around the demands of the “news cycle”, and the advantage that control of the initiative gives to the terrorist. Pressures to report quickly, to “scoop” competitors, allow terrorists to present claims or make statements that might be refuted or critically commented on if time were available. Terrorists often provide names and details of individual victims to control the news media through their desire to humanise or personalise a story but the impact on the survivors (victims) is of minimal importance to the terrorists. What is important is the

intended psychological impact that the news of their death or suffering will cause in a wider audience.

7) ‘Illegality of methods’ is where terrorism is a criminal act; by choosing to identify himself (or themselves) with military terminology, as discussed under the insurgencies below, or with civilian imagery (“brotherhood”, “committee”, etc.), he (or they) is a criminal in both spheres. The violations of civil criminal laws are self-evident in activities, such as murder, arson, and kidnapping, regardless of the legitimacy of the government enforcing the laws. If the terrorist claims that he is justified by using such violence as a military combatant, he is a *de facto* war criminal under international law and the military justice systems of most nations. 8) ‘Preparation and support’ are when the actual terrorist operations are the results of extensive preparation and support operations. Media reporting and academic study have mainly focused on the terrorists’ goals and actions, which are precisely what the terrorists intend. This neglects the vital but less exciting topic of preparation and support operations. Significant effort and coordination are required to finance group operations, procure or manufacture weapons, conduct target surveillance and analysis, and deliver trained terrorists to the operational area. Meanwhile the time and effort expended by the terrorists may be a drop in the bucket as compared to the amount spent to defend against them (DTIC, 2003).

D. Types of Terrorist Incidents

The 9/11 attack by Al-Qaeda on the World Trade Centre in New York, United States on 11 September 2001 is the reference point for the New Terrorism category; hence, it brings some new perspectives on terrorism. Al-Qaeda, which hitherto carried out attacks on targets outside of the United States borders has brought its “war” to its enemy’s doorstep. That particular attack also became the turning point in the fight against terrorism on the urging of the United States government. In addition, the event started the beginning of debates on Islam and Muslims as terroristic in nature. There are usually seven types of terrorism attacks, namely bombing, hostage-taking, armed attack, arson, hijacking, biological/radiological/chemical attacks, and others (DTIC, 2003).

Bombings are the most common type of terrorist act since the improvised explosive devices are inexpensive, easy to make, and modern devices are getting smaller (harder to detect). They also have very destructive capabilities; for example, on August 7, 1998, two American embassies in Africa were bombed where over 200 people died, and over 5,000 civilians were injured. Terrorists can also use materials that are readily available to the average consumer to construct a bomb. Arson and fire bombings are easily conducted by terrorist groups that may not be as well-organised, equipped, or trained as a major terrorist organisation since the incendiary devices are cheap and easy to hide. They usually target a utility, hotel, government building, or industrial centre to portray an image that the ruling government is incapable of maintaining order. Armed attacks (such as raids and ambushes) and assassinations (killing of selected victims, usually by small arms) are very deadly such as drive-by shooting is a common technique employed by unsophisticated or loosely organised terrorist groups. As for assassinations, terrorists have assassinated specific individuals with aims for psychological effect (DTIC, 2003).

Hostage-takings is where terrorists use kidnapping and hostage-taking to establish a bargaining position and to elicit publicity. Kidnapping is difficult but, if successful, it can gain terrorists money, release of jailed comrades, and publicity for an extended period. Hostage-taking not only involves the seizing of a facility and the taking of hostages, it also provokes a confrontation with the authorities, it forces the authorities to either make dramatic decisions or to comply with the terrorists' demands. It is overt and designed to attract and hold media attention. The terrorists' intended target is the audience affected by the hostage's confinement, not the hostage. Hijackings (seizing by force of a surface vehicle, its passengers, and its cargo) and skyjackings (the taking of an aircraft, which creates a mobile, hostage barricade situation) provides terrorists with hostages (a human shield, making retaliation difficult) and draws heavy media attention (Brandt, *et. al.*, 2009).

In addition to the acts of violence discussed above, there are also many other types of violence that can exist under the terrorism framework. Terrorist groups conduct maiming against their own people as a form of punishment for security violations, defections, or informing and conduct robberies and extortion when they need to finance their acts and they do not have sponsorship from sympathetic nations. Historically, terrorist attacks by using nuclear, biological, and chemical (NBC) weapons have been rare. Due to the extremely high number of casualties that NBC weapons produce, they are also referred to as weapons of mass destruction (WMD). However, a number of nations are involved in arms races with neighbouring countries because they view the development of WMD as a key deterrent of attack by hostile neighbours. The increased development of WMD also increases the potential for terrorist groups to gain access to WMD. It is believed that in the future terrorists will have greater access to WMD because unstable nations or states may fail to safeguard their stockpiles of WMD from accidental losses, illicit sales, or outright theft or seizure. Determined terrorist groups can also gain access to WMD through covert independent research efforts or by hiring technically skilled professionals to construct the WMD (Reed-Schrader, *et. al.*,2019).

E. The Evolution of Terrorism

Terrorism is continuously changing. While at the surface it remains "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear…" it is rapidly becoming the predominant strategic tool of adversaries. As terrorism evolves into the principal irregular warfare strategy of the 21st Century, it is adapting to changes in the world socio-political environment. Some of these changes facilitate the abilities of terrorists to operate, procure funding, and develop new capabilities. Other changes are gradually moving terrorism into a different relationship with the world at large. To put these changes into context, it will be necessary to look at the historical evolution of terrorism, with each succeeding evolution building upon techniques pioneered by others. This evolution is driven by ongoing developments in the nature of conflict and international relations. It is also necessary to consider some of the possible causes of future conflicts, in order to understand the actors and their motivations.

When describing the evolution of terrorism and use of terror through history, it is essential to remember that forms of society and government in the past were significantly different from what they are today. Modern nation-states did not exist in their present form until 1648 (Treaty of Westphalia), and the state's monopoly on warfare, or inter-state violence, is even more recent (Gross, 1948). The lack of central government made it impossible to use terror as a method of affecting a political change, as there is no single dominant political authority. Also, the absence of central authority meant that the game of warfare was open to many more players. Instead of national armies, a variety of non-sovereign nobility, mercenaries, leaders of religious factions, or mercantile companies participated in warfare. Their involvement in warfare was considered to be perfectly legitimate. This is in contrast to the modern era, where nations go to war, but private participation is actually illegal.

Early theories of terrorism - The period of warfare and political conflict that embroiled Europe after the French Revolution provided inspiration for political theorists during the early 1800s. Several important theories of social revolution developed during this time. The link between revolutionary violence and terror was developed early on. Revolutionary theories rejected the possibility of reforming the system and demanded its destruction. This extremism laid the groundwork for the use of unconstrained violence for political ends. The ideologies that embraced violent social change were Marxism, which evolved communism, and anarchism. Both were utopian; they held that putting their theories into practice could produce ideal societies. Both advocated the complete destruction of the existing system. Both acknowledged that violence outside the accepted bounds of warfare and rebellion would be necessary. Communism focused on economic class warfare, and assumed seizure of state power by the working class (proletariat) until the state was no longer needed, and eventually disposed of. Anarchism advocated more or less immediate rejection of all forms of governance. The anarchist's belief was that after the state is completely destroyed, nothing will be required to replace it, and people could live and interact without governmental coercion. In the short term, communism's acceptance of the need for an organisation and an interim coercive state made it the more successful of the two ideologies. Anarchism survived into the modern era and retains attraction for violent extremists to this day.

20th Century Evolution of Terrorism **-** In the early years of the 20th Century, nationalism and revolutionary political ideologies were the principal developmental forces that acted upon terrorism. When the Treaty of Versailles redrew the map of Europe after World War I by breaking up the Austro-Hungarian Empire and creating new nations, it acknowledged the principle of self-determination for nationalities and ethnic groups (DTIC, 2003). This encouraged minorities and ethnicities not to receive recognition to campaign for independence or autonomy. However, in many cases, self-determination was limited to European nations and ethnic groups and denied others, especially the colonial possessions of the major European powers, creating bitterness and setting the stage for the long conflicts of the anti-colonial period.

In particular, Arab nationalists felt that they had been betrayed. Believing they were promised post-war independence, they were doubly disappointed; first when the French and British were given authority over their lands; and then, especially when the British allowed Zionist immigration into Palestine in keeping with a promise contained in the Balfour Declaration (Balfour, 1917). Since the end of World War II, terrorism has accelerated its development into a major component of contemporary conflict. Primarily in use immediately after the war as a subordinate element of anti-colonial insurgencies, it expanded beyond that role. In the service of various ideologies and aspirations, terrorism sometimes supplanted other forms of conflict completely. It also became a far-reaching weapon capable of effects no less global than the intercontinental bomber or missile. It has also proven to be a significant tool of diplomacy and international power for states that are inclined to use it.

The seemingly quick results and shocking immediacy of terrorism made some consider it as a shortcut to victory. Small revolutionary groups not willing to invest the time and resources to organise political activity would rely on the "propaganda of the deed" to energise mass action. This suggested that a tiny core of activists could topple any government through the use of terror alone. The result of this belief by revolutionaries in developed countries was the isolation of the terrorists from the population they claimed to represent, and the adoption of the Leninist concept of the "vanguard of revolution" by tiny groups of disaffected revolutionaries. In less developed countries, small groups of foreign revolutionaries such as Che Guevara arrived from outside the country, expecting to immediately energise revolutionary action by their presence (Guevara, 2002).

F. Terrorism in Southeast Asia

Southeast Asia is a region surrounded by sea since all Southeast Asian countries are on the seaboard (except Laos). Indonesia and the Philippines are essentially archipelago countries in the region. Historically, with the exception of Thailand, all Southeast Asian countries were under colonial rules for the greater part of their modern history and in most of them armed rebellion against colonial powers was the violent part of their journey to nationhood. In many of these countries, there are ethnic and religious minorities who are at one point of time or another in their respective histories were involved in armed rebellion, and hence by simple definition involved in terrorism. In the case of Kampuchea, there was once a state-sponsored terrorism under the Khmer Rouge regime in 1975 until ten years later.

Being a maritime region, sea routes and ports are vital "facilities" to the Southeast Asian region. The Strait of Malacca is the busiest trade sea route. The strait is 600 miles long and about 26 tankers and 200 boats use its narrow sea-lane daily (Ho, 2006). They carry 525 million tonnes of goods worth USD390 billion daily. The narrow straits is bordered by three littoral countries, namely Indonesia, Malaysia and Singapore. To the south of Singapore is the territory of Indonesia, comprising big and small islands. On the other side of Peninsular Malaysia, there is the maritime border between the Malaysian State of Sabah and the Southern Philippines.

On land, most terroristic attacks in Southeast Asian countries are revolutionary, ideological or religious in nature. In Indonesia, recent terrorist attacks were carried out by "Islamic" groups either with affiliation to foreign terror groups, such as Al-Qaeda or the ISIS or non-affiliated home-grown disaffected groups. Attacks were in the form of bombing of churches or non-mainstream Islamic sects such as Ahmadia and the Shias, and the bombing of tourism targets on the island of Bali. The bombing of churches happened mostly on the island of Java and a few on the island of Sulawesi. Ethnic unrest has also happened in Ambon.

In Thailand, many violent attacks happen in the restive southern provinces where there are the Malay Muslim minority. Attacks are carried out against security force installations or mobile targets and sometimes at markets. The mode of attacks comprises bombings, including roadside explosive devices and shooting of individual targets. These violent incidents are carried out by the "freedom fighters" not terrorism groups.

In the Philippines, terror attacks are attributed to the communist party's New People's Army (NPA) in the north and the Muslim autonomy seeking fighters, such as the Mindanao National Liberation Front (MNLF) and the Mindanao Islamic Liberation Front (MILF) in the south. The types of attack are armed assaults, bombings against military targets and armed forces. However, in the south there are groups that are classified as terror organisations by the United States. They are the Abu Sayyaf Group (ASG), al-Qaeda, Jemaah Islamiyyah (JI).

G. Piracy

Another important aspect of "terrorism" incident in the Southeast Asian regions is piracy. Many parties especially prefer to include piracy or sea robbery in the list of terrorism and therefore, these should be dealt with under the counter-terrorism programmes. By definition, terrorism is politically motivated, while piracy or robbery is financially motivated. Acharya (2007) said that "of all the international terrorist incidents over a period of the last 30 years, only 2% of the attacks involved maritime assets." The reasons for such an observation are, most of the terrorists are basically land-lubbers, second, targets on land are generally easier to attack than targets at sea (to attack targets in open seas needs careful and costly planning), and special skills and sophisticated weapons are needed to attack targets at sea. By extension, terrorists who attack targets at sea are most probably the people who live in maritime localities, and in possession of naval skills as well as weaponries. People living in Southeast Asian countries live in maritime areas. They possess naval skills but the only resources they need to acquire are the weaponries. Sjaastad (2007) defined Piracy as an "activity that takes place in the high seas, not in the territorial waters of some littoral states".

The United Nations Convention on the Law of the Sea (UNCLOS) defines piracy as, firstly, any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed: (i) on the big seas, against another ship or aircraft, or against persons or property on board such ship or aircraft and, (ii) against a ship, aircraft or persons or property in places outside the jurisdiction of any state. Secondly, by any act of voluntary participation in operation of a ship or an aircraft with knowledge of facts, making it a pirate ship or aircraft and thirdly, any act of inciting or of intentionally facilitating an act that is firstly or secondly defined in sub-paragraph. This definition, combined with the social and geographical make-up of Southeast Asia, tends to "exclude" violent acts at sea from the scope of terrorism. This has a vital impact on countermeasures against terrorism.

H. Terrorism in Malaysia

Geographically, Malaysia is comprised of two lands, which are separated by the South China Sea, namely the Malaysian Peninsular and the two states on the Island of Borneo. The Straits of Malacca lies on the west coast of Peninsular Malaysia, while the Sulu Sea forms a border between the north Bornean state of Sabah and the South Philippines. Due to its proximity with the Southern Philippines' semi-lawless area and the border being porous, Sabah has experienced violent and terroristic attacks. Most of the attacks have been kidnap-for-ransoms. The Abu Sayyaf group is the most active actor in this respect. The terrorists attack targets on shore as well as at sea, taking the people, especially vessel crews back to their hideouts in the Southern Philippines and making ransom demands. They do not attack ports in the area instead they target crews and tourists on islands and the only big incident was the attack on the town of Lahad Datu on 11 February 2013. In most cases, hostages were freed when ransoms were paid.

In Peninsular Malaysia, the most violent terroristic attacks were carried out by local militants. In July 2015, two men attacked a nightclub in Puchong, Selangor, a suburb of Putrajaya, by using grenades, causing injury to eight people. On 2 July 2000, a band of militants under the Al-Maunah group attacked and occupied an army camp in Gerik, Perak for a week. Earlier on in the 1990s, there was the *Kumpulan Mujahidin Malaysia* (KMM), which aimed to overthrow the Malaysian government and replace it with an Islamic regime. By 2004, KMM was no longer active.

It seems that there are few terrorist groups in Malaysia that give great threats to the country's security and foreign parties, except for the occasional incursions into Sabah waters by the groups in the Southern Philippines. In Peninsular Malaysia, the terrorists are too few to be of any threat and damage from the few attacks that did take place, was small in nature. They were merely small groups whose members were incited by the religious vision of their leaders.

The same cannot be said in regard to the sea. Malaysia shares its western maritime border with Indonesia in the Straits of Malacca. Being the busiest sea trade route in the world, ships plying the narrow Straits of Malacca risk being attacked by terrorists and criminals alike. In 2001–2005, there were 72 attacks on harbours and anchorages, 28 robberies at sea and 14 kidnap-for-ransoms. On harbours and anchorages, 51 out of the 72 attacks were carried out on the Indonesian side of the maritime border and so were 20 of the 28 robberies. In the case of kidnap-for-ransoms around the Straits of Malacca and Straits of Singapore, the majority were carried out in the Indonesian waters and by mostly Indonesia-based groups. The *Gerakan Acheh Merdeka* (GAM) was suspected of carrying out kidnap-for-ransom attacks but it admitted to only two cases.

As a whole, terrorist groups in Malaysia are external in nature. Sjaastad, (2007) concluded that the level of terrorist activity in Malaysia is considered comparatively low to other Southeast Asian nations. The Malaysian government maintains that its strict laws and police activity have undermined the existing networks of terrorism in Malaysia and have continued to prove to be the effective deterrents to extremism. However, in August 2018, the Defence Minister of Malaysia, Mohamad Sabu expressed his concerned about 100,000 Rohingya refugees in Malaysia that are vulnerable to be recruited by terrorist groups. “We are very concerned that the Rohingya refuges could be manipulated to become suicide bombers or recruited into terrorist cells in this region,” he said (The Star, 2018). Bukit Aman Special Branch Counter Terrorism Division head, Deputy Comm. Datuk Ayob Khan, said that there were already four cases of IS trying to recruit members from the Rohingya community in Malaysia since 2015.

I. Trends in Terrorism

As a conflict method that has survived and evolved through several millennia to flourish in the modern information age, terrorism continues to adapt to meet the challenges of emerging forms of conflict, and exploit developments in technology and society. Terrorism has demonstrated increasing abilities to adapt to counter-terrorism measures and political failure. Terrorists are developing new capabilities of attack and improving the efficiency of existing methods. Additionally, terrorist groups have shown significant progress in escaping from a subordinate role in nation-state conflicts, and becoming prominent as international influences in their own right. They are becoming more integrated with other sub-state entities, such as criminal organisations and legitimately chartered corporations, and are gradually assuming a measure of control and identity with national governments.

Adaptive Capabilities of Terror Groups - Terrorists have shown their ability to adapt to the techniques and methods of counter-terror agencies and intelligence organisations over the long term. The decentralisation of the network form of organisations is an example of this. Being adopted to reduce the disruption caused by the loss of key links in a chain of command, a network of organisations also complicates the tasks of security forces, and reduces predictability of operations. Terrorists have also been quick to use new technologies, and adapt existing ones to their uses. The debate over privacy of computer data was largely spurred by the spectre of terrorists, planning and communicating with encrypted data beyond law enforcement's ability to intercept or decode this data. To exchange information, terrorists have exploited disposable cellular phones, over the counter long-distance calling cards, Internet cafes, and other means of anonymous communications. Embedding information in digital pictures and graphics is another innovation employed to enable the clandestine global communication that modern terrorists require.

Terrorists have also demonstrated significant resiliency after disruption by counter-terrorist action. Some groups have redefined themselves after being defeated or being forced into dormancy. The Shining Path of Peru (Sendero Luminosa) lost its leadership cadre and founding leader to counter-terrorism efforts by the Peruvian government in 1993. The immediate result was severe degradation in the operational capabilities of the group. However, the Shining Path has returned to rural operations and organisation in order to reconstitute itself. Although not the threat that it was, the group remains in being, and could exploit further unrest or governmental weakness in Peru to continue its renewal. In Italy, the Red Brigades (Brigate Rossi) gradually lapsed into inactivity due to governmental action and a changing political situation. However, a decade after the supposed demise of the Red Brigades, a new group called the Anti-Capitalist Nuclei emerged exhibiting a continuity of symbols, styles of communiqués, and potentially some personnel from the original Red Brigade organisation. This ability to perpetuate ideology and symbolism during a significant period of dormancy, and re-emerge under favourable conditions demonstrates the durability of terrorism as a threat to modern societies (Strong, S., 1992).

Increasing Capabilities of Terrorists - Terrorists are improving their sophistication and abilities in virtually all aspects of their operations and support. The aggressive use of modern technology for information management, communication and intelligence has increased these activities' efficiency. Weapons technology has become increasingly available, and the purchasing power of terrorist organisations is on the rise. The readily available technologies and trained personnel to operate them allow the well-funded terrorists to equal or exceed the sophistication of governmental counter-measures. Likewise, due to the increase in information outlets, and competition with increasing numbers of other messages, terrorism now requires a greatly increased amount of violence or novelty to attract the attention it requires. The tendency of major media to compete for ratings and the subsequent revenue realised from increases in their audience size and share produced pressures on terrorists to increase the impact and violence of their actions to take advantage of this sensationalism.

J. Cyber Terrorism

Until recently, terrorism was associated with physical acts of violence and crime, for example, killings, bombings, kidnappings and destruction of property. Starting in the 20th Century the increasing advent of technology, and more specifically systems controlled by computers, have seen a new form of criminal activity that has often combined destruction of property with financial crime, propaganda, economic warfare and possibly physical harm to innocent human lives. Cyber-terrorism is relatively "young" in its evolution and has been associated with individuals, terrorist groups and state actors or countries, which in particular, could escalate into cyber war.

Viruses, Malware and Trojans - Computer viruses have been around for almost as long as networked computers have existed. "Creeper" is credited as being the first virus that infected DEC machines on the ARPANET (predecessor of the Internet) in the 1970s. Today, viruses, adware, malware and Trojans may be considered as a nuisance by most everyday computer users. They are often used by criminals to either steal personal information or turn unsuspecting computers into zombie bots, used to generate spam or conduct distributed denial of service (DDoS) attacks. Methods of deployment include infected application files, infected documents, virus attachments in emails, infected USB keys/thumb drives and "drive by infections", where a website is hacked to inject malicious code to the computers that just happen to visit it. This realm of computer viruses, rootkits and Trojans is not limited to hackers, terrorists and organised crime mafias. Governments and their associated agencies have also been implicated in designing and deploying sophisticated systems to conduct espionage against other states. Stuxnet, Dugu and Flame are just some examples that may have involved state actors, both in their design, deployment and targets, and certainly do blur the line between cyber terrorism and cyber warfare (Janczewski, L. ed., 2007).

Networked Infrastructure - Electrical grids, the banking system, water distribution, traffic management, communication systems, air traffic control, mass transit, and military systems, all tend to be operated in some sort of a networked fashion. Connectivity, in this case, does not imply that these systems are openly connected to the Internet and may use private networks (physical or virtual). The problems occur when security is often compromised for the sake of convenience and cut corners. To manage the electrical grid or the traffic management system in a city remotely, connectivity is needed. Does it make sense to build a completely private network (dedicated cables) for each of these infrastructure systems? In some cases, yes, but many implementations tend to piggyback on existing shared infrastructure, believing that it can be fully secured. Hackers and cyber terrorists are able to find these vulnerabilities and exploit them to access the core systems, which can be destructive to this networked infrastructure. Therefore, protecting security infrastructure is much harder than expected and leads to vulnerabilities that can only be countered by constant vigilance and expert personnel is a cost that is often overlooked (Janczewski, L. ed., 2007).

Criminal elements - Cybercrime and cyber terrorism do often intersect in that one can be used to fund the other (either in its virtual or physical form). Organised crime is deeply involved in sophisticated cybercrime activities that one would see with spam, identity theft, bank fraud, shady prescription medication sales, drugs, pornography, human trafficking, prostitution, virtual heists, including stealing bitcoin and other cryptocurrency fraud, credit card fraud, money laundering, peddling fake or stolen merchandise, phone fraud, malware/spyware/ransomeware and other nefarious activities. The funds and expertise they gain from their cybercrime sprees allow them to expand their virtual and ″bricks and mortar″ operations, often making them cyber mercenaries available to the highest bidder whether they are terrorist groups, countries or other criminals.

Terrorist Propaganda - The Internet has also proven to be a great venue for terrorist groups to spread their propaganda. Websites extolling terrorist views started cropping up almost as soon as the Internet started on its ascent as a revolutionary medium for communication. This is problematic but those that try to use this as an excuse to censor online content and discussions do miss the point that this is also a great eye opener to the majority of the people that do not subscribe to such views. It exposes terrorists to law enforcement agencies (as part of their investigations and by attracting terrorists to disclose their agendas through "honey pots"), the media and the public. As mentioned in the above section, networked infrastructure and websites, though they may be “secured” by passwords, encryption or other more sophisticated tactics will always be vulnerable.

How to protect against Cyber Terrorism - Most cyber terrorism targets are large organisations; governments, utilities, infrastructure, businesses, and financial institutions, but there are things that individuals can do to ensure they can protect themselves or minimise the impact of cyber terrorism. First, use strong passwords (long in length and a combination of alphabets, numbers and special characters). Second, use different passwords for different websites. Third, update systems when patches are released or vulnerabilities discovered (update your operating system, browsers, anti-virus/security programmes, firmware, etc.). Fourth, use more secure operating systems (like Linux) where possible. Fifth, use virtual machines (with software like Virtualbox) when installing unknown software or visiting sketchy web sites. Sixth, secure personal networks (Wifi passwords with encryption and firewalls). Seventh, do not install random, untrusted software on devices, especially on smartphones and tablets. Eighth, test personal network for vulnerabilities, and ninth, secure data by using strong encryption where possible (Janczewski, L. ed., 2007).

2.3 Definition of Risk Assessment

Risk assessment is a process of evaluating potential risks that may appear in a project, operational sites, or an organisation (Jiaqi, 2017). It is an intensive process, starting from discovering what the potential risks are, where they are and what assets matter the most and how to mitigate the said risks to an acceptable level for the business to go on (Ng, 2003). A risk assessor must find out all about the systems, processes and people involved, the threats and elements of vulnerabilities and be familiar with all security aspects, be it physical and environmental, administrative and management as well as the countermeasures (Ng, 2003). Meanwhile, there are many risk assessment methods, such as BN, ER, TOPSIS, and ETA, which often reduce to their components of analysis such as threats, vulnerability, frequency, severity and exposure. The disadvantage of a risk assessment is that it is related to the subjective estimations of the risk values. Therefore, it is important to select a professional expert to do the task (the UK National Cyber Security Centre, 2016). Conducting a risk assessment is a complex and lengthy process; thus, it is best to focus certain risk assessment projects on a defined area of an organisation, such as physical condition of port facilities (according to Tech Target) (Jiaqi, 2017).

Table 2.2: Definition of Risk Assessment

Guidelines and Standards	Definition of Security Risk Assessment
NIST Risk Management Guide	Risk assessment is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.
NIST Guide for Security Certification and Accreditation	The periodic assessment of risk to agency operations or assets, resulting from the operation of an information system is an important activity required by the Federal Information Security Management Act of 2002 [FISMA].
The IT Governance Institute	Risk assessment is the identification and analysis by management of relevant risks to achieve predetermined objectives, which form the basis for determining control activities. Note: The IT Governance Institute recognises that risk assessments may be performed at the company level or an individual activity level.
The ISO 17799	Risk assessment is the systematic consideration of the business harm which is likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.

A. Security Risk Assessment

Security risk assessment measures the strength of overall security programmes and provides information for future improvements. It gives an indication to the management department on the level of effective measurement of its security control and how well it protects its assets or facilities (Landoll, 2005). The goal of a security risk assessment is to assess the risks faced by the organisation in respect of its assets and information and then use that information to mitigate those risks and effectively preserve the organisational mission. In the myriad spheres of governing regulations, guidelines and standards, ‘‘security risk assessment’’ is defined in numerous ways. Some definitions are more detailed than others in terms of how an assessment is performed. Some definitions focus on the result of the assessment, while others focus on the approach. Security risk assessment is defined as an objective analysis of effectiveness of the current security controls that protects an organisation’s assets and a determination of the probability of losses to those assets (Landoll, 2005).

B. Types of Risk Assessment

Generally, there are two types of risk assessment, namely qualitative and quantitative risk assessments. In quantitative risk analysis, numeric values (e.g. monetary values) are independently assigned to the different risk assessment components as well as the level of potential losses. When all elements (asset value, threat frequency, safeguard effectiveness, safeguard costs, uncertainties and probability) are quantified, the process is considered to be fully quantitative (Ng, 2003). Qualitative risk analysis does not assign numeric values to the risk assessment components. It is scenario-based and the assessors or participants go through different threat-vulnerability scenarios and try to answer a "what if" type of question. Generally, qualitative risk assessment tends to be more subjective in nature.

C. Benefits of Conducting Risk Assessment

Risk Assessment "has become a proven technology that addresses risks in a structured manner and ensures that risks are managed in the most effective way." (Mullai, 2006). A properly managed risk assessment can bring many benefits to an organisation.

First, risk assessment recognises and is able to control potential hazards at a workplace or an organisation. Proper risk assessment begins with identification of potential hazards and their risks on the organisational operations, and assessing their vulnerabilities and impact to the business's ability to provide services and operations. It also helps an organisation to select the best option to mitigate threats or instituting countermeasures. Hazards are conditions, characteristics or situations that exist at a work place or operation sites and can cause potential harm. An organisation that has proper risk assessment can mitigate hazards and contribute towards its efficient operations. Seaports are part of the world's trade systems. They provide livelihood to cities where they are located and to neighbouring cities from which the goods are handled and move into their economies. Seaports and cities handle voluminous goods and they may attract attacks by criminals who are looking for spoils from their actions and terrorists who "like" the potential publicity they may get from their deeds. The risk ensuing from these threats should be properly assessed for the organisation and the authorities to be able to avoid catastrophes and potential losses (Ng, 2003).

Second, risk assessment can lead to awareness among the staff of an organisation or worksites. Awareness leads to healthy and safe work environment and practices. This in turn prevents potential losses in the said organisation in terms of downtime, medical costs, operation and disruptions. Risk assessment can be made as training tools for the staff (Ng, 2003). Third, risk assessment can reduce incidents and accidents at a workplace or operation site. Incidents and accidents are costs to an organisation, which may become costly if not properly managed. Risk assessment promotes better allocation of resources in the safety management and eventually overall efficient cost management and good work practice in the organisation or workplace.

Fourth, a security risk assessment is an important element for any organisation that seeks to protect its assets. A port security refers to the safeguarding of vessels, harbours, the port itself, waterfront facilities, and cargo from internal or external threats, such as losses or injuries from accidents or criminal or terroristic acts. These threats need to be assessed in respect of the overall port security and security objectives. Finally, proper risk assessment can lead to overall risk-preparedness. A high degree of risk-preparedness can prevent potential losses for the organisation or workplace. Reactive measures are not good management practice as compared to preventive ones (Ng, 2003).

In a nutshell, security risk assessment is necessary for the following reasons:

1. Checks and balances - Security risk assessment provides a review of an organisation's current assets protection. The assessment consists of checking up the work of security operation staff, determining the adequacy of the programme and taking note of any areas that require improvements. Security risk assessment checks and balances exercise on the organisational asset's integrity (Landoll, 2005).

2. Periodic review-The best security systems notwithstanding, an organisation requires periodic reviews of its systems. Periodic reviews provide information on how effective is the security system and offer necessary adjustments to its programmes, considering changing threat environment and business mission. Changes in an organisation's business ecosystem may affect its security systems too. Security risk assessment, therefore, acts as a periodic review mechanism for an organisation, especially seaports (Landoll, 2005).

3. Risk-based spending - An organisation or business concern usually has limited resources to spend on security issues and without security risk assessment, it may not have an understanding of the threats and subsequently the risks it faces and its assets that need protection. Resources allocated or spent on security items may not be suitable to its mission and this may cause overspending or inefficient spending. Security risk assessment plays an important role in helping an organisation to have a risk-based spending system that will save its spending on security items (Landoll, 2005).

4. Requirement - In many instances, security risk assessment is a required element for a security programme in accordance with the established regulations. These regulations include ISPS Code, HIPAA, GLBA, FERC Cyber Security Standards, ISO 17799, OMB A-130, and many others. If for no other reasons, many organisations conduct a security risk assessment simply because it is required by law (Landoll, 2005).

5.Security risk assessment secondary benefits - Aside from the obvious primary benefits mentioned above, security risk assessment has secondary benefits to an organisation in the form of possible knowledge transfer from the security assessment team to the organisation's other staff, increased communications in regard to security among its business units, increased security awareness within it, and the results of the security risk assessment may be used to measure its security posture and compare its previous and future status (Landoll, 2005).

D. Weaknesses Encountered in Risk Assessment

While there are countless benefits to be gained by an organisation in conducting risk assessments in its operations, there are however, a number of difficulties encountered in the process by the organisation. Ng (2003) listed a few difficulties, but the most common is the time factor. Many system and infrastructure owners complain that they do not have enough time to rigorously carry out the whole risk assessment process.

In other cases, the organisations do not possess adequate knowledge and skills to carry out the risk assessment on their assets and processes. Some do not know where and how to start the processes. However, there are many guidelines in the market on risk assessment and management. The difficulties that lie in the form of some guidelines are too general, while others are too detailed. There are also differences between the various levels of guidelines. The way to be out of the above difficulties is to resort to outsourcing the tasks to external or third-party experts. This solves the common problems but to some organisations, this method is costly and there is always a possibility for the organisation to become over-dependant on the vendors. Whichever way it is, it is imperative for an organisation to carry out risk assessment and risk management on its operations and assets.

E. Risk in Maritime Transportation

There are three parties involved in a ship's safety throughout its life, which are the ship designer who is actively involved during the planning and building stage, the shipbuilder during its construction and finally the ship owner when the ship is in operation, including the training stage for the ship operators (Soares & Texeira, 2001). Soares and Texeira (2001) also stated that the existing maritime safety risk can be estimated based on accident statistics. The study allows the identification of the time and safety levels, and safety differentiation according to the ship features, such as type, size, and age. Accidents are caused by the ship structural failure and/or human errors. Galic (2014) classified the causes of maritime accidents into unintentional human error, intentionally caused by man, accidents due to technical failure and accidents due to poor weather (wind, waves, and lightning). Meanwhile, Soares and Texeira (2001) put the responsibilities on ship designers, builders and operators. Galic (2014) attributed the factors affecting maritime safety to shippers, ports and port authorities, coastal countries and international community. According to them, between 1996 and 2005, there were 84 fatalities per 100,000 seafarers. Losses of 50% were due to sinking, followed by grounding or stranding (18%), fires and explosions (15%) and hull failures (2%).

The International Maritime Bureau (IMB) data until 2014 showed that factors affecting navigation safety are professional (in-) competence, insufficient manning on board ships, piracy and language barrier, especially among crews. In regard to piracy, the IMB identified that the eastern and western coasts of Africa and Indonesia (on the Straits of Malacca and Singapore Straits) as the locations of frequent piracy attacks. Accidents, to a certain extent, indicate the type and level of risks in maritime transportation. The following list shows the type of accidents and risks in maritime transportation: 1) Foundered includes ships that sank as a result of heavy weather, springing of leaks, breaking in two and other causes that did not fit in other categories. 2) Fire and explosion cover cases in which fire and explosion are the first event reported in accidents. 3) Collision includes ships lost as a result of striking or being struck by another ship. 4) Contact covers the cases in which the ships collide with another external body, which is not a ship, nor the bottom. This category only started to be recorded after 1980, included in collision before that date. 5) Wrecked or stranded include the ship lost as a result of touching the sea bottom. 6) Hull or machinery damage include accidents that were initiated by one such failure.

2.4 Risk Assessment Methodologies

There are many methodologies available for the risk assessment exercises. Security practitioners have to decide and choose which is the most suitable for their respective organisations.

Firstly, the asset audit approach which is an approach that looks at the assets the organisation has and makes assessments on whether or not they are adequately protected (Scott, 1973). This approach requires a few steps starting with information asset identification by identifying all organisational data that has to be assessed, stored, processed, transmitted or accessed. The data may include programme source codes, backup tapes and customer information. Then, determine the data flow (which identified informational asset arrives and leaves the system). The third step is to determine the different threat mechanisms that can be used to acquire the information as data that enters the system, is stored in the system and leaves the system. Then, determine how likely it is that each identified threat mechanism will occur and assess the impact of data being disclosed, corrupted or destroyed or unavailable for a certain period of time. Finally, select the relevant safeguards or controls that need to be implemented to protect the organisation's information assets.

These controls can be technical (e.g. install personal firewalls on all remote users' computers) or non-technical (e.g. acceptable use policy or security awareness programmes). The asset audit approach is an easy-to-use and straightforward method for assessing risks by giving the reviewers and owners a direct approach of looking at all the information assets and their risk exposure. The people involved in the asset audit process will also get better understanding of how information flows in and out of, as well as, being stored into the system. With this knowledge and insight, the reviewer can have a better picture of what assets and at which locations are at risk, and thus need protection.

Secondly, the Pipeline Model method where it can prove useful for sizing up the security of transactional systems (Brewer, 2003) where the risks are assessed on a "pipeline". Each pipeline is made up of five process components, which is active process (all processes that make the transaction happen), communications process (responsible for sending/receiving messages (data) over the networks), stable data process (responsible for inserting stable information into the pipeline), enquiry process (responsible for extracting information from the pipeline), and access control process (responsible for controlling human access to the pipeline). The security requirements for each pipeline are derived from the security policy of the organisation. Each pipeline is reviewed according to the mentioned five components to determine whether the security requirements are met, and if not, what are the gaps needed to be addressed.

Thirdly, the attack trees, which are a variation of fault trees which provide a methodical way of describing the security of systems based on who, when, how, why and with what probability an attack will happen (Schneier, B., 1999). The top of the attack tree or its root node represents the ultimate goal of the attacker and the branches and leaf nodes show the different ways of attaining the goal. The following steps describe how an attack tree can be built, starting with identifying all threat agents that might attack the system. These would include dishonest or disgruntled employees, script kiddies, users, administrators, and competitors. Second, explore and consider the ultimate goal or goals of each threat agent. Each goal will then be the root node of each attack tree. Then, identify all possible ways which the threat agent could use to attain the goal; the attack methods then become the second level goals that come under the root node. After that, for each second level goal, consider whether there is the next level of details or ways of attaining the sub-goal. This process is repeated until each of the leaf nodes on the attack tree is a single and specifically defined method. Finally, review and evaluate each attack path to determine the likelihood of each method being used to attack the system, assess its business impact if the ultimate goal was attained by the attacker and what countermeasures can be used to stop the attack. The attack trees method of risk assessment may not be suitable for a novice security reviewer who may not have enough experience and knowledge to have the insight needed to identify all the different attack methods that would be used by different attackers.

Besides the above risk assessment methodologies which have been used and proven to be effective and practical, there are also other popular risk assessment methods that were developed and used in the security industry, such as OCTAVE which stand for Operationally Critical Threat, Asset and Vulnerability Evaluation (Alberts, C.J., *et al*, 1999, Storms, 2004), Risk Management Guide for Information Technology Systems, developed by the National Institute of Standards and Technology (NIST) (Stoneburner, 2002), and a self-help guide for risk assessment - Security Self-Assessment Guide for Information Technology Systems, (Swanson, 2001) which provides a quick and low-cost method of assessing the security within an organisation through a series of self-assessment questionnaires. Liu (2012) proposed a method in which the results of threat assessment, vulnerability assessment and impact assessment were gathered to determine a numeric value of risk for each asset and threat pair (Federal Emergency Management Agency (US) (Brown, 2003; Kennet, 2005)) in accordance with the following risk formula:

$$Risk = T \times V \times I \qquad (2.1)$$

Where,

T = threat rating, V = vulnerability rating and I = Impact Rating

The entire process of risk assessment can be summarised as firstly, identify the assets and people that need protection. Secondly, perform a threat assessment to identify and define the threats that could cause damage or harm to the facility and its inhabitants. Thirdly, conduct a vulnerability assessment to identify weaknesses that might be exploited by terrorists or aggressors. Lastly, compute the risk by using the results of the asset value, threat, and vulnerability assessments.

A. Bayesian Network (BN) Introduction

BN are graphical models that combine probability theory with graph theory (Jordan, 1998), which means that they can adopt reasoning under uncertainty (Jensen & Nielsen, 2007). They are capable of combining various pieces of information and use expert judgement to compensate for the absence of secondary data and deal with incomplete information. The inferences of BN were originally discovered by Thomas Bayes (Bayes & Price, 1736). Then it was developed into an attempt to combine (incorporate) probability theory into a system, to help in decision-making (Neapolitan, 1990). Later, it focused on game theory in the early 1930s and 40s (Shafer, 1990).

The games later evolve into sequential games versus uncontrolled nature and abstractions, such as decision trees, were developed. Therefore, Bayesian decision theory gained increased popularity (Wald, 1950) in the 1950s. In the 1960s the basic Bayesian theory was then developed into a more relevant level (Howard, 1968; North, 1968; Raiffa, 1968). BN, which was the first marriage of the Bayesian Probability Theory with Networking Techniques, was developed at Stanford University in the 1970s (McCabe *et al*., 1998). The BN approach had gained speedy development with the advent of good computing facilities, and was able to process the probability information in conditioned networks. In the 1980s, BN was used in the field of expert systems (Pearl, 1982, Bayes & Price, 1736, Spiegelhalter & Knill-Jones, 1984). The first real application of BN was MUNIN (Muscle and Nerve Inference Network) (Andreassen *et al*., 1989).

Since then onwards, BN becomes increasingly popular and is used to solve real-world problems (Szolovits & Pauker, 1993; Russell & Norvig, 2016). Some examples include the building of expert systems to assist in Artificial Intelligence analyses, medical diagnosis and software development (Heckerman *et al*., 1995). Recently, BN leads to many new applications with very complex problems that require the processing of large number of variables to overall uncertainty cases. It also expands into systems risk assessors and reliability analysis.

Earlier works indicated the similarities between BN and QRA (Quantitative Research Analysis) approaches which show the potentials of BN in modelling and analysis capabilities

(Cagno *et al*., 2000; Mahadevan & Rebba, 2005). Then BN covers a wide variety of fields, such as decision analytic issues (Kuikka *et al*., 1999; Barton *et al*., 2008; Helle *et al*., 2011), integrated modelling (Varis & Kuikka, 1997; Molina *et al.,* 2010; Borsuk *et al.,* 2012; Rahikainen *et al.,* 2014) and participatory modelling (Bromley *et al.,* 2005; Castelletti & Soncini-Sessa, 2007; Carmona *et al.,* 2011; Mantyniemi *et al*., 2013), analysing human behaviour related to uncertainties in the implementation of management actions (Haapasaari *et al*., 2007; Haapasaari & Karjalainen, 2010) and compiling and formalising expert knowledge (Lecklin *et al.,* 2011). BN has now become available in inexpensive software systems since they were successfully applied to a variety of problems.

BN provides a tool to deal with more than one problem that has uncertainties in it and is complex, and BN's role in the design and analysis of machine learning algorithms is really important. The advantage of BN in using a graphical model is the modularity, where it becomes a complex system by combining simpler and smaller models. The probability theory ensures the whole system is consistent and provides ways to interface models to data. The graph side of graphical models allows appealing interface by modelling an interacting a set of variables and efficient algorithm data structure.

B. Event Tree Analysis (ETA) Introduction

Event Tree Analysis (ETA) is a logical modelling technique for both "success" and "failure" that explored responses through a single starting event and then placed a path for assessing probabilities of the outcomes (Clemens, *et. al*., 1998). This analysis technique is used to analyze the effects of any functioning or failed systems, given that an event has occurred (Wang *et. al.,* 2000). ETA is a modelling technique, which produces branches of events from one single event by using Boolean Logic. ETA will identify all consequences of a system that may happen after the starting event. By using ETA as a tool in risk assessments, outcomes can be prevented from occurring by providing a risk assessment of the probability of occurrence and forward logic process (Ericson & Clifton, 2005).

I) History of ETA

ETA was first introduced in 1975 on The Reactor Safety Study called WASH 1400 for the nuclear power plant safety study and the technique was called Probabilistic Risk Assessment (Byrne, and Hoffman, 1996). The design was adopted in 1968, as United Kingdom Atomic Energy Authority (UKAEA) to optimize the steam generating heavy water reactor. It uses the assumption that the protective system would either work or fail. ETA identifies all risks that follow an initiating event, some of which can be eliminated due to their effects being too small to affect the overall result. In an underwater excavation project in the Han River, Korea, a risk analysis was conducted by using an earth pressure balance Tunnel Boring Machine. ETA was used to quantify risks, by providing the probability of occurrence of an event, in the initial design stages of the tunnel construction to prevent possible accidents because then tunnel constructions in Korea were known for being top in injury and fatality rates within the construction industry (Hong & Eun-Soo; 2009).

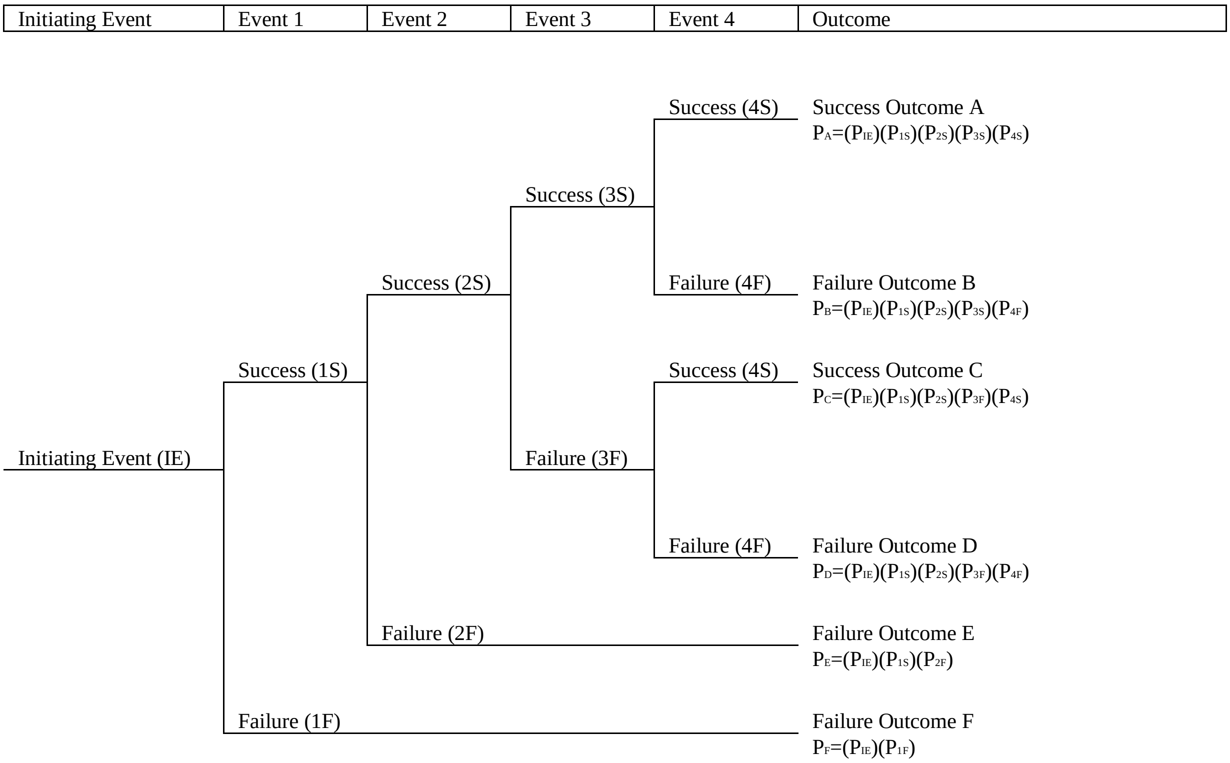


Figure 2.1: ETA Diagram Example

II) Theory of ETA

ETA starts with a set of initiating events that change the state of the system (Ericson, 2005). An initiating event is an occurrence that starts a reaction, such as a spark can start a fire that can lead to another event (intermediate events) such as a factory burning down, and then finally a consequence, for example, the burnt factory no longer produces goods. Each initiating event leads to another event, where the probability of each intermediate event or occurrence may be calculated until an end state is reached (the outcome of a factory no longer producing goods) (Ericson, 2005). Intermediate events are commonly split into a "success/failure" or "yes/no" categories but they may also be split into more than two as long as they do not occur at the same time. A spark, as an initiating event, has the chance of turning into a fire or not, as well as the probability that the fire spreads throughout the factory or not.

End states can be categorised as either “success” or “loss”, for example, a “success” end-state would be that there was no fire started and the factory still produces goods. Meanwhile, a “loss” end-state would be that a fire did start and the factory could no longer continue goods production. The “loss” end state can be any state at the end of the path that results in a negative outcome of the starting event. The “loss” end state is highly reliant upon the totality of a system, for example, the declining quality of products is a loss to the manufacturer (Ericson, 2005). The following list describes some of the examples of “loss” end-states:

- Loss of life or injury/illness to personnel (Ericson & Clifton, 2005).
- Failure of a mission (Ericson & Clifton, 2005).
- Loss of system availability (Ericson & Clifton, 2005).
- Damage to the environment (Ericson & Clifton, 2005).
- Damage to or loss of equipment or property (including software) (Ericson & Clifton, 2005).
- Unexpected or collateral damage as a result of tests.

III) ETA’s Advantages and Disadvantages

ETA in Risk Analysis

ETA can be used in risk assessments by determining the probability that is used to determine the risk when multiplied by the threat of the event. ETA is a tool that makes it easy to see what path is creating the highest probability of failure for a particular system. It is common to find single point failures that do not have any intervening events between the starting event and a failure. With ETA, single point failures can be targeted to include an intervening step that will reduce the overall probability of failure, and thus lessen the risks in a system. The idea of adding an intervening event can happen anywhere in the system for any path that generates “highs” of a risk; the additional intermediate event can reduce the probability, and thus lessen the threat.

Table 2.3: Advantages and Limitation of the ETA

Advantages of the ETA

Enables assessment of multiple, co-existing faults and failures (Clemens *et. al.*, 1998).
Functions simultaneously in cases of failure and victory (Clemens *et al*., 1998).
No need to anticipate end events (Clemens *et al.*, 1998).
Areas of single point failure, system vulnerability, and low payoff countermeasures may be identified and assessed to deploy resources properly (Clemens *et al.*, 1998).
Paths in a system that lead to a failure can be identified and traced to display ineffective countermeasures (Clemens *et al.*, 1998).
Can be performed at various detail levels (Ericson, 2005).
Visual cause and effect relation (Ericson, 2005).

Relatively easy to learn and execute (Ericson, 2005).
Models complex systems in an understandable manner (Ericson, 2005).
Combines hardware, software, environment, and human interactions (Ericson, 2005).
Follows fault paths across system boundaries (Ericson, 2005).
Permits probability assessment (Ericson, 2005).
Commercial software is available (Ericson & Clifton, 2005).

Limitations of the ETA

The initiating challenge must be identified by the analyst (Clemens *et al*, 1998).
Pathways must be determined by the investigator (Clemens *et al.*, 1998).
The level of loss for each path may not be distinguishable without further analysis (Clemens, et al., 1998).
Addresses only one Initiating Event at a time (Clemens et.al, 1998).
Success or failure probabilities are difficult to find (Clemens et al., 1998).
Can overlook subtle system differences (Ericson, 2005).
Partial successes/failures are not distinguishable (Ericson, 2005).
Requires an analyst with practical training and experience (Ericson, 2005).

IV) ETA Software

Although ETA can be relatively straightforward, it can be used for more complex systems to build diagrams and complete calculations more quickly with little human error. There is a lot of software available to assist in conducting an ETA. The software is not accessible from the local store but can be easily found with an online search. In the nuclear industry, Risk Spectrum PSA software usually uses ETA combined with fault tree analysis.

C. Analytic Hierarchy Process (AHP)

The AHP is an approach that builds a hierarchy (or ranking) of decision items by using comparisons between each pair of items expressed as a matrix (Pair-wise Comparison). Paired comparison yields weighting scores that take into account the level of importance for each criterion and sub-criterion. It is based on the mathematical structure of consistent matrices to generate the right weights (Merkin, 1979; Saaty, 1980 and 1994, Rahman, N.A., 2012). AHP was developed to optimise decision-making when the decision makers are faced with a mix of qualitative, quantitative, and sometimes conflicting factors that have to be taken into consideration. AHP so far is very effective in making decisions that are complicated, and often irreversible.

In getting the right decision for an organisation in the present situation as well as in the future, it is essentially important to apply intelligence, wisdom and creativity to evaluate the benefits of a decision, the risks involved, the expenses and the possible impacts if the decision goes wrong. Decision-making methods vary from the simple tossing of a coin, to the more structured decision-making tools; and a sound decision-making tool involves the consideration of all important and relevant factors. One such decision-making tool is the AHP developed by Thomas Saaty. Thomas was a professor at the Wharton School of Business and a consultant with the Arms Control Disarmament Agency. Meanwhile he may face a problem of dealing with high costs and a host of considerations dealing with many factors that were conflicting with each other and not easily specified. He then developed AHP in the 1970s as a way of dealing with weapons trade-offs, resource and asset allocations, and decision-making (Alexander, 2012).

AHP forms a hierarchy from a list of problems by using the judgement of decision makers, and the complexity of the problems is represented by the number of levels in the hierarchy. The hierarchy is used to generate ratio scaled measures for decision alternatives and values that alternatives have against organisational goals and project risks. AHP is typically used in prioritising factors that have impacts on organisational productivity, and in evaluating the quality of investment proposals, choosing among several strategies to improve safety features in certain products, estimating costs for materials requirement planning and selecting desired software components from several software suppliers. AHP is suitable in analysing both quantitative and qualitative criteria and can take a large quantity of criteria into consideration. It can also facilitate the construction of a flexible hierarchy to address the problems (Rahman, 2012).

D. Evidential Reasoning (ER)

The evidential reasoning (ER) approach has been developed by Dempster in 1967 and then refined by Shafer in 1976 on the basis of decision theory, in particular, the utility theory (Rahman, 2012). For certain reasons, the ER approach is often referred to the Dempster-Shafer theory of evidence or D-S theory. In theory, the ER approach is an evidence-based multi-criteria decision analysis (MCDA) approach where it was created for dealing with problems that have quantitative and qualitative criteria under uncertainty by utilising individual knowledge, experience and expertise in the forms of belief functions (Rahman, 2012).

It has been used to support decisions, analyses, assessment and evaluation activities such as organisational self-assessments (Keeney, *et al*., 1976) based on a range of quality models, offshore design (Wang *et al*., 1995), system evaluation on large engineering project (Yang & Sen, 1997), artificial intelligence, in particular the theory of evidence, environmental impact assessments (Yang & Xu, 2002) statistical analysis and computer technology, crude oil tanker selection (Lee, 2008), and container line security assessment (Riahi, 2010).

The ER approach has recently been developed on evidential reasoning algorithms (Xu *et. al*, 2006) to aggregate criteria for generating distributed assessments, and the concepts of the belief and plausibility functions to generate a utility interval for measuring the degree of ignorance. A conventional decision matrix used for modelling an MCDA problem is a special case of a belief decision matrix (Wang *et al*., 2006 & Yang, 2013). The major advantages of the ER approach are as follows (Riahi, 2010):

i) It is capable of providing its users with a greater flexibility by allowing them to express their judgments both subjectively and quantitatively.
ii) It accepts data of different formats with various types of uncertainties as inputs, such as single numerical values, probability distributions, and subjective judgments with belief degrees.
iii) It is capable of accommodating or representing the uncertainty and risk that is inherent in decision analysis.
iv) It allows all available information embedded in different data formats, including qualitative and incomplete data, to be maximally incorporated in assessment and decision-making processes.
v) An assessment of an option can be more reliably and realistically represented by a belief decision matrix than by a conventional decision matrix.
vi) As a hierarchical evaluation process, it is capable of offering a rational and reproducible methodology to aggregate the data assessed.
vii) It allows assessment outcomes to be represented more informatively.
viii) It is capable of obtaining the assessment output using mature computing software, called the Intelligent Decision System (*IDS*) (Yang & Xu, 2002).

Chapter 3: Model Development on Risk Probability of Terrorist Attacks on Seaport Terminal Facilities by Using Bayesian Network (BN)

Summary

Ports are exposed to various risks, both in their internal operation as well as external business interactions with other maritime logistics companies. While traditional safety and security policies are able to deal with accidents, theft, and hazard-based risks in ports, a new risk assessment is urgently required to tackle those that are caused by threats, such as terrorist attacks. Terrorist attacks have always been classified as a disruption risk because they pose a bigger risk of causing enormous damage, unlike a natural disaster. In contrast to natural disasters, such as storms or earthquakes, terrorist attacks do not have a similar pattern among them and usually terrorists will attack a port at its weakest point or where it can cause the highest impact values. Therefore, it is important for port stakeholders to identify and pinpoint which of the port facilities have the highest impact value for any terrorist attacks. This model development is motivated by security prioritisation and the risk reduction process of port facilities. This first technical chapter describes an advanced risk analysis methodology to identify and prioritise the port facilities under study in the element of uncertainties. The model developed is Bayesian Network (BN) Risk Assessment, which is used for uncertainty data and combined with Root Cause Analysis (RCA). The model considers different types of possible terrorists, different types of attacks, security breaches and different types of port sites/facilities that may be targeted. Realising the different threat modes incorporated in the model, the outcomes can either be a standalone technique for prioritising critical systems, such as port facilities with high-risk or as part of a decision-making method for security control.

3.1 Introduction

There have been many studies conducted on supply chain risks in regard to new policies development, new technologies application and various information technology programmes. Supply chain risks include operational and disruption risks (Tang, 2006). Operational risks are mostly related to uncertainty elements in a process, such as customer demands, amount of supply, and cost fluctuations. Disruption risks involve natural and human disasters, such as earthquakes, floods, hurricanes, terrorist attacks, financial crises, or labour strikes (Kleindorfer & Saad, 2005, Feng *et al*., 2010, Bhattacharya *et al*., 2013, Acciaro & Patrizia, 2013).

The development on supply chain risk studies is due to supply chain disruptions and terrorist attacks, one of which is the September 11 incident in 2001. These events involve high risk factors and to deduce a common pattern that can lead to the development of predictable preventive measures is difficult if we use the traditional quantitative risk assessment methods because of incomplete or unavailable historical data. This makes the threats and risks impossible to be completely eliminated and they can only be reduced with emergency responses and preparedness through a careful study.

In any whole supply chain network of a port operation, there are a number of pit-stops that the cargo needs to go through (Hu & Zhu, 2009). Each pit-stop, such as a port or a depot, is called a node and connections among the nodes are called links. Acting as the critical node point, as a sea and land interface, a port plays a crucial role to ensure smoothness and efficiency of an increasingly complex supply chain network (Robinson, 2002; Ng, 2007, Yang, 2014). Therefore, there are high threat potentials and vulnerabilities to such nodes due to the involvement and interactions of numerous stakeholders (Brooks, 2008).

If a terrorist attack occurs and strikes a supply chain node, it may be a little too late for the port operator to take emergency action without any preparation and facilities (Snyder et. al., 2008). The goals of this study are:

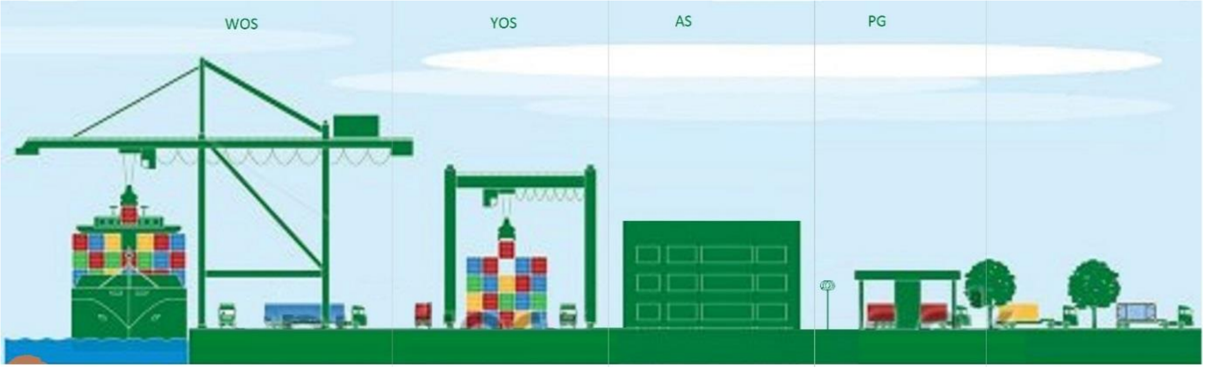
1- To identify the types of possible attacks.

2- To identify different types of facilities that can be a target.

3- To identify which of the facilities are potentially most vulnerable in terms of security.

A port performs four main functions in its business which are to 1) ensure the legal, and economic interests of the state are protected, 2) promote the state's interests into a wider regional economy, 3) handle import and export goods, and 4) act as a trade hub where various modes of transport interchange (such an interchange consists of loading, discharging and transit of goods). Such a colossal function requires the port to have massive facilities to execute its myriad operation. Facilities in a port are called by various names such as Wharf, Quay, Harbour, Container Terminal, Oil/Chemical/Gas Terminal, Bulk Terminal, Passenger Terminal, Repair/Maintenance Facilities, Maritime Administration, Administration Office, Container Yards, Cargo Warehouse, Storage Facilities, and Port Entry Point (Port Gate). The different names assigned to the facilities are sometimes confusing and in some cases their roles tend to overlap. To avoid such confusion and for easy understanding, this study adopts the stand that port operations are divided into the following four categories.

All the port facilities under study are categorised into; 1) port gate (port entry point via road, and train), 2) wharf on sites (which cover wharf, quay, harbour, container terminal, oil/chemical/gas terminal, bulk terminal, passenger terminal), 3) yard on sites[1] or storage facilities (which cover container yard, cargo warehouse), and 4) administrative on sites (which covers repair/maintenance facilities, maritime administration, administration office, security port office, and the fire department) (See Figure: 3.1).



Wharf on Sites   Yard on Sites   Administration Sites   Port Gate

Figure 3.1: An Overview of the Generic Port Facilities

3.1.1 - Port gate

A gate is a point of entry to a certain place, such as a port that is enclosed by walls. It controls the entry or exit of individuals or vehicles through the gap in the wall or fence to prevent unwanted access to a controlled environment (Jonathan, 2014). In a port, gates are used to control the access of outsiders to its facilities by only allowing their workers and customers to enter the port compound (visitors are admitted only by special permission or on request). Gates provide a security barrier to the ports, and they are configured in two ways, namely high-security and low-security. High-security barriers are those that are capable of stopping heavy vehicles from travelling at high speeds in a short distance such as deployable bollards, phalanx barriers, and crash rated barriers. The low-security barriers comprise of simple constructions such as rising arm gates, lift-arm gates, single or double swing gates and sliding gates. Rising and lift-arms gates provide the least security but can be deployed quickly and are usually used in parking lots. Sliding and swing gates provide higher security against vehicles and pedestrians but are slower to deploy (Norman, 2010).

[1] In this instance, for "yard on sites/storage facilities", the study decides to use yard on site rather than storage facilities because in the case of the port under study, about 75% of its business uses containers and the term "container yard" is more familiar and acceptable to the experts rather than "storage facilities".

3.1.2 - Wharf on sites

Wharf is an old English term referring to a port structure which commonly comprises fixed platforms. They can be made from timber, masonry, cement or concrete, built alongside the water, with sufficient depth to allow vessels access to load and unload cargo/containers. In some other places, the term "quay" is commonly used, especially in the United Kingdom, Canada and other Commonwealth countries, while in the United States, wharf is more commonly used. Besides wharf and quay, in some contexts, terms like pier, berth or jetty are also used. Wharf is used for loading and unloading not only containers and bulk cargo but also liquid cargo such as chemicals, oil and gas and human passengers too (from cruise ships).

3.1.3 - Yard on Sites

Yard on Sites often refers to places or areas next to the wharf on sites, and its purpose is to minimise long journeys to and from the loading and unloading processes. In the case of container transhipment, container lorries just need to deposit the containers that are unloaded from the ships at the wharf onto the container yard near the wharf and immediately return to the wharf for the next job. Such short process saves time, fuel, and vessels' berthing time to the benefit of the port operators.

3.1.4 - Administration Sites

Administration on site covers a lot of port facilities, such as the administration office, port security office, and fire department and repair/maintenance facilities. The administration office is responsible for ensuring all the administrative activities within the port run efficiently by providing instructions to employees and parties throughout the port. It also handles recruitment and deployment of workers and vets them (ensuring they have clean records and do not have links or ties to terrorist organisations), and institutes policies for the port. The Port Security Office in turn is responsible for securing the port from any threats by creating a safe and secure environment that encourages good behaviour and vice versa. The port security staff often communicate frequently with the operating and information systems office for the latter's expert advice and assistance, especially for ports that use high-end technologies. A fire department is put in place inside the port area for safety precautions since the port sometimes handles dangerous and hazardous goods, and a huge amount of flammable chemicals and oils. If a fire breaks out, the fire department will be the first to respond and if the fire is too big it takes action to control and put it out. The repair or maintenance facilities are given the responsibility to conduct regular checks on the equipment and repair heavy machinery if there are breakdowns.

3.1.5. Novelty of the Study

There are a lot of studies on port maritime discussing about security that involve around ISPS code which is the most accepted regulation used by all port in the world. The studies analyze the regulation, criticized it and propose a better regulation to counter security risk. But this regulation is not only regulated with mind frame of combating terrorism, it is also for other purposes such as combating thieveries, robberies, piracy, sabotage, strike and combating natural disaster. Such regulation used for multi purposed were excellent since it can cover a lot of aspect of security. However, it can underestimate on terrorist threat since it tried to cover other aspect. In this study, the model development was created only to counter terrorist attack. Therefore, historical data were heavily used in developed this model. From historical data, a list of scenarios was developed that represent all of the historical data. An expert opinion was taken in order to verify the relevant of the scenarios the models.

3.1.6. List of Scenarios

In this study, a few different scenarios were listed based from data given from GTD (Global Terrorist Database). This scenario happens repeatedly from 110 cases of terrorist attack in maritime seaport. From all these cases, four stand out scenarios were listed such as terrorist trying to bomb the port, terrorist trying to ramp the port gate or wharf, terrorist trying to attack using weapons and terrorist attack by disguising themselves and attach them from inside the port.

The first scenario was a suicide attack attempt by using a tampered truck or land vehicles targeting port gates. This was a direct external attack and had high risk since the target is easily approachable by the public. However, as compared to other attacks, the impact and consequences are mild. Port gates do not have high value as compared to other port facilities and usually, a port has more than one gate. However, such attacks can disrupt the flow of goods into and out of the port. If one of the port gates was attacked, people at the port may want to quickly get out and this can cause traffic bottlenecks at other gates. In September 2010 in Somalia, suicide bombers in an explosives-laden truck, tried to drive into a port but they were stopped by the Somali police. The two suicide bombers were injured, but no damage was done to the port (Guled, 2010). If such a scenario was not handled quickly by the security response forces, it would have caused a disaster at the port. It was even possible that second and third trucks were ready to strike (after the first truck started the attack) and, had they been there, they would have been able to infiltrate that port after the gate was destroyed.

In the second scenario, terrorists hijacked a vessel and overcame the security personnel to attack the wharf on site. Hijacking a vessel in the Straits of Malacca was not an easy task. The terrorists had to face the coast guards and marine police from three littoral countries; Malaysia, Indonesia and Singapore (Bradford, 2004). If the terrorists were able to avoid this first obstacle, they still had to face the problem of the straits being narrow and the waterway has different depths (in which inexperienced captains would risk grounding the vessel instead of escaping). However, if the terrorist(s) managed to slip through these two barriers, the impact (of port destruction) and losses would be high.

The third scenario involved the smuggling of tampered containers which contained explosives (Yang, 2006). This may require some internal assistance. A terrorist who posed as a worker inside a port may infiltrate by using two methods, such as a worker coming in as a newcomer and working with the terrorists from the start. The other method was that the terrorists got one of the workers and turned him to their side (via bribes or threats to his life). This complex scheme required long plan and time consuming, but, if the terrorists managed to attack, the impact and losses would be very high.

The fourth scenario was a complex attack, which started with the terrorists or their agents infiltrating the port workers, who then helped a terrorist to disguise as a bona fide visitor – such as a truck driver or a shipping agent - entering the port compound and bringing with him concealed attack weapons. Port workers, who were actually the terrorists, might also give internal help to a group of armed persons to sneak into ports, regroup with the inside cells and commence an attack. Such attack may target administration sites, container yard and wharf. If the terrorists managed to attack the targeted ports by using container bombs and/or attack weapons, the impact and losses would be very high.

3.2 Bayesian Network (BN) and Root Cause Analysis (RCA)

In this technical chapter, the BN approach is adopted wholly with the RCA approach inserted at the beginning of the BN.

3.2.1 Characteristic of BN and Bayes Theorem

BN can do various prediction, diagnosis, and it can model the interdependencies among other factors and once we look at the port security issues, there is a lot of factors having interaction (relationship). BN can model the interdependencies among the root causes while fault tree analysis can't do that, fault tree can only do (either and or). It is either (1,0) probabilities, in fault tree this event can be interpret with either happen or not. But Bayesian network, if this event happened and that event happen, it can happen in a certain degree, that the beauty of Bayesian. Plus, Bayesian can do forward risk analysis and back work risk analysis. If there is any new information, all the other nodes can be update to see, how the situation can change in dynamic way. See BN introduction in section 2.3(F1).

I) Characteristics of BN

Based on the structural level of BN's graph, a probabilistic network model contains nodes that represent variables and the links between nodes, which represent a different kind of relation among the variables. Each variable represents an event, and this event has its state, level, value, options and choice (Kjaerulff & Madsen, 2005). The domain of a variable can be discrete (discrete domains are always finite) or continuous. For example, T is a variable that consists of three states, which are A, B, C, the names of the state are determined by technical information gained from reading materials, expert advice and personal knowledge.

The content of the BN method can be described as a directed acyclic graph (DAG) which contains nodes, arrows/arcs (links between the nodes) and a set of probabilities tables. The nodes (usually drawn as a circle) represent random variables with values, which are usually expressed in numbers and ranges (Wang & Trbojevic, 2007). Directed arrows are links between pairs of nodes representing dependence relationship between the variables. Each relationship is described by an arrow and link, connecting the parent nodes to an influenced child node (the arrowhead will point to the child nodes). A conditional probability table (CPT) on each of the nodes will show the level of dependence relation between the nodes (Rahman, N.A., 2012).

In general, the characteristics of this method contain two items which are nodes and arcs. The nodes can be categorised into four types, which are the parent node (the initial/ independent variables), the child node (dependent variables), the root node (node without parent) and the leaf node (node without children) (see Figure 3.2) (Hansen, 2000). A more complicated model (Figure 3.3) shows that the DAG has 3-tier level, which is R and T as the root nodes, which are also parents to the X node. X is a child node to R and T, and at the same time becomes a parent to the other two nodes, L and C. Finally, L and C are also known as the "leaf nodes" because both of them have no children nodes.

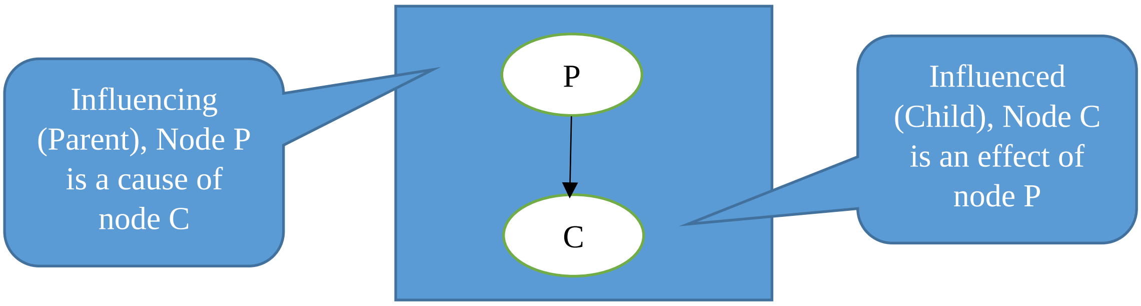

Influencing (Parent), Node P is a cause of node C
P
C
Influenced (Child), Node C is an effect of node P

Figure 3.2: The Simplest BN with Two Basic Nodes (Rahman, 2012)

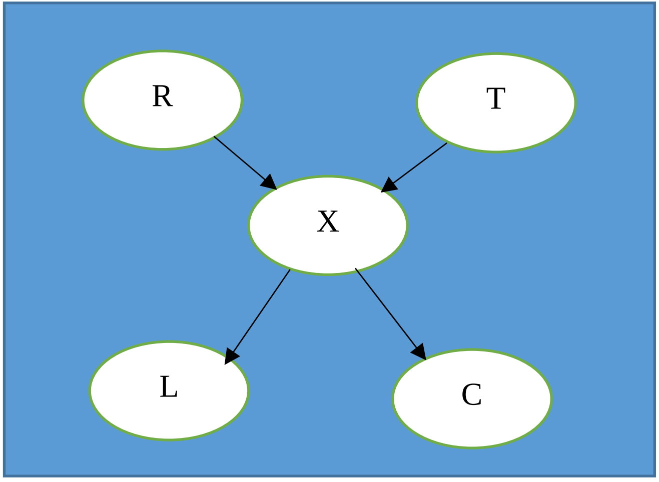


Figure 3.3: A BN Model with 5 Nodes (more than 2 Nodes)

In the BN approach, the data collection process can be conducted by using a qualitative method, a quantitative method or a combination of both. The collected data has to be transferred to a specific value between zero and one (Further explanation will be given in Section 3.3 (Step 5).

The next characteristic is the probability of nodes in the BN, which is defined as a way of conveying knowledge or belief that an event will occur/has occurred. If a node is a leaf node, then its probability distribution is marginal (unconditional), and if a node has a parent then it is conditional (Figure 3.3) (Wang & Trbojevic, 2007). The probability distribution can be categorised into two groups. The first one is prior probability and the second is posterior probability. Prior probability is defined as an event inferred before new information becomes available, while posterior probability event is the conditional probability that is assigned after the new information arrives/is received. Examples of conditional probability are $P(X \mid R, T)$, $P(L \mid X)$ and $P(C \mid X)$ in Figure 3.4. Further discussion will be carried out in Section 3.3 (Step 5(3)).

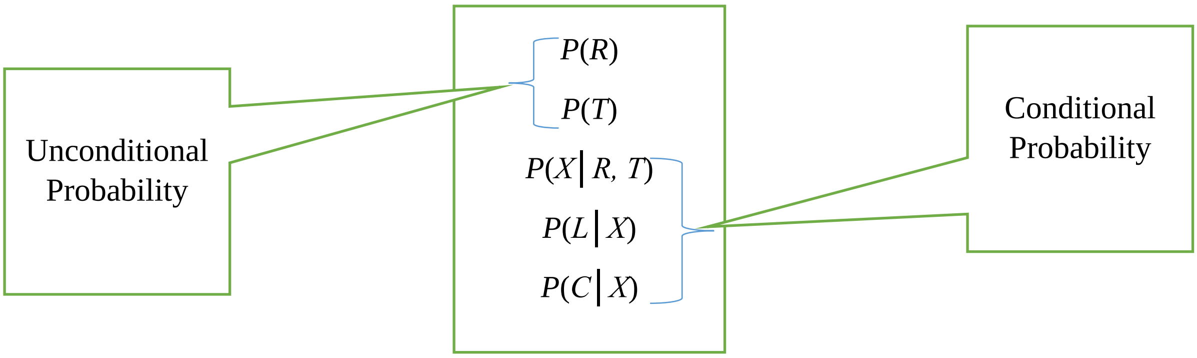


Figure 3.4: An Example of Unconditional Probability and Conditional Probability

II) The Bayes' Theorem

Bayes' Theorem is a mathematical formula used to calculate one of the probability distributions, which are posterior probabilities, and then to measure the rational belief of probabilities. It is followed by the rules of probability and depends heavily on conditional probabilities in the theory of evidence and model. According to Hayes (1998), the Bayes' Theorem is a probability of a parameter value, given the observation is equal to a probability of the observation, given the parameter value multiplied by a prior probability of the parameter value divided by a total probability of the observation (Equation 3.1).

$$\left(\begin{array}{c}\textit{Probability of a}\\ \textit{parameter value}\\ \textit{given the observation}\end{array}\right)=\frac{\left(\begin{array}{c}\textit{Probability of}\\ \textit{the observation}\\ \textit{given the}\\ \textit{parameter value}\end{array}\right)\times\left(\begin{array}{c}\textit{Prior Probability of}\\ \textit{the parameter value}\end{array}\right)}{\textit{Total probability of the observation}} \tag{3.1}$$

The basic rule of probability (also known as the Bayes' Rule) can be put in the equation as follows:

$$P(A\,|\,B)\ =\frac{P(A,B)}{P(B)} \tag{3.2}$$

Which is usually written as:

$$P\ (A,\,B)\ =P\ (A\,|\,B)\ P(B) \tag{3.3}$$

This is in fact, the basic form of the Bayes' Theorem and $P\ (A,\ B)$, is called a joint probability. The Bayes' Rule allows an update to event 'A' given the information about another event 'B'. If the model is a discrete variable, then the definition of Bayes' Theorem can be put into the equation as follows:

$$P(A\,|\,B)\ =\frac{P(B\,|\,A)P(A)}{P(B)} \tag{3.4}$$

Where, the symbol " $|$ " represents "given" or "on the condition of". *P* (*A*) is usually named *prior probability* of 'A' occurring, while *P* ($A|B$) is named *posterior probability* of 'A' occurring given the condition that 'B' has occurred. The probability *P* ($B|A$) is called the *conditional probability* of 'A' occurring given that 'B' occurs too. *P* (*B*) is the marginal probability of 'B' occurring. When there are three events, the Bayes' Rule will follow Equation 3.5, given the names of the three events were Event A, Event B, and Events C (Jensen & Nielsen, 2007):

$$P(A|B,C) = \frac{P(B|A,C)P(A|C)}{P(B|C)} \tag{3.5}$$

The algorithms allow the impact of evidence about one node, enabling the propagation of other nodes in multiple-connected trees, and making BN a reliable engine for probabilistic inference. In Bayes' Theorem multiple-connected trees, the algorithms allow the impact of evidence (for one node) to be connected to other nodes, which means if some new information or data happen to change one node, the other nodes that are connected will also be affected, making BN reliable for a probabilistic inference. For a complete understanding of BN, several journals, articles or books can be used as guides, such as Pearl (1988), Neapolitan (1990, 2004), Oliver and Smith (1990), Charniak (1991), Jensen (2007) and also Korb and Nicholson (2003).

BN has a number of advantages, such as it develops a model that can be updated from time to time in case new information arrives, and determines whether or not to take the new information into consideration. It has intuitive visual representation and is able to conduct an analysis by incorporating qualitative and quantitative data and the output is easy to interpret (Rahman, 2012). This method is expected to produce a valuable result on the risk of the assets in container terminals and the security vulnerability of the port.

3.2.2 RCA Introduction

Root Cause Analysis (RCA) is used for the process of identifying nodes in this study. This approach explains how the attack event could happen to the container terminal due to uncertain conditions while simultaneously looking for a mechanism that could be used to explain about causality (Rooney & Heuvel, 2004). Apart from that, this technique can also be used to define major causes, sub-causes and root causes that influence the risk of a terrorist attack at a container terminal. It is also easy to visualise possible relations among the risks, and forecast which of them may have a higher risk than others.

3.3 Methodology: Use of BN in the Risk Analysis of Terrorist Attack in Ports

BN application is used to identify and prioritise the port facilities risk of being attacked by terrorists. The assessment process is shown in Figure 3.5, which shows the seven steps of assessment, some of which require additional approaches, for example a discussion with selected experts, a mathematical algorithm (for conducting analysis of qualitative and quantitative data), a brainstorming technique (for identifying the states of the evaluation nodes), and a cause and effect analysis technique (for determining the evaluation nodes). All the seven steps in the assessment of identifying and prioritising the port facilities under uncertainties are described as follows:

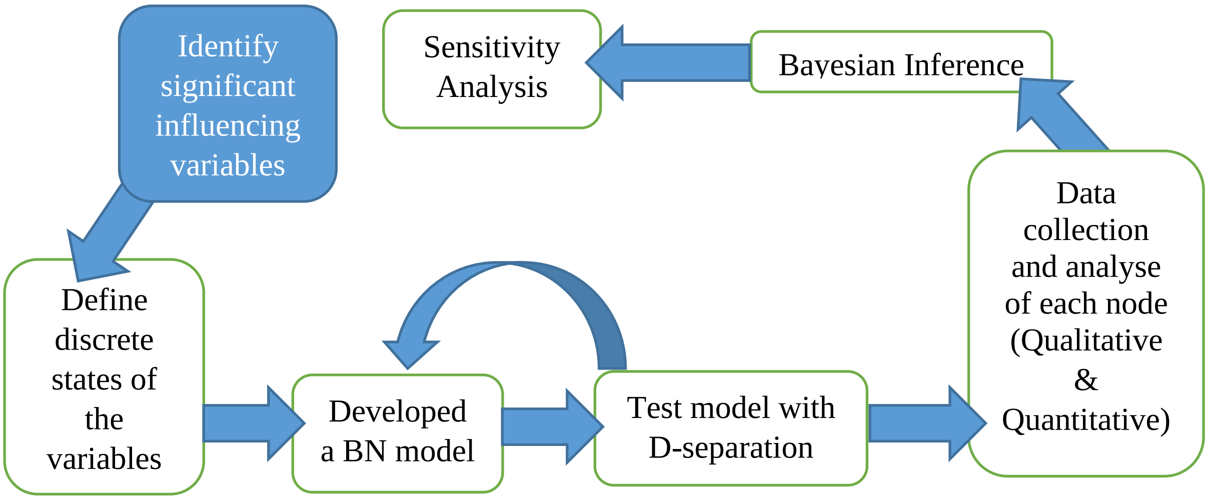

Identify significant influencing variables
Sensitivity Analysis
Bayesian Inference
Data collection and analyse of each node (Qualitative & Quantitative)
Define discrete states of the variables
Developed a BN model
Test model with D-separation

Figure 3.5: The Assessment Procedure of a BN Method

Step 1: Identify Significant Influencing Nodes

A few steps are used in selecting nodes for BN Modelling. Firstly, RCA is used to identifying nodes in this study. The general process of RCA starts with defining the problem, gathering data related to the problem and finding the ‘causes’ at every step of an event listed. The causes are taken to mean "What are the factors that have significant effects on the port facilities’ vulnerabilities?". Then the causes are classified into causal factors that relate to occurrences in the flow of the event and identify all other harmful factors that have equal or better claim to be called "root causes". If there are multiple root causes, those causes must be clearly revealed for later selection. Lastly, the corrective action(s) are identified to prevent recurrence of each harmful event. Apart from that, this technique can also be used to define the major causes, sub-causes and root causes that influence the risk of a terrorist attack at a container terminal. It is also easy to visualise the possible relation between the “most high-risk” risks.

In term of terrorist attack in port facilities, Global Terrorism Database (GTD, 2016) has been used to acquired historical data, this database has an archive of terrorist attack records from the whole world. All their record of terrorist attack cases was pile up in the same places but a few features of engine search provided in this website allows the viewer to limit their search into a specific case. In this case, terrorist attack on maritime were selected from 2001 until 2015 (GTD start to charge their viewer when asking for latest information), but these cases were terrorist attack on port and on vessel attack. After receiving all the data, 110 cases of port maritime were pick up by read each of the attack circumstances (See Figure 3.6 and Appendix 1).

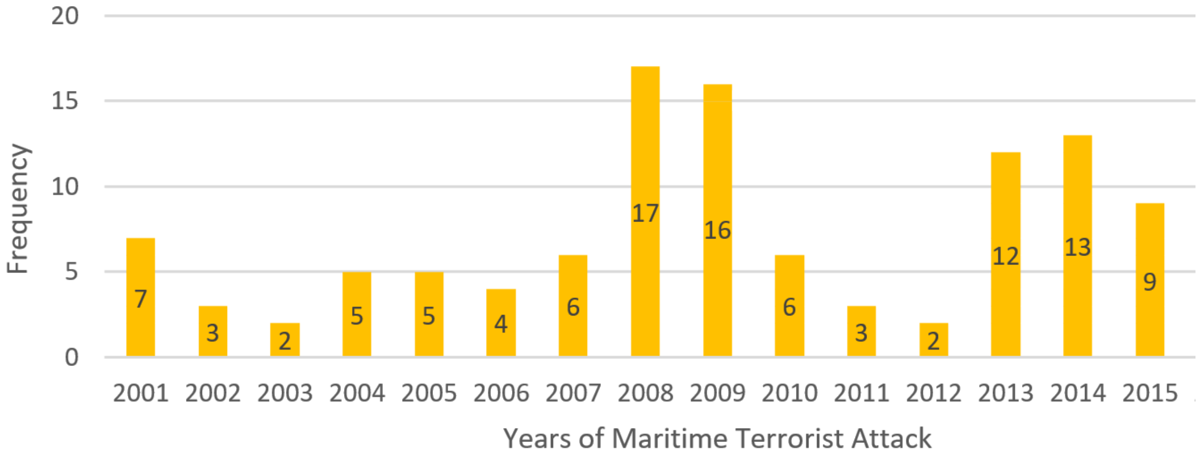


Figure 3.6: Frequency of Maritime Terrorist Attacks on Port Facilities 2001-2015

These events are then dissected in a sequence of events, with these questions asked: "What are the factors that have a significant effect on the port facilities' vulnerabilities?"; "Where were the terrorists' first and second attacks and are the attacks from external or internal?", (possibly the terrorists have inside help), and the possibility of different types of attack, such as explosive, collision or weaponry attack. The nodes that determine the risks of port facilities are identified based on these events. After nodes with a significant effect on the vulnerabilities of port facilities are selected, a model will be developed.

Table 3.1: List of Potential Nodes Selected Explained by Using Case as Example (See 3.1.6)

Potential Nodes	Case(s) of terrorist attack
Using Tempered Trucks	This situation is similar to hijacking a fuel truck; for example, in September 2010 in Somalia, suicide bombers in an explosives-laden truck tried to drive it into a seaport but they were stopped by the Somali police. The two

	suicide bombers were injured, but no damage was caused to the port (Guled, 2010). From these incidents, three nodes have been derived which are using tampered truck, a suicide attempt using the truck and an attack on the port gate.
Overcome the Prevention of Unauthorised Entry	A lot of cases are of vessels being hijacked usually when they (the vessels) are at sea. Since the terrorist's plan to attack the seaport, they need to overcome the security of the vessels first, take control of the vessels and then finally proceed to attack the seaport.
Suicide Collisions by Trucks/Vessels	The number of terrorists who die by killing themselves is very high on land (Santifort-Jordan and Todd 2014). For ports, it is possible to use one bulk vessel fully loaded with dangerous goods for a suicide mission, targeting port facilities. Bulk shipping vessels receive less attention compared to container vessels (Yang, 2006). This approach is similar to the aeroplane hijacked on September 11, 2001. Another possible situation is when criminals place explosives onto the vessel, arming with explosives it and crashing it at port facilities. In April 2004, three small Iraqi boats exploded killing three U.S. soldiers and injuring four more near Basra Oil Terminal. From these incidents, four nodes have been derived which are an attempt to enter the vessel (unauthorised entry), hijack the vessel, a suicide attempt using the vessel and an attack on the seaport wharf.
Using Tampered Containers	Another way to attack a port is by using remote devices and cargo container tampering. Imagine a situation where explosives are placed in a container (container tampering). The container is assumed to be equipped with special signal devices that can be remotely detonated when it (the container) arrives at the desired location (The News, 2008 and Yang, 2006). A similar incidence happened in February 2008, when a terrorist planted a bomb packed in a parcel container at the Tanjung Priok Port in Jakarta, Indonesia. The bomb disposal unit managed to deactivate the bomb, but no group claimed responsibility for the attempted bombing (People Daily, 2008). In another case, a small bomb in a trash bin exploded in Port of Spain but the explosion did not result in casualties and damage. Nobody claimed responsibility for the attack. (BBC Monitoring 2005, GTD 2016). From these incidents, one node has been derived which is an attempt to tamper the container with explosives. Terrorists need inside help from port employees to falsify information regarding the container manifest and to evade routine inspections.
Smuggling Unauthorised Containers (Bombs)	Terrorists may smuggle in weapons such as a bomb, or firearms, and use them to attack a port. On April 2007, unidentified gunmen killed one person and seriously injured another person in a weapon attack on a crew boat operated by ExxonMobil (Rigzone 2007). A similar incidence happened in May 2009, when an unidentified man placed a small plastic container near the ticketing booth of the super ferry line at the Nasipit International Port, the largest seaport in North-eastern Mindanao, Philippines. The authorities managed to detonate it safely. No casualties occurred, and no group claimed responsibility. (Philippine Daily Inquirer, 2009). From these incidences, one node has been derived which is attempt to tamper the container with explosives, attempt to smuggle the container into the port with some inside help, avoid detection during routine inspections, attack using container bomb on either wharf or container yard.

Overcome Identification for Employee	To attack a port, terrorists need to enter the port area, which is quite challenging. Thus, the need for spies and traitors to infiltrate the organisation. This treasonous act succeeds because terrorists use baits such as religious motivation, similar political views and wealth (Eichensehr, 2009). They (spies and traitors) may help external terrorists by introducing weapons (concealed weapons) into port compounds and tampering with documentation, allowing unchecked containers to enter the port. However, becoming an employee in order to conduct an attack as an internal terrorist is difficult and time-consuming. They need to get an interview, be employed as employees, need to overcome the individual security background checks and work in the port for a while to gain the port operator's trust. Only then, they can attack the port from the inside. From these incidences, four nodes have been derived which are terrorist infiltrating the organisation, tampering with the documentation, allowing an unauthorised item such as a weapon into ports, allowing armed attackers overcome the prevention of unauthorised entry, attacking seaport using weapons and terrorists may attack administration sites.
Overcome Identification of Visitors	There is another type of possible attack i.e.by external terrorists disguised as bona fide visitors to the port overpowering the port security outfits. The related node is the terrorist disguised as a visitor with an intention to attack the Port. They claim themselves as truck drivers or shipping agents. Their goal is to enter the port and bring in explosives and weapons with inside help. The terrorists can also be disguised as ship crew or captain to overcome the security outfit. Once they successfully enter a port terminal, the port is highly vulnerable because they can blow themselves up with explosives already loaded on board. A similar incidence happened in Galle, Sri Lanka on 18 October 2006, where terrorists disguised as fishermen attempted a suicide attack using five boats loaded with explosives. However, the navy was able to detect these vessels as a threat to the security check-point. Three of the vessels were neutralised, but the other two vessels exploded at the port entrance (Raman, 2010).

These scenarios started with the potential perpetrator(s) overpowering port security, at which point each node was assigned with two states, i.e., YES (Yes, the perpetrator was able to pass the security) and NO (No, the perpetrator was unable to pass the security). Then, it will show risk probability for each of the four facilities in the port in two "states", i.e. (1-Risky, 2-Safe). In the end, the security level was denoted, also with two "states", (low and high).

From these incidences, the related nodes were terrorist(s) by using tampered truck(s), to cause a collision on targeted Port Gate. The related nodes were terrorists, disguised as visitors with intention to attack the port. Subsequently, seven types of risks were identified and from these, 19 significant nodes were derived for this study. These nodes are given in table 3.2.

Table 3.2: Initial Nodes List

1. Using Tampered Truck(s)
2. Hijack Using Vessel(s)
3. Overcome the Prevention of Unauthorised Entry
4. Suicide Collision by Trucks/Vessels
5. Using Tampered Containers
6. Overcome Identification of Employees
7. Overcome the Prevention of Unauthorised Document Access
8. Smuggling Unauthorised Containers (Bombs)
9. Overcome Routine Security Inspections
10. Container Bomb Attacks
11. Overcome Identification of Visitors
12. Overcome the Prevention of Unauthorised Introduction of Items into Port Facilities
13. Armed Attackers Overcoming the Prevention of Unauthorised Entry
14. Weapon Attacks
15. Port Gates
16. Wharf Operation Sites
17. Yard Operation Sites
18. Administration Sites
19. Security Level

The nodes were derived from previous records of terrorist incidents and accident events (Yang, 2006; Global Terrorism Database, 2014b). These records were based on terrorist attacks on maritime events and incidences from different modes, such as air, road, and sea. After discussions with Six selected experts, 19 nodes were taken as a fundamental idea to develop the BN model, incorporating the risk of terrorist attacks on a container terminal. These 19 nodes were selected through historical data using expert judgement.

A judgement is the act of conducting judgement involve weighing the evidence that available and reaching a balanced conclusion from it. An expert role is to provide these judgements because they have developed the best experience to make a sound evaluation. They have the knowledge on the evidence given and able to weight various evidence and interpret the relative importance of various fact and able to form a realistic view from limited or self-conflicted evidence (Hora, 2009). A selected expert is defined as an individual who has appropriate experience in the maritime security field and particularly has 5 years to 20 years involvement in maritime safety and security aspect.

Step 2: Define Discrete States of the Nodes (events)

In general, a node is indicated in uppercase (X), a state is indicated in lowercase (x); the second state is indicated by lowercase (y), while an event is considered as an outcome of a set of nodes. The purpose of defining the states of the nodes is to assign the prior probabilities by using the brainstorming technique with the expert(s) advice (Yang, 2006). Therefore, two axioms were incorporated to be acceptable under the BN algorithm (Kjærulff & Madsen, 2005):

- For any events, $0 \leq P(X=x) \leq 1$, with $P(X=x) = 1$ if and only if X=x happens with certainty. A probability is a non-negative real number ≤ 1 (less than or equal to 1), and it equals 1 if and only if the event has happened for sure.

- For any two mutually exclusive events X=x and X=y, the probability that either X=x or X=y occurs is $P(X=x \text{ or } X=y) = P(X=x) + P(X=y)$. If two events cannot happen together or simultaneously, then the probability that either one of them happens is equal to the sum of the probabilities of their individual occurrences.

Table 3.3: The Description of the Nodes

Nodes	Definition and the state
Using Tampered Truck (UTT)	UTT is defined as an act of tampering a vehicle such as truck/car/motorcycle to launch an attack using the land route. This act is possibly executed by a suicide terrorist attacker, suggesting a suicide bombing attack might happen around the entry point. For a land vehicle, it is quite difficult since it may be gunned down before it crashes the port gate, or crash the security post (Ahram Online 2013). Then arming it with explosives may be the best way to maximise the casualties (Tribune 2013). Therefore, the state of UTT was (1) Yes, the terrorist succeeds in tampering trucks to attack the port and (2) No, the terrorist fails in tampering the truck to attack the port.
Hijacking Using Vessel (HUV)	HUV is defined as an act of hijacking a vessel to launch an attack using the sea route. This act is executed possibly by a suicide terrorist attacker, suggesting a suicide bombing attack might happen around the wharf area (Raman, 2010). For a vessel, it is possible to attack just by ramming the wharf with the vessel. However, to increase the number of casualties, arming it with explosives may be the best way. Therefore, the state of HUV is (1) Yes, the terrorist succeeds in hijacking the vessel to attack the port and (2) No, the terrorist fails in hijacking the vessel to attack the port.
Overcome the Prevention of Unauthorised Entry (OPUE)	Overcoming the Prevention of Unauthorised Entry (OPUE) – is defined as an act of overcoming the security on the port container terminal and entering the facilities either by force (detected) or stealth (undetected). The security facilities are physical installations such as high fences, gates, security checkpoints, and physical persons such as water security guards (Raman, 2010). Therefore, the state of OPUE is (1) Yes, the terrorist succeeds in surpassing the security installations to enter the wharf and (2) No, the terrorist fails in surpassing the security installations to enter the wharf.
Suicide Collision by Trucks/Vessels (SCBTV)	SCBTV is another form of attack by attacking from outside. The drivers (of trucks or pilots of vessels) attempt to ram the wharf or port gates, sacrificing themselves and in the process cause the maximum damage to the port facilities (Sangam 2013). Therefore, the state of SCBTV is (1) Yes, the terrorist manages to use the tampered trucks/vessels to attack the port and (2) No, the terrorist is unable to use the tampered trucks/vessels to attack the port.

Using Tampered Containers (UTC)	UTC is tampering with the containers by equipping them with explosives or concealed weapons without being detected by the port security office. There are many ways of avoiding detection such as putting the explosives in secret compartments or forging the container seals, but the best way is by getting inside help from among the port workers to oversee all transactions (Yang, 2006). Therefore, the state of UTC is (1) Yes, the terrorist succeeds in tampering the container to attack the port and (2) No, the terrorist fails in tampering the container to attack the port.
Overcome Identification of Employee (OIE)	OIE is defined as an act of infiltrating the container terminal port administration as a worker. There are two possible ways of the infiltration which are either by impersonating a bona fide employee in the port or recruiting an existing employee of the port to assist in the attack plan. An internal worker (terrorist) acts in sabotaging the security by documentation forgery, disabling security surveillance, loosening up of the security in the facilities etc. (Eichensehr, 2009). Therefore, the state of OIE is (1) Yes, the terrorist succeeds in infiltrating the container terminal port administration as a worker and (2) No, the terrorist fails in infiltrating the container terminal port administration as a worker.
Overcome the Prevention of Unauthorised Document Access (OPUDA)	OPUDA is done by internal worker(s) forging the documentation regarding the content of the container without being detected by the security system or officers (Eichensehr, 2009). This node is connected to UTC since it allows the tampered container to enter the port. Therefore the state of OPUDA is (1) Yes, the terrorist succeeds in forging the documentation regarding the content of the container without being detected by the security system or officers and (2) No, the terrorist fails in forging the documentation regarding the content of the container without being detected by the security system or officers.
Smuggling of Unauthorised Containers (SC)	SC is done using forged documentation and information, by which the internal terrorist manages to smuggle in the container undetected (Eichensehr, 2009). Therefore, the state of SC is (1) Yes, the terrorist succeeds in smuggling in the container undetected and (2) No, the terrorist fails in smuggling in the container undetected.
Overcome Routine Security Inspections (ORI)	ORI is an act of a terrorist (such as an internal worker) avoiding detection from the port security officer(s)' routine checks on the container that has been tampered with. Therefore, the state of ORI is (1) Yes, the terrorist succeeds in avoiding detection from the port security officer(s) routine checks, and (2) No, the terrorist fails in avoiding detection from the port security officer(s)' routine checks
Container Bomb (CB)	CB is an attack by an explosion, using a container rigged with bomb(s) for maximum damage. Container bomb may have been used at Wharf on-site or yard on site. Therefore, the state of CB is (1) Yes, the terrorist succeeds in bombing the port and (2) No, the terrorist fails in bombing the port.
Armed Attackers Overcome the Prevention Unauthorised Entry (OPUEArmy)	OPUEArmy – external armies are defined as military forces of terrorist organisations trained in combat and equipped for fighting. These groups may enter the port terminal facilities with inside help. Therefore, the state of OPUEArmy is (1) Yes, the terrorist succeeds in infiltrating the port with inside help (2) No, the terrorist fails in infiltrating the port with inside help.

Overcome Identification of Visitor (OIV)	OIV is defined as an act of infiltrating the container terminal port administration as a visitor. There are many ways to infiltrate the port since ports receive a lot of visitors daily. A terrorist may enter the port disguised as a student on a student trip, or as a businessman, or as a reporter doing an interview etc. External terrorists in disguise can sabotage port facilities, disable security surveillance, loosen up the security procedures in the facilities etc. (Eichensehr, 2009). Therefore, the state of OIV is (1) Yes, the terrorist succeeds in infiltrating the port as a visitor and (2) No, the terrorist fails in infiltrating the port as a visitor.
Overcome the Prevention of Unauthorised Introduction of Items into Port Facilities (OPUIIPF)	OPUIIPF - Internal worker and (or) external person on site enters into port facilities openly. This limits the opportunity for them to carry explosives and big firing artillery compared to other terrorist attackers. This explains why their role was restricted to sabotage, and assisting other attackers. However, if they also want to participate on the day of the attack, they will need to smuggle in concealed weapons for themselves. Therefore, the state of OPUIIPF is (1) Yes, the terrorist succeeds in smuggling in weapons into the port and (2) No, the terrorist fails in smuggling in weapons into the port.
Weapons Attack (WA)	WA - concealed weapons has been regarded as another way of attack besides suicide collision and container bombing. These weapons are possibly used by three different types of attackers (external army, internal worker(s) and external person on sites). Therefore, the state of WA is (1) Yes, the terrorist succeeds in attacking the port using weaponry and (2) No, the terrorist fails to attack the port using weaponry.
Port Gates (PG)	PG has the probability of attacks by suicide attack bombing (see table 3.1). Therefore, the state of PG is (1) the Port Gates are considered Risky and (2) the Port Gates are considered Safe.
Wharf Operation Site (WOS)	WOS - The possible attacks on wharf are in the form of suicide bombings, container bomb attacks and artillery attacks. Therefore, the state of WOS is (1) the Wharf Operation Site is considered Risky and (2) the Wharf Operation Site is considered Safe.
Yard Operation Site (YOS)	The possible attacks on yards come from container bomb attacks and artillery attacks. Therefore, the state of YOS is (1) the Yard Operation Site is considered Risky and (2) the Yard Operation Site is considered Safe.
Administration Site (AS)	The possible attacks on administration sites come in the form of artillery attacks. Therefore, the state of AS is (1) the Administration Site is considered Risky and (2) the Administration Site is considered Safe.
Security Level (SL)	This refers to the Security level of the port in all the four stated facilities. Therefore, the state of SL is (1) the Security Level is considered Low and (2) the Security Level is considered High.

By using the same techniques, as described in Step 1, a simple state definition mechanism was used to determine the state of all nodes in Table 3.4. A node, the 19th, was added to determine the security level for the whole port.

Binary number are extremely simple to implement, where any system that has a “YES” and “NO” or “RISKY” and “SAFE” states can be used to encode data. Binary number is the lowest states possible and It is easy to understand (It is the most effective way to communicate with industry expert). The scenarios given in the terrorist attack assumption were suitable in using two states since it provides a clear understanding whether "YES" the terrorist attack were successful or "NO" the attack were not successful. It is the best way to get an unambiguous result. But this approach does not constrict the possibility for another place to add more state for their nodes (it depends on the location and its scenario).

Table 3.4: The Nodes and Their States

Descriptions of Nodes	Abbreviation	States
1.Using Tampered Truck(s)	UTT	Yes, No
2.Hijacking Using Vessels	HUV	Yes, No
3.Overcome the Prevention of Unauthorised Entry	OPUE	Yes, No
4.Suicide Collision by Trucks/Vessels	SCBTV	Yes, No
5.Using Tampered Containers	UTC	Yes, No
6.Overcome the Identification of Employees	OIE	Yes, No
7.Overcome the Prevention of Unauthorised Document Access	OPUDA	Yes, No
8.Smuggling in of Unauthorised Containers (Bombs)	SC	Yes, No
9.Overcome the Routine Security Inspections	ORI	Yes, No
10.Container Bomb Attacks	CB	Yes, No
11.Overcome the Identification of Visitors	OIV	Yes, No
12.Overcome the Prevention of Unauthorised Introduction of Items in Port Facilities	OPUIIPF	Yes, No
13.Armed Attackers Overcome the Prevention of Unauthorised Entry	OPUEArmy	Yes, No
14.Weapons Attack	WA	Yes, No
15.Port Gates	PG	Risk, Safe
16.Wharf Operation Site	WOS	Risk, Safe
17.Yard Operation Site	YOS	Risk, Safe
18.Administration Site	AS	Risk, Safe
19.Security Level	SL	Low, High

Step 3: Developing a BN Model

After identifying the nodes and their states, the next step was to confirm the relations between them and construct a qualitative network to represent all the nodes and their dependencies. The knowledge about understanding various dependencies was then used to construct the causal structure of the risk of terrorists attacking container port facilities (Rahman, N.A., 2012). The graphical representation permits a direct expression of the fundamental qualitative relationships. Figure 3.7 is an initial BN model that represents the risk of a port facilities attack by terrorists.

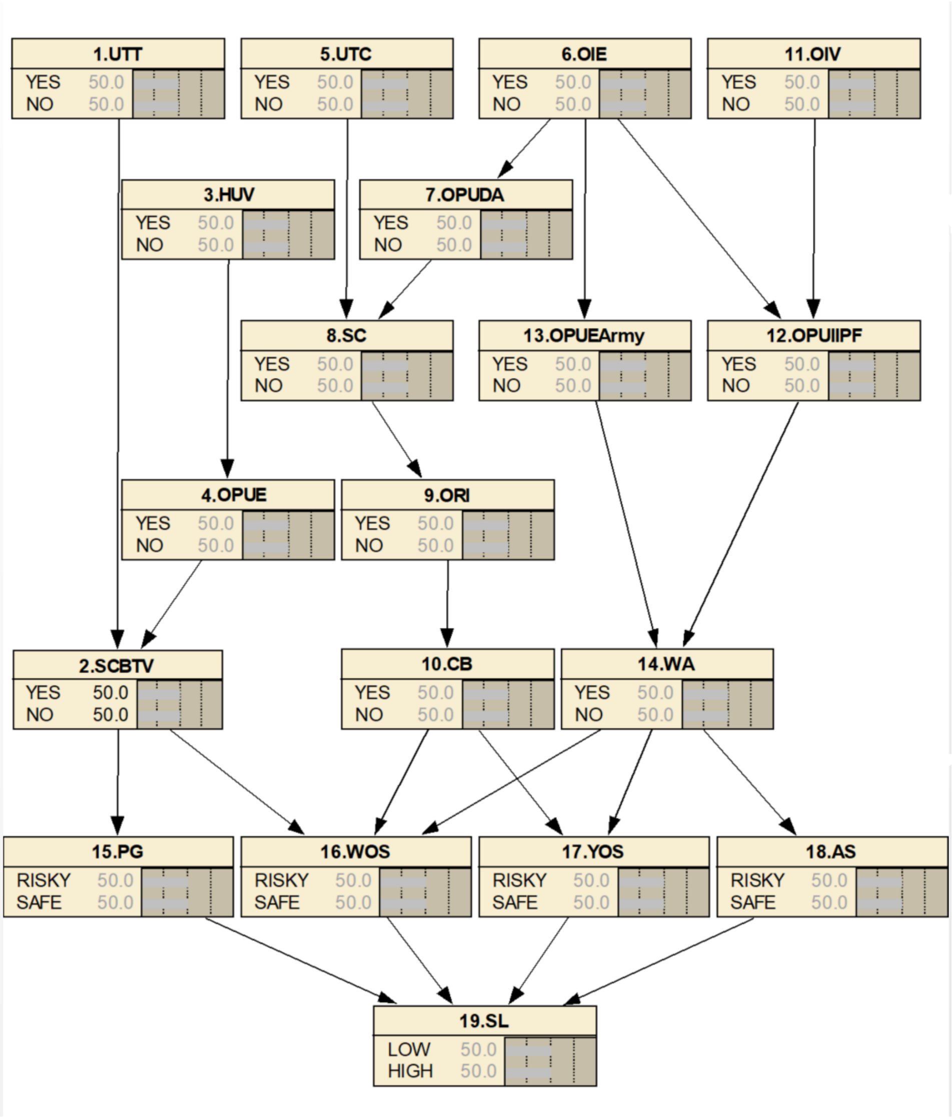


Figure 3.7: The Original BN Model the Risk of Port Facilities Attack by Terrorist

Top-down and bottom-up approaches were used in developing the model in Figure 3.7, where it is defined as an approach that begins at the high level then works downwards to the place of attack. For example, the node “Suicide Collision by Truck/Vessel (SCBTV)” was influenced by nodes “Using Tempered Truck(s) (UTT)”, and “Vessel Hijackers Overcome the Prevention of Unauthorised Entry (OPUE)” nodes (See Figure 3.8). The suicide collision had a dependent relation with both of the parent nodes. The difference between both nodes was that one of the nodes referred to attacks from the land and sea. Some parts of this model are further discussed in Step 4.

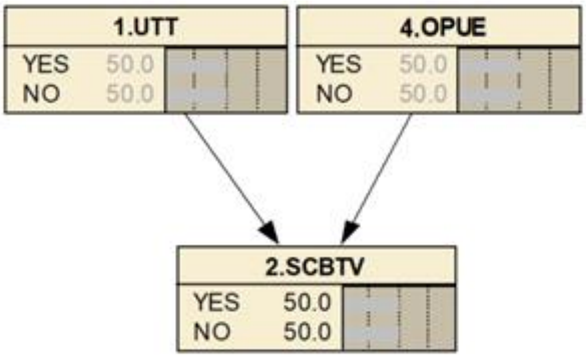


Figure 3.8: Sample of Nodes from BN Model Representing the Risk to a Container Terminal from Terrorist Attack

Step 4: Check and Modify the Model by Using a D-Separation Technique

The Bayes net assumption says:

"Each variable is conditionally independent of its non-descendants, given its parents. (Massachusetts Institute of Technology, 2015)"

There are three different types of connection, as follows:

- Serial Connection (head-to-tail) X ⇨ Z ⇨ Y

X had an influence on Z, and Z had an influence on Y. The evidence about Y will influence the certainty of X through Z and if the state of Z is known, then the channel is blocked (X and Y become independent); in other words, X and Y are d-separated given Z.

- Diverging Connection (tail-to-tail) X ⇦ Z ⇨ Y

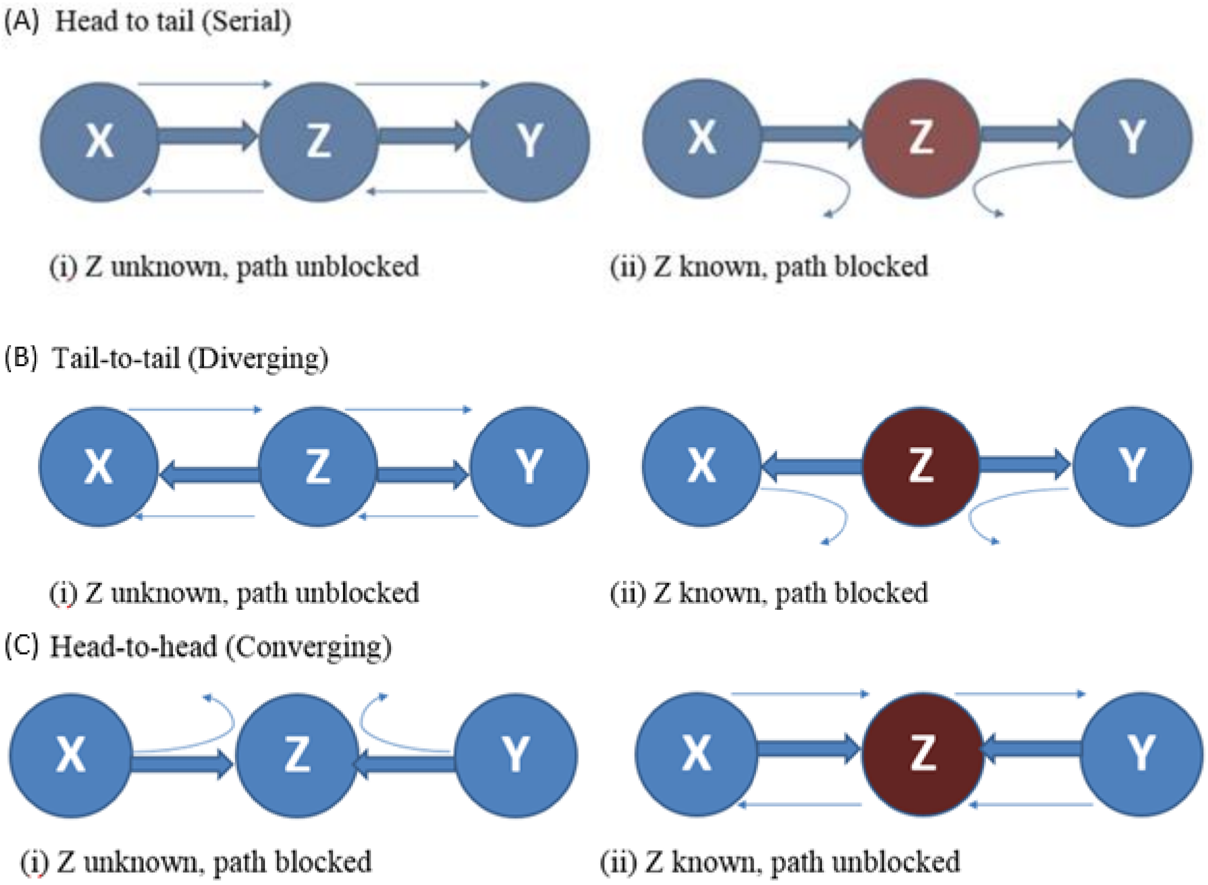
X and Y was influenced by Z, therefore, that is evidence that both X and Y are dependent. However, if the state of Z is known (observed), then the channel is blocked (X and Y become independent); in other words, X and Y are d-separated given Z.

- Converging Connection (head-to-head) X ⇨ Z ⇦ Y

X and Y had an influence on Z, therefore, that is evidence that both X and Y are independent. However, if the state of Z is known (observed), then the channel is unblocked (X and Y become dependent).

BNs encode the dependencies and independencies between nodes and each node in a BN is independent of its ancestors given the values of its parents (Rahman, N.A., 2012). Therefore, Pearl (1986) proposed a concept of d-separation. The definition of d-separation is two sets of nodes X and Y, are d-separated in a BN by a third set, Z (excluding X and Y), if and only if every path between X and Y is "blocked", where the term "blocked" means that there is a middle node, Z (distinct from X and Y). To learn more about how to read such statements from a *DAG*, it is convenient to consider each possible basic kind of connection in a *DAG*. A detailed explanation can be found in literature, such as Jensen and Nielsen (2007).

Based on these three kinds of connections (See Figure 3.9), where the red nodes represent the ones with information/known), if the information is given to the middle node, the flow of information will be closed for the serial and diverging connections. Otherwise, both of them allow the flow of information. In the converging connection, the flow of information will be closed if no information is given to the middle node of the connection; otherwise, it allows the flow of information.


(A) Head to tail (Serial)

(i) Z unknown, path unblocked

(ii) Z known, path blocked

(B) Tail-to-tail (Diverging)

(i) Z unknown, path unblocked

(ii) Z known, path blocked

(C) Head-to-head (Converging)

(i) Z unknown, path blocked

(ii) Z known, path unblocked

Figure 3.9: Ball Bayes Algorithm

For example, Figure 3.10 shows a model for the relations between rain (no rain, light drop, medium rain, heavy rain), water levels (low level, medium level, high level), and Flooding (yes, no). If the water level was not observed, then knowing that the flood was Yes, it is natural to assume that the water level was high, which in turn will be related to the rainfall. On the other hand, if the water level was observed, then knowing that there had been flooding, will not inform anything new about the rainfall.

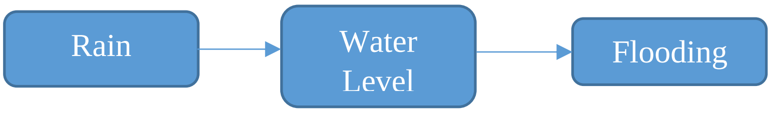


Figure 3.10: A Causal Model for Rain, Water Level, and Flooding

D-separation can be verified by using the “Bayes Ball” concept, which it was designed to compute the relevant part of a BN given a query and information (Shachter, 1998). The main idea is to pass the Bayes Ball (normally starts with the observed nodes) to nodes in the DAG in different ways. Then, it may bounce back, be blocked, and/or pass through, depending on whether the node is dependent on its parents, and on the direction from which it came.

The “Bayes Ball” algorithm is defined as follows: firstly, consider the serial and diverging connections in the BN as in the first and second rows of Figure 3.10. If Z is informed (known), all balls cannot get through, which indicates that X and Y become conditionally independent. In the converging connections, two arrows from the Node X and Node Y point to Node Z. If Z is unknown, then X and Y are conditionally independent and hence the ball does not pass through, which is indicated by the curved arrows. By applying the essential d-separation concept described in Step 4, it is possible to investigate every single node from root to leaf stages of the model. To demonstrate the practical usage of the concept in checking the accuracy of the network in this methodology, each node with its link in Figure 3.7 will be checked with care. However, a few problems were discovered from the model. The explanation of the problems and their corrections are stated in the paragraph below.

Assuming under the converging head-to-head nodes, UTT and OPUE are the parent nodes influencing the event SCBTV child node. SCBTV then acts as a parent node influencing PG and WOS (Figure 3.11). Now, the d-separation concept is used to verify the network model. The relation between UTT and OPUE is first investigated. Suicide attacker(s) used a tampered vehicle and the attack was at the port gate from land. Another suicide attack was from the sea by hijacking a vessel and then there was an attempt to attack the wharf by a collision.

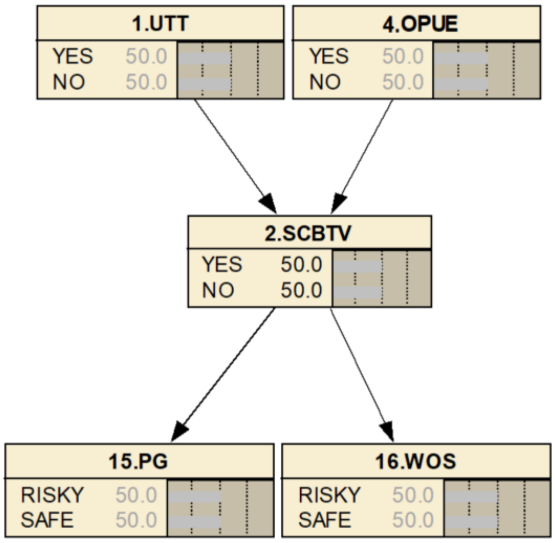


Figure 3.11: Partial Diagram of the BN Model Representing the Risk of Port Facilities Attack by Terrorist [2]

However, there was a problem when investigating the relation between UTT and WOS because UTT did not influence WOS through SCBTV. WOS was influenced from OPUE after SCBTV node. Therefore, SCBTV nodes must be separated into two different individual nodes: one specified for UTT, and another will be assigned to OPUE. This corrective measure changed from ["converging nodes" to "diverging nodes"] to "parallel serial nodes" (see Figure 3.12). Such measure was carried out for the complete BN, and the accuracy of the model is acknowledged.

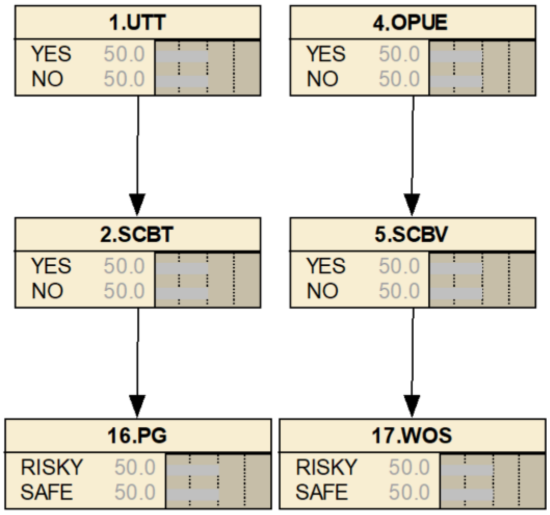


Figure 3.12: Partial of the BN Model Representing the Risk of Port Facilities Attack by Terrorist after Modification

[2] The diagram and model of Netica shows a grey number in it and this represent it is an empty node (No information was inserted yet). Thus, the number were automatically put in number 50:50).

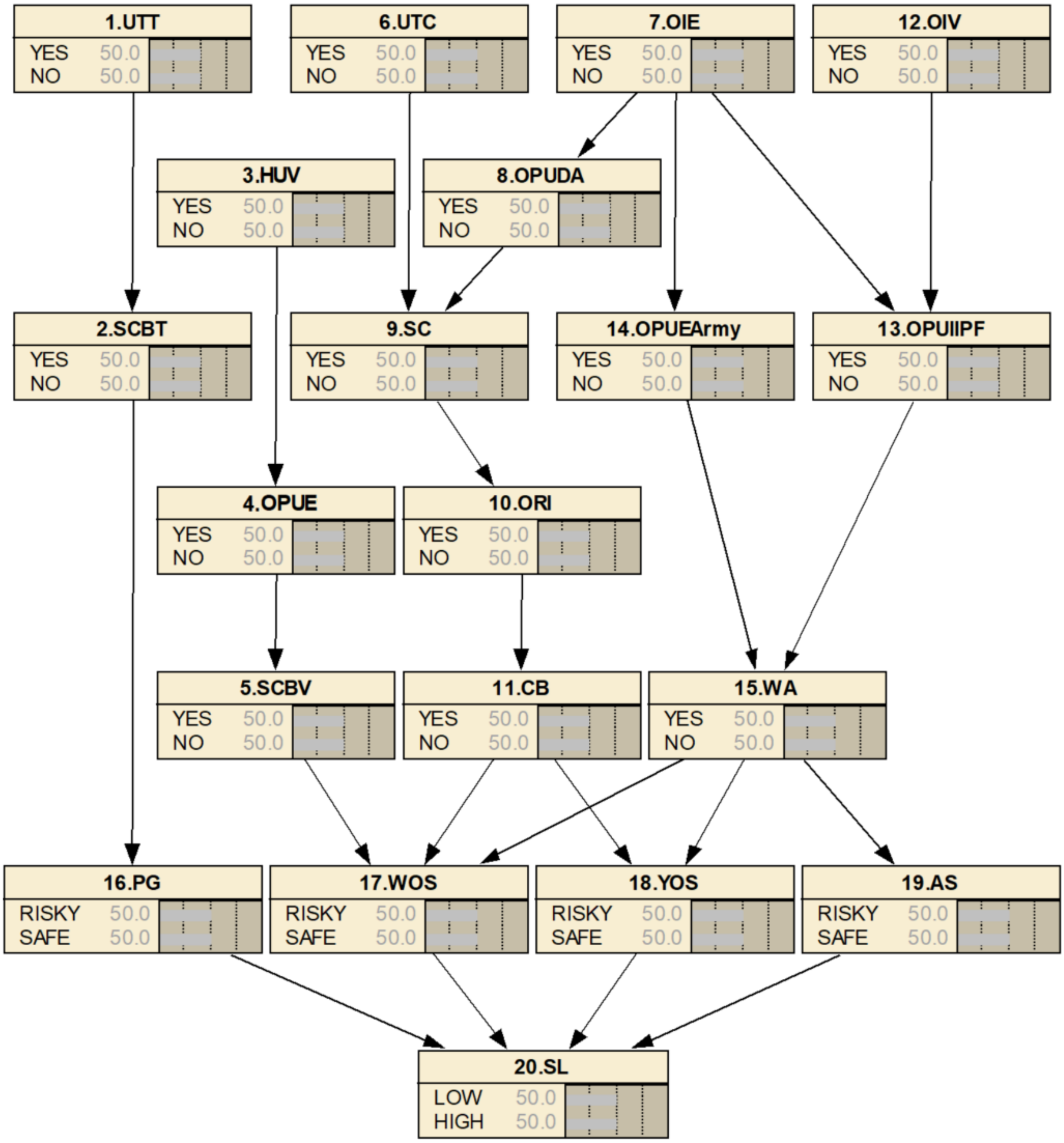


Figure 3.13: The New BN Model Representing the Risk of Port Facilities Attack by Terrorist

Step 5: Data Collection and Analysis of Each Node

There are two types of data used in this model, namely quantitative and qualitative data. Quantitative data can be obtained from several reliable sources, such as the global terrorism database which provide the historical data regarding previous terrorist attack on maritime section (See Step 1: Identify Significant Influencing Nodes). Quantitative data are used in prior data collection involved in developing the model. Qualitative data was gathered through interview sessions and a set of questionnaires. The collection of the qualitative data requires personal views, experience and knowledge from an expert to give a pertinent judgement on certain issues (See Step 1: Identifying Significant Influencing Nodes). In this study, six expert were selected as respondent).

1- Collecting Data under Assumption

From previous risk assessments on terrorist attacks, a lot of researchers argued that it was impossible to predict the probability of terrorist attitude towards port container terminals. Terrorist groups or organisations have members who are intelligent, robust and flexible which makes it quite impossible to gauge their movements (Ezell, 2010). Brown (2011) mentioned that terrorists did not act randomly, in fact they sought information and exploited weaknesses in defences to increase the impact of attacks. Empirical research also confirmed the inability of most experts to accurately predict other countries' political actions and combatants (Tetlock, 2010). Incorporating expert judgements into PRA assessments of terrorism risks was never established as an empirically valid method for predicting these risks (Brown, 2011). Therefore, to make sure of a consistent feedback from different experts, an assumption was made that the terrorists have already set their target on the port to attack.

A justification for setting up the condition was to make sure there will be no huge difference in the results received from different experts. For example, Expert A thinks the terrorist will attack with 20% probability, while another expert (Expert B) has a different opinion that the terrorist will attack with 80% probability. Those differences in expressed probabilities of the terrorist attack on a container port terminal may create a different outcome in determining the risk of the port. Since the data were collected under an impression of imminent attacks, it was expected that they may indicate a high risk rather than a low risk.

2- Qualitative data calculation

There were 20 qualitative data sets that were gathered through the interview sessions and a set of questionnaires (Appendix 2). These data sets were obtained from the selected experts who were originally from the shipping backgrounds. Table 3.5 illustrates the range of probability levels that would give an idea to the experts to provide their judgement according to the situation(s) given in the questionnaire. Basically, this probability rate was divided into two parts which were 1) highly likely (right-hand side) and 2) highly unlikely (left-hand side). This guide started from 50 as a middle value to differentiate the probability rate between the right and left-hand sides. However, the determination of what term should be used to express both sides was dependent on the state name for each node (Rahman, 2012).

Table 3.5: The Transformation Process from the Probability Rate to the Probability Value

00 Highly unlikely	10	20	30	40	50	60	70	80	90	100 Highly likely

All feedback received from the experts was transformed into a probability value (ranging from 0 and 1). ‘50 rating’ is a middle value that can be translated as ‘0.50 (highly unlikely) + 0.50 (highly likely)’ of the probability value, while the probability rating from ‘100 to 00’ on both right-hand to left-hand sides can be transformed to the probability value as ‘highly likely to highly unlikely’ (as shown in Table 3.6). The total probability value of each node must be summed up to 1.0, for instance 0.43 (highly unlikely) + 0.57 (highly likely) = 1.0. Table 3.6 illustrates the basic foundations of the probability rate applied in this study.

Table 3.6: The Basic Foundations of the Probability Rate Applied

Probability Rate	Probability Value for Highly Unlikely	Probability Rate	Probability Value for Highly Likely
00	0.0	50	0.5
10	0.1	60	0.6
20	0.2	70	0.7
30	0.3	80	0.8
40	0.4	90	0.9
50	0.5	100	1.0

Due to the number of experts is six (more than 1), an average probability value for every single state of each node has to be calculated by using the following equation:

Equation 3.6

$$\begin{pmatrix} Average \\ probability\ value \\ for\ a\ state \end{pmatrix} = \frac{\begin{pmatrix} Total\ Probability\ rate\ given\ by \\ expert\ for\ the\ same\ state/event \end{pmatrix}}{Total\ total\ number\ of\ expert} \qquad (3.6)$$

As an example, the node “CB” will be used to demonstrate how this formula functions. This node has two states “YES” and “NO”. If “ORI=YES”, the selected experts have to provide their judgment on the probability rate of the node “CB”. The experts A, B, C, D, E and F wrote five different numbers (between 100 – 50 for example 70) on the right-hand side of a probability rate (Table 3.7). Thus, this probability rate can be transformed into 0.7 of the probability values for the state “YES” and automatically the probability value of the state “NO” is (1.0 – 0.7) = 0.30. The average probability value can be computed by using Equation 3.6 for each state. For example, if “ORI=YES”, the average probability value of the state “YES” for the node “CB” is equal to 0.8 [(0.75+0.80+0.83+0.79+0.85+0.78) ÷ 6 = 0.8], while the average probability value of the state “NO” is equal to 0.2 [(0.25+0.20+0.17+0.21+0.15+0.22) ÷ 6 =

0.2]. Table 3.8 shows the average probability values of the node “CB”, given by the selected experts. This calculation technique was applied to all the qualitative data in order to obtain the average probability values for each node.

Table 3.7: The Definition of the Fundamental Concept of the Probability Rate and Probability Value

0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
→										
00	10	20	30	40	50	60	70	80	90	100 Succeeded on attack

Table 3.8: The Average Probability Values of the Node “CB”

	ORI=YES		ORI=NO	
	YES	NO	YES	NO
EXPERT 1	75	25	0	100
EXPERT 2	80	20	0	100
EXPERT 3	83	17	0	100
EXPERT 4	79	21	0	100
EXPERT 5	85	15	0	100
EXPERT 6	78	22	0	100
AVERAGE	80	20	0	100

3- Results from the interviews and questionnaires

Six experts (from port security and maritime departments) were undertook to a survey. Below are the results acquired from their answers to the questionnaires distributed to them.

Table 3.9: The UCPT Data Collected from Expert Judgement on Given Nodes

Nodes	P(+)	N(-)
UTT	44.7	55.3
OPUE1	32.7	67.3
UTC	80.3	19.7
OIE	80.0	20.0
OIV	83.0	17.0

Table 3.10: The CPT Data Collected from Expert Judgement on Given Nodes

Nodes		P(+)	N(-)
SCBT	UTT	Yes	No
	Yes	71.67	28.33
	No	0.00	100.00
HUV	OPUE1	Yes	No
	Yes	43.33	56.67
	No	0.00	100.00
SCBV	HUV	Yes	No

			Yes	73.00	27.00
			No	0.00	100.00
OPUDA			OIE	Yes	No
			Yes	66.00	34.00
			No	0.00	100.00
OPUEARMY			OIE	Yes	No
			Yes	72.67	27.33
			No	32.67	67.33
SC		UTC	OPUDA	Yes	No
		Yes	Yes	58.33	41.67
			No	38.33	61.67
		No	Yes	65.67	34.33
			No	0.00	100.00
OPUIIPF		OIV	OIE	Yes	No
		Yes	Yes	70.67	29.33
			No	44.67	55.33
		No	Yes	32.00	68.00
			No	0.00	100.00
WA		OPUEARMY	OPUIIPF	Yes	No
		Yes	Yes	79.67	20.33
			No	47.00	53.00
		No	Yes	34.00	66.00
			No	0.00	100.00
ORI			SC	Yes	No
			Yes	55.67	44.33
			No	0.00	100.00
CB			ORI	Yes	No
			Yes	80.00	20.00
			No	0.00	100.00
Port Gate			SCBT	Risk	Safety
			Yes	76.00	24.00
			No	0.00	100.00
Yard Operation Site		CB	WA	Risk	Safety
		Yes	Yes	70.00	30.00
			No	66.00	34.00
		No	Yes	55.00	45.00
			No	0.00	100.00
Wharf Operation Site	SCBV	CB	WA	Risk	Safety
	Yes	Yes	Yes	66.00	34.00
			No	53.00	47.00
		No	Yes	56.33	43.67
			No	54.00	46.00
	No	Yes	Yes	72.67	27.33
			No	65.33	34.67
		No	Yes	61.33	38.67
			No	0.00	100.00

Administration Site	CW	Risk	Safety
	Yes	62.33	37.67
	No	0.00	100.00

The data were then inserted in the Bayesian model created by using NETICA and then the result was generated. Figure 3.14 shows the results acquired by using NETICA.

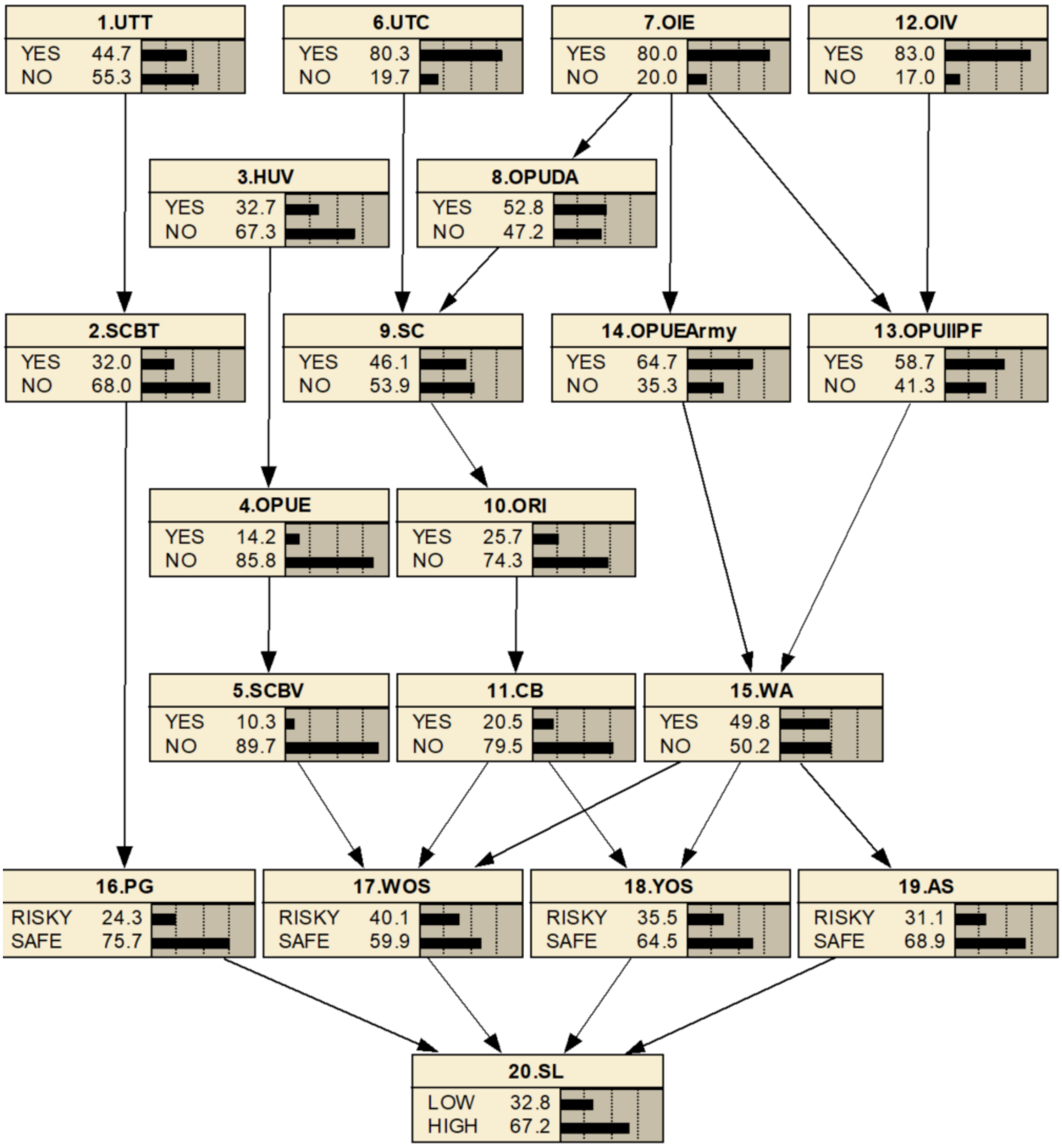


Figure 3.14: The Result of NETICA after Generating the New BN Model Representing the Risk of Port Facilities Attack by Terrorist

4- Unconditional Probability

Five Unconditional Probabilities Tables (UCPTs) collected from the selected experts are presented in Table 3.11. The first UCPT is for the UTT with probabilities of successful attack on Container Port Terminal at 44.7% and unsuccessful attacks at 55.3%. The second UCPT is for the HUV with probabilities of successful attacks on Container Port Terminal at

32.7% and unsuccessful attack at 67.3%. The third UCPT is for the UTC with probabilities of successful attack on Container Port Terminal at 80.3% and unsuccessful attack at 19.7%, while the fourth UCPT which is for OIE with probabilities of successful attack on Container Port Terminal at 80% and unsuccessful attack at 20%. Lastly, the fifth UCPT is for the OIV with probabilities of successful attack on Container Port Terminal at 83% and unsuccessful attack at 17%.

Table 3.11 UCPT of Using Tampered Truck(S), Overcome the Prevention Unauthorised Entry, Using Tampered Container, Overcome the Identification of Employees and Overcome the Identification of Visitors

Five Unconditional Probabilities Tables (UCPTs)			
1	UTT	State	Probability
		Yes	44.7
		No	55.3
2	HUV	State	Probability
		Yes	32.7
		No	67.3
3	UTC	State	Probability
		Yes	80.3
		No	19.7
4	OIE	State	Probability
		Yes	80.0
		No	20.0
5	OIV	State	Probability
		Yes	83.0
		No	17.0

5- Conditional Probability

19 Conditional Probabilities Tables (CPT) are presented in Table 3.12. These CPTs were divided into three groups viz. the methods of attack, the targeted sites and the level of security.

Table 3.12: The First CPT Group (Sequence of Terrorist Attacks)

The first CPT Group - Sequence of terrorist attacks				
1	SCBT	UTT	Yes	No
		Yes	71.67	28.33
		No	0.00	100.00
2	OPUE	HUV	Yes	No
		Yes	43.33	56.67
		No	0.00	100.00
3	SCBV	OPUE	Yes	No

			Yes	73.00	27.00
			No	0.00	100.00
4	OPUDA		OIE	Yes	No
			Yes	66.00	34.00
			No	0.00	100.00
5	OPUEARMY		OIE	Yes	No
			Yes	72.67	27.33
			No	32.67	67.33
6	SC	UTC	OPUDA	Yes	No
		Yes	Yes	58.33	41.67
			No	38.33	61.67
		No	Yes	65.67	34.33
			No	0.00	100.00
7	OPUIIPF	OIV	OIE	Yes	No
		Yes	Yes	70.67	29.33
			No	44.67	55.33
		No	Yes	32.00	68.00
			No	0.00	100.00
8	WA	OPUEARMY	OPUIIPF	Yes	No
		Yes	Yes	79.67	20.33
			No	47.00	53.00
		No	Yes	34.00	66.00
			No	0.00	100.00
9	ORI		SC	Yes	No
			Yes	55.67	44.33
			No	0.00	100.00
10	CB		ORI	Yes	No
			Yes	80.00	20.00
			No	0.00	100.00

The Second group of CPTs were for targeted sites, where the states were different (risk and safety). From here, which facilities on the port were more at risk as compared to the others could be determined.

Table 3.13: CPT of the Targeted Sites

Port Gates			SCBT	Risk	Safety
			Yes	76.00	24.00
			No	0.00	100.00
Yard Operation Sites		CB	WA	Risk	Safety
		Yes	Yes	70.00	30.00
			No	66.00	34.00
		No	Yes	55.00	45.00
			No	0.00	100.00
Wharf Operation Sites	SCBV	CB	WA	Risk	Safety
	Yes	Yes	Yes	66.00	34.00
			No	53.00	47.00

		No	Yes	56.33	43.67
			No	54.00	46.00
	No	Yes	Yes	72.67	27.33
			No	65.33	34.67
		No	Yes	61.33	38.67
			No	0.00	100.00
Administration Sites			CW	Risk	Safety
			Yes	62.33	37.67
			No	0.00	100.00

The third group of CPTs refers to the security level, where the different given states were "Low Security" and "High Security". From here, it could determine whether the port security was good or not.

Table 3.14: CPT of Security Level

Security Level	PG	WOS	YOS	AS	Low	High
	Yes	Yes	Yes	Yes	100.00	0.00
				No	75.00	25.00
			No	Yes	75.00	25.00
				No	50.00	50.00
		No	Yes	Yes	75.00	25.00
				No	50.00	50.00
			No	Yes	50.00	50.00
				No	25.00	75.00
	No	Yes	Yes	Yes	75.00	25.00
				No	50.00	50.00
			No	Yes	50.00	50.00
				No	25.00	75.00
		No	Yes	Yes	50.00	50.00
				No	25.00	75.00
			No	Yes	25.00	75.00
				No	0.00	100.00

6- Validation

If the model is sound and its reasoning logical, the results from the model must at least follow the following two axioms (Rahman, 2012):

Axiom 1. A slight increment in the degrees of belief that an attack will happen should certainly result in the effect of a relative increment in the degrees of belief of the Risk of facilities being attacked.

Axiom 2. The total influence magnitudes of the combination of the probability variations from x attributes (evidence) on the values should be always greater than the one from the set of $x - y$ ($y \in x$) attributes (sub-evidence).

If these axioms are met, it is concluded that the developed models are reliable and acceptable to be used for the case study (see Step 6: Bayesian Inference).

Step 6: Bayesian Inference

Bayesian inference is a method of statistical inference in which the Bayes' Theorem was used to calculate how belief in a proposition changes due to evidence. In Bayesian inference, a probability value of each state of the corresponding node is represented in two ways: a prior probability distribution and a posterior probability distribution. A prior probability distribution is an initial value that is assigned through data records given by the selected experts. By using the prior probability, a posterior probability can be calculated after giving evidence of the selected state. It is called updated probability. The probability of each value will be calculated by using the NETICA software tool.

In respect of the data collected, the Weapons Attack (WA) nodes in Figure 3.15 is examined.

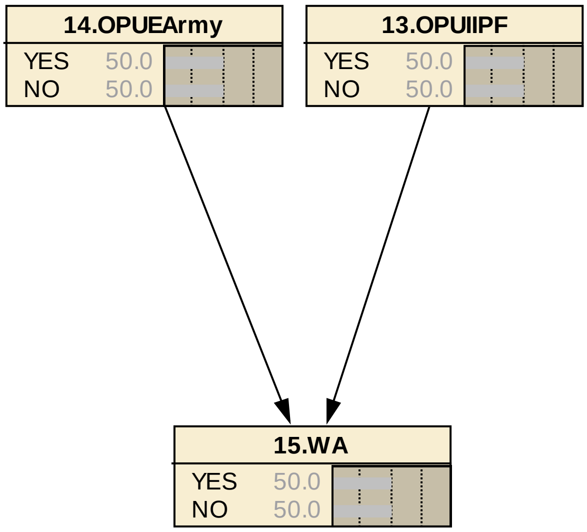


Figure 3.15: A Partial BN Model for Weapons Attack (WA), OPUEARMY and Overcome the Prevention of Unauthorised Introduction of Items in the Port Facilities (OPUIIPF)

OPUEARMY (Conditional Probability)

Yes	0.7267
No	0.2733

For example, P (OPUEARMY - Yes) =0.7267

OPUIIPF (Conditional Probability)

Yes	0.7067
No	0.2933

For example, P (OPUIIPF - Yes) =0.7067

By using the conditional probability values given in the CPT for each node, the prior probability values can be obtained.

WA (Conditional Probability)

	OPUEARMY	Yes		No	
	OPUIIPF	Yes	No	Yes	No
WA	Yes	0.7967	0.47	0.34	0.00
	No	0.2033	0.53	0.66	1.00

For example, the prior probability value of the node "Concealed Weapons: Yes" is calculated as follows:

P (WA-YES) = ∑P (OPUEARMY-YES, OPUEARMY-NO, OPUIIPF-YES, OPUIIPF-NO) (3.7)

P (WA-YES) = (0.7967 × OPUEARMY-YES × OPUIIPF-YES) + (0.47 × OPUEARMY-YES × OPUIIPF-NO) + (0.34 × OPUEARMY-NO × OPUIIPF-YES) + (0 × OPUEARMY-NO × OPUIIPF-NO)

P (WA-YES) = (0.7967×0.7267×0.7067) + (0.47×0.7267×0.2933) + (0.34×0.2733×0.7067) + (0×0.2733×0.2933)

P (WA-YES) =0.574996667

The same result obtained from Netica = Concealed Weapon YES=0.575 thus 0.575≈0.574996667

The probability value of the node "Concealed Weapons-Yes Successful" is known to be 0.575 while the one for "Concealed Weapons-No and Unsuccessful" is 1.000- 0.575=0.425. Such values can also be calculated using the Netica software tool, as shown in Figure 3.16.

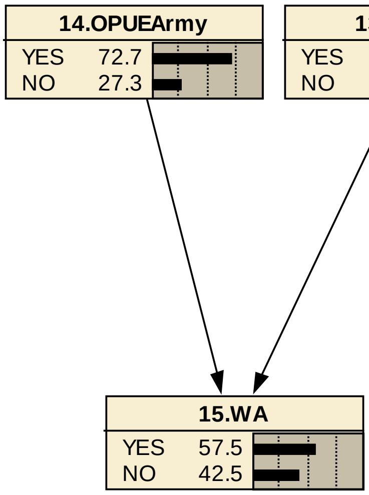


Figure 3.16: A Partial BN Model for Concealed Weapons (WA), Overcome the Prevention of Unauthorised Entry 3 and Overcome the Prevention of Unauthorised Introduction of Items in the Port Facilities (OPUIIPF)

The process of computing the prior probability value of node WA is called pre-posterior analysis. To continue, a piece of evidence is entered to the node "*OPUEARMY absolute NO*" with the purpose of determining the updated posterior probability values of the node "Concealed Weapons". The posterior probability value of the node "*WA-NO*" given "*OPUEARMY absolute NO*" is computed using Equation 3.8.

1.OPUEARMY absolute NO (With Conditional Probability)

Yes	0.0
No	1.0

2.OPUIIPF (Conditional Probability)

Yes	0.7067
No	0.2933

For example, P (OPUIIPF - Yes) =0.587

3.WA (Conditional Probability)

OPUEARMY	Yes		No	
OPUIIPF	Yes	No	Yes	No
Yes	0.7967	0.47	0.34	0.00
No	0.2033	0.53	0.66	1.00

$$\mathrm{P\ (WA - NO \,|\, OPUEARMY\ absolute\ NO)} = \frac{\mathrm{P\ (OPUEARMY{-}NO,WA{-}NO)}}{\mathrm{P\ (OPUEARMY{-}NO)}} \tag{3.8}$$

$$\mathrm{P\ (WA - NO \,|\, OPUEARMY\ absolute\ NO)} = \frac{\sum \mathrm{P\ (OPUEARMY - NO, OPUIIPF - YES,\ OPUIIPF - NO)}}{\mathrm{P\ (OPUEARMY - NO)}}$$

$$\mathrm{P\ (WA - NO \,|\, OPUEARMY\ absolute\ NO)} = \frac{\mathrm{(0.66 \times OPUEARMY - NO \times OPUIIPF - YES) + (1 \times OPUEARMY - NO \times OPUIIPF - NO)}}{1.0}$$

$$\mathrm{P\ (WA - NO \,|\, OPUEARMY\ absolute\ NO)} = \frac{(0.66 \times 1 \times 0.7067) + (1 \times 1 \times 0.2933)}{1.0}$$

$$\mathrm{P\ (WA - NO \,|\, OPUEARMY\ absolute\ NO)} = 0.759722$$

After giving a piece of evidence to the node *OPUEARMY absolute NO* in Figure 3.17, the result shows that the new posterior probability value of the node "*WA-NO*" increased from 0.575 to 0.76≈0.759722.

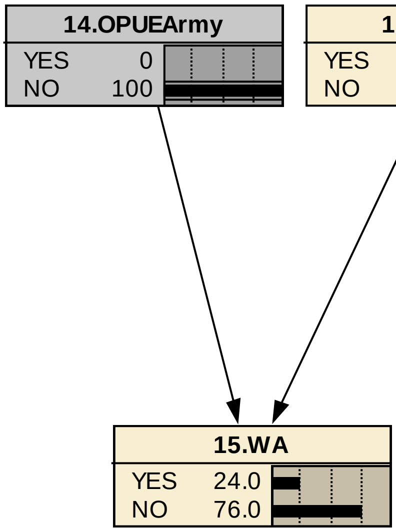


Figure 3.17: A Partial BN Model for Concealed Weapons (WA), Absolute-No Overcome the Prevention of Unauthorised Entry 3 and Overcome the Prevention of Unauthorised Introduction of Items in the Port Facilities (OPUIIPF)

Step 7: Sensitivity Analysis

Sensitivity analysis is the process of analysing how sensitive the result of a belief update (propagation of evidence) is to variations of the parameter value in the model. According to

Lucia and Mark (2001), parameter sensitivity is usually used as a series of tests in which the modeller sets different parameter values to see how a change in the parameter causes changes in the model. Also, sensitivity analysis helps build confidence in the model by studying uncertainties that are often associated with parameters in the model (Lucia & Mark, 2001).

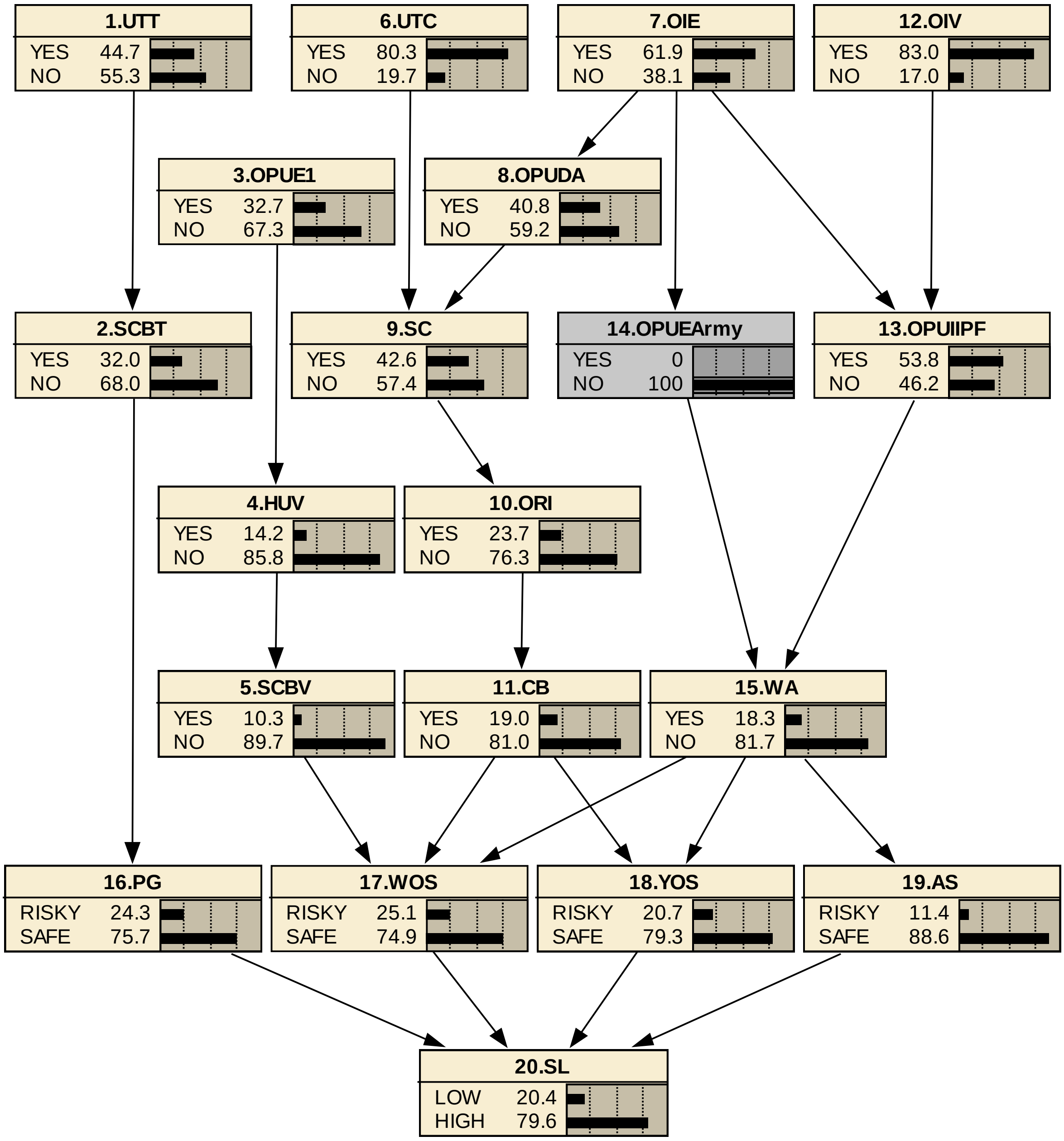


Figure 3.18: The Analysis of the Node Concealed Weapons Given the Evidence to the Node OPUEARMY Absolute NO

Sensitivity analysis allows the determination of what level of accuracy is necessary for a parameter to make the model sufficiently useful and valid. Therefore, sensitivity analysis indicates which parameter values are reasonable for use in the model. Further explanations on the matter can be found in literature, such as Pearl (1986, 1988), Lauritzen and Spiegelhalter (1988) and Castillo *et al*. (1997).

This step discusses the robustness of the BN model through sensitivity analysis. This is a very useful technique to identify the most sensitive parameter of a network. Besides, the sensitivity analysis also describes the functional relation between the parameter and the probability of the hypothesis. This can be used to compute the impact of different variations in the parameter value. The purpose of this step is to analyse how sensitive is the terrorist model about an attack on the port when there are changes in parameters or inputs.

To conduct the sensitivity analysis, one output node "Weapons Attack" (WA) and two input nodes "OPUEARMY", and "OPUIIPF" were used. One of the input nodes will be given different variations in probability values. If the output node is not influenced by an input node, then the input node is considered to be insignificant and has to be eliminated. Thus, further investigation is required for this situation. For example, by giving 100% of probability NO-increase to the node "OPUEARMY" =Absolute "NO", the posterior probability value of the node "WA=NO" increases from 57.5% to 76%. This means that the output node of this model was sensitive to the probability changes of the input nodes.

3.4 Conclusion

The developed models are dynamic and can be used in different situations based on uncertain situations faced by port operators. In real practice, port operators can add or drop any node or parameter based on uncertain situations they face. The models can also be applied in different service routes due to the flexibility of dealing with uncertain conditions. The output may be different if different situations are adopted, the total number of experts whether more or less than three, different seaport terminal characteristics are studied, and different numbers of inputs are included. Port operators are expected to concentrate their security attention more on the wharf operation site, which shows the highest vulnerabilities and is most likely to be attacked, followed by the yard operation site and the Administrations Site; Port Gates have the least risk as compared to other facilities, but the differences are not too far apart.

This chapter deals with the study about the risk of port container terminal facilities being attacked by terrorists, in which the novelties are:

- Determine the risk of being attacked from the view of the perpetrators (terrorists).
- Determine which of these potential facilities are most vulnerable.

- Develop a model from historical data of previous attacks combined with expert's prognosis from journals.
- Consider the possibility that a terrorist attack may come from the land and from the inside instead of only restricting it to an attack from the sea or waterway.

Chapter 4: Consequences Analysis of Terrorist Attacks on the Wharf by Using Event Tree Analysis and Bayesian Network (BN)

Summary

This chapter focuses on the analysing the consequences of terrorist attacks at the wharf by using an event tree. It is a continuation from the previous chapter, where a further study conducted on the subject of how effective are the security countermeasures on the wharf site and the aftermath due to the attack. Since the security countermeasures are complex and too big to be included in the event tree, a new approach was taken by combining event tree with a BN. In this chapter, three small Bayesian models were developed to predict the outcome of security countermeasures towards the probability of terrorist attacks on the seaport. These probability outcomes will then act as the countermeasures in the event tree analysis to calculate the consequence of the terrorist attack on the wharf site port terminal. The researcher then shows that BN is able to predict the probabilities of countermeasure effectiveness, which in turn allows the security countermeasure (i.e. retaliating to the terrorist attack on seaport) model to be generalised and applied in other circumstances.

4.1 Introduction

Wharf on site plays an important role in a seaport container terminal operation by accepting vessels. Competition between seaports in neighbouring areas is high, which makes it imperative for the port operator to minimize or eliminate downtime (i.e. no operations) due to delays or maintenance. From the previous chapter, the researcher calculated that terrorists are highly likely to attack the wharf operation site of a seaport since that will cause greater damage and more severe consequences to the port.

Every seaport has its own security team to prevent thefts and other security threat and a safety team to promote a safe working environment. These teams are also able to respond to any terrorist attack on the seaport which can reduce possible damage from such attacks. In this study, these groups are categorized as the response team that handles countermeasures against terrorist attacks. The goal of this study is to discover the effectiveness of the security countermeasures used to counter the terrorist attacks.

4.1.1 Problem, Gap and Novelty

Event tree is widely used in predicting the consequences of workplace accidents, such as fire and nuclear. There is no study yet on terrorist attack and seaport by using this event tree approach, and without previous historical data, event tree cannot be used to predict the success and failure probabilities of such attacks. Therefore, BN approach is used to cover that weakness. In event tree, two important dimensions are used which are an initiating event and the countermeasure. The initiating event for this study was the risk of terrorist attack to the wharf site and the countermeasures for the event were called security countermeasures or retaliation countermeasures. The event tree diagram creates multiple path starting with initiating event (the attack) and completed with three small BN model in analysing the security countermeasure's ability in countering the attack. Previously, another study has done a similar approach which has inspired this combination of method. Pereira (2015) have combine a bow tie model with Bayesian. Such integrated model combines three method (Fault Tree Analysis, Even Tree Analysis and BN) were then simplified by using only two method which is ETA and BN.

4.1.2 Scope and Limitation

Due to time constraints, the study concentrated on the consequences of an attack on the wharf operation sides of the seaport. The selection of facility in this study was based on the finding in the previous technical chapter that terrorist attacks were more likely targeted at the wharf on site rather than the other three facilities, i.e. yard on site, administration site and port gates, in that descending order, respectively.

4.1.3 Existing Countermeasures

Security countermeasures are critical in predicting the capability of a port in responding to terrorist attacks. In this study, it was established that the countermeasure troops were carefully assessed (in terms of their training and experience in handling this type of events, their security facilities, and their armoury supplies to fight back the attackers). The existing security countermeasures in this particular port come under two teams which are the Port Police and the Port Fire Fighters but for this study, they were treated as one department since their work decreased under a similar job scope (that is, responding to disasters and/or attacks).

There are a few threats arising out of a terrorist attack on the wharf, namely the crash or collision attack on the wharf by using vessels, an attack by using weapons, explosions during vessel collision with the wharf and fires at the wharf on site. Below are some countermeasures or responses that may work against such attacks:

I) Existing Countermeasures against Terrorist Attack (Collision and Attack by Using Weapons)

The Port Police and Firefighters are trained to keep the port safe from threats, prior to, during and after an attack. Prior to an attack, a port can detect an approaching vessel by using an Automatic Identification System (AIS) and monitors the vessel as it approaches the port. Precautions are triggered if the vessel does not respond to enquiries or requests as it approaches the port. The AIS is an automatic tracking system that is used on ships and vessel traffic services (VTS). A vessel with a gross tonnage exceeding 1,600 is required to install AIS, which enables its movement to be monitored via satellites. This system is actually a primary method of collision avoidance in water transportation (Navcen, 2018). An unauthorized vessel approaching a port at high speed and ignoring vessel traffic services' instructions is considered as an indicator of something suspicious happening on board. Usually, such a vessel is required to change the helmsman (Navigating Officers/Chief Officer) to a local navigator to avoid grounding on the specific route. The unresponsive communication behavior would be the best indicator that a potential problem is posed by the approaching vessel (the best scenario is that the vessel has communication issues and the worst scenario is the vessel is being hijacked by unknown pirates/terrorists).

During a terrorist attack, the countermeasure team would take steps to evacuate all non-security staff (an emergency alarm is activated accompanied by announcements via a PA system (Public Address System) with instructions on what to do and where to go.). The best defence is one that is done without injury and loss of life. All evidence of post-attack, will be preserved and recorded for an easier insurance claim and a report to the police, and shareholders.

II) Existing Countermeasures to Explosions

During or after a terrorist attack, prior to possible explosions, it is important for the security staff to prevent an explosion by identifying and detecting the bomb, chemical exposure, possible liquid or gas leaks that can cause explosions. Alert and forewarn possible victims to evacuate or take cover if an explosion is imminent. If indeed explosions occur, the countermeasure team needs to arrange for an evacuation of all non-security staff (emergency alarm is activated followed by announcements over the PA system with specific instructions on what to do and where to go). The best countermeasure is one that is done without causing injury and loss of life. In post-attack, the security team needs to conduct checks to prevent any potential secondary explosion and all evidence will be preserved and recorded for an easier insurance claim and a report to the police, and shareholders.

III) Existing Countermeasures against Fires

In case of fire, the security staff (the fire-fighters) need to understand how it started, spread and the best possible control measures. During a fire event, the fire-fighters should try and be able to put it under control, as well as reduce damage and save lives. After the fire event, an attack or explosions, the countermeasure team needs to give priority to finding the substance, liquid or gas or any material that started or caused the fire.

4.1.4 Bayesian Network (BN)

Refer to Bayesian Introduction in Section 2.4(A).

4.1.5 Event Tree Analysis (ETA)

Refer to Event Tree Analysis Introduction in Section 2.4(B).

The event tree diagram was perfect for this study since it creates multiple path starting with initiating event (the attack). But it is difficult to calculate the countermeasures in ETA, thus, here where BN start to play their role in analysing the security countermeasure's ability in countering the attack. The Bayesian can model interdependencies between the countermeasure nodes while here, the ETA insufficiently enough as a diagram. BN requires a more complicated condition and it is not suitable for this model.

The Idea of combining BN with ETA start from journal Pereira (2015) title "A Probabilistic Risk Analysis in Manufacturing Situational Operation". This journal uses a bowtie analysis and integrated it with Bayesian. See figure 4.1 and figure 4.2.

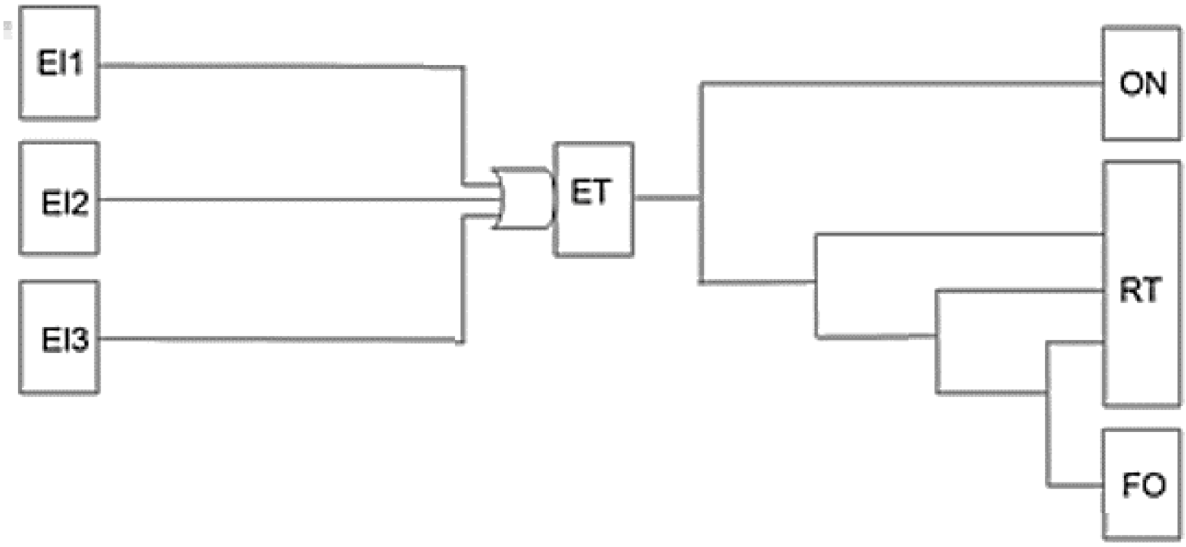


Figure 4.1: Bow-tie model (Pereira *et al.*, 2015)

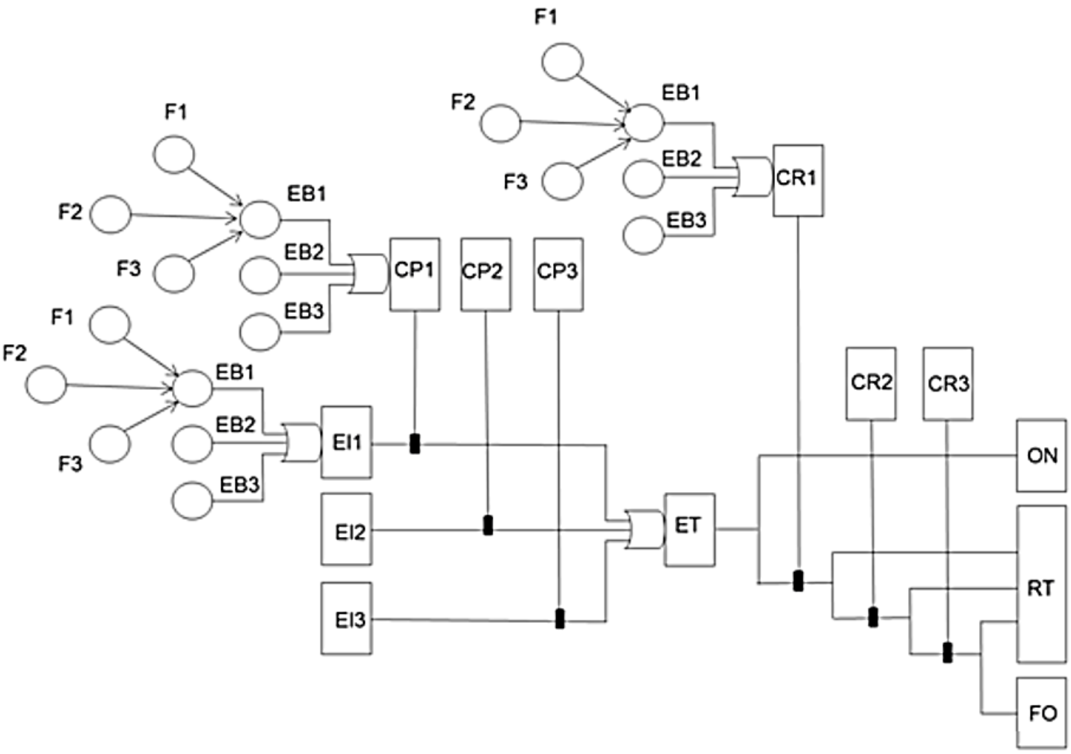


Figure 4.2: Integrated model (Pereira *et al.*, 2015)

Such integrated model combines three method (Fault Tree Analysis, Even Tree Analysis and BN) were then simplified by using only two method which is ETA and BN. For further illustration of the model, see Figure 4.3.

4.2 Methodology

ETA evaluates future accident consequences that might happen because of an initiating event. It is a 'forward-thinking' process, for example, the analyst begins with an initiating event and develops the following sequences of events with different probabilities of outcomes or potential accidents, accounting the successes and failures of the safety functions as the 'accidents' progress.

Mathematical Concepts

Event tree diagram creates all possible paths starting from the initiating event. It starts from the left side horizontally branching to the right. The vertical branch represents the success (up) or failure (down) of the initiating event. At the end of the vertical branch in the first event, a horizontal line is drawn and on each of them the top (success) and down (failure) is notated in writing. This line is written with a tag, which represents the path such as 1S, where '1' is the event number and 'S' is a success (Figure 4.3), and this process continues until the end state. When the ETA diagram reaches the end state, the outcome/consequence probability equation is written (Clemens *et al*., 1998), (Ericson, C. A., 2005). If the diagram is too big to be illustrated on a single page, it is possible to separate branches and draw them on different pages. These pages can be connected by transfer symbols. Note that for a sequence of 'n' events, there will be 'two' branches of the tree. However, in some cases the number may be reduced by removing impossible branches (Høyland, 2009).

$$1 = (\text{probability of success}) + (\text{probability of failure}) \qquad (4.1)$$

The probability of success can be derived from the probability of failure.

$$\text{Overall path probability} = (\text{probability of event 1}) \times (\text{probability of event 2}) \times (\text{probability of event n....}) \qquad (4.2)$$

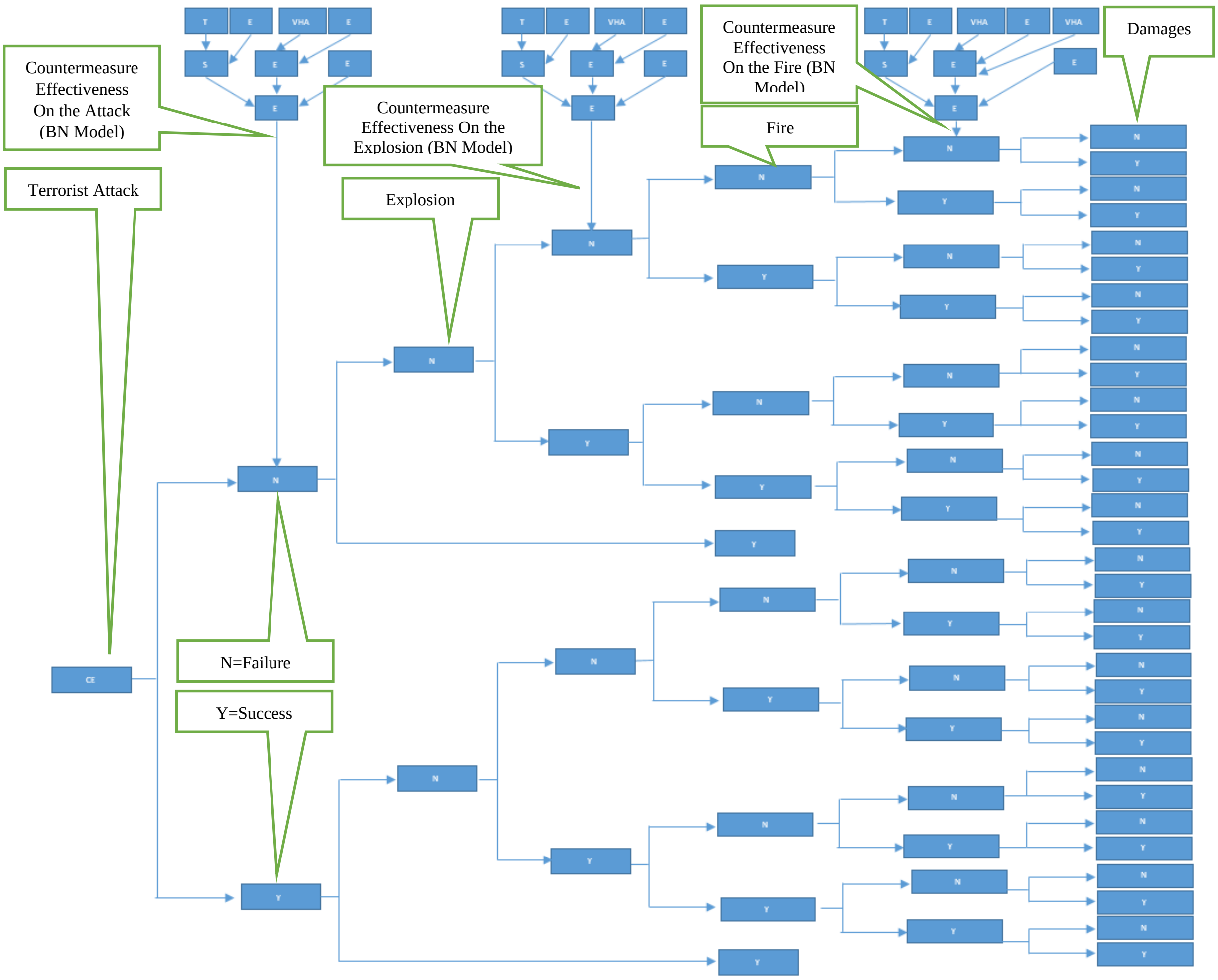

Countermeasure Effectiveness On the Attack (BN Model)
Terrorist Attack
Countermeasure Effectiveness On the Explosion (BN Model)
Explosion
Countermeasure Effectiveness On the Fire (BN Model)
Fire
Damages
N=Failure
Y=Success
CE
T
E
VHA
S
N
Y

Figure 4.3: An Early Blueprint of an ETA Model Combined with Bayesian Network.

The probabilities of success and failures for the countermeasures and events can be calculated by using a BN. The probability of "success" can also be calculated from 1 equals the probability of "success" plus the probability of "failure" (Ericson, 2005). For example, in the equation 1 equals the probability of success plus the probability of failure. If we know that the probability of failure equals 0.1 from BN, then through calculation we can solve the probability of success. Where the probability of success equals 1 minus the probability of failure then, we would have the probability of success equal to (1) minus (0.1) and the probability of success is equal to 0.9.

Steps to perform ETA and BN: (Clemens *et al.*, 1998; Ericson, 2005).

A) Step one: Identify an initiating event of interest.
B) Step two: Identify the safety functions designed to deal with the initiating event.
Since this study incorporates BN inside ETA, BN steps were placed in step two of ETA:

I) Identify significant influencing nodes
II) Define discrete states of the nodes
III) Developing a BN Model to check and modify the model by using a d-separation technique
IV) Data collection and analysis of each node
V) Bayesian inference and sensitivity analysis

C) Step three: Construct the ETA and Then Combine with Three Mini BN Models
D) Step four: Obtain event failure probabilities; if the failure probability cannot be obtained use fault tree analysis to calculate it.
E) Step five: Identify and evaluate the outcome risk then recommend corrective action.

Step 1: Identify an initiating event of interest

The aim of ETA is to determine the probability of the negative outcome that can cause injury and loss. It is important to acquire detailed information to understand the initiating event, accident scenario and intermediate events in order to construct the ETA diagrams. The ETA begins with the Initiating Event where the consequence of this event follows the “success” or “failure” categories. Each of the paths developed is associated with the percentage of ‘success’ or ‘failure’ occurring, where the overall probability of the event that occurs for that path can be calculated.

Firstly, define what needs to be involved or where to draw the boundaries. Then, identify the initiating events. This study adopts the initiating event from the previous chapter (Chapter 3). Under the assumption that the terrorists are targeting the seaport’s container terminal, it is predicted with a high likelihood that the wharf operation site will be attacked. This attack will immediately shut down the port operation and cause a lot of damage especially to the wharf sites, heavy metal equipment such as quay cranes, rubber tyre gantries, and prime mover lorries operating near to the place of attack. Based on expert judgements, written journals (Yang, 2006) and historical data (Global Terrorism Database, 2014a), it is most likely that the terrorists will attack by using a hijacked vessel and ram it up to the seaport or ram it with explosives.

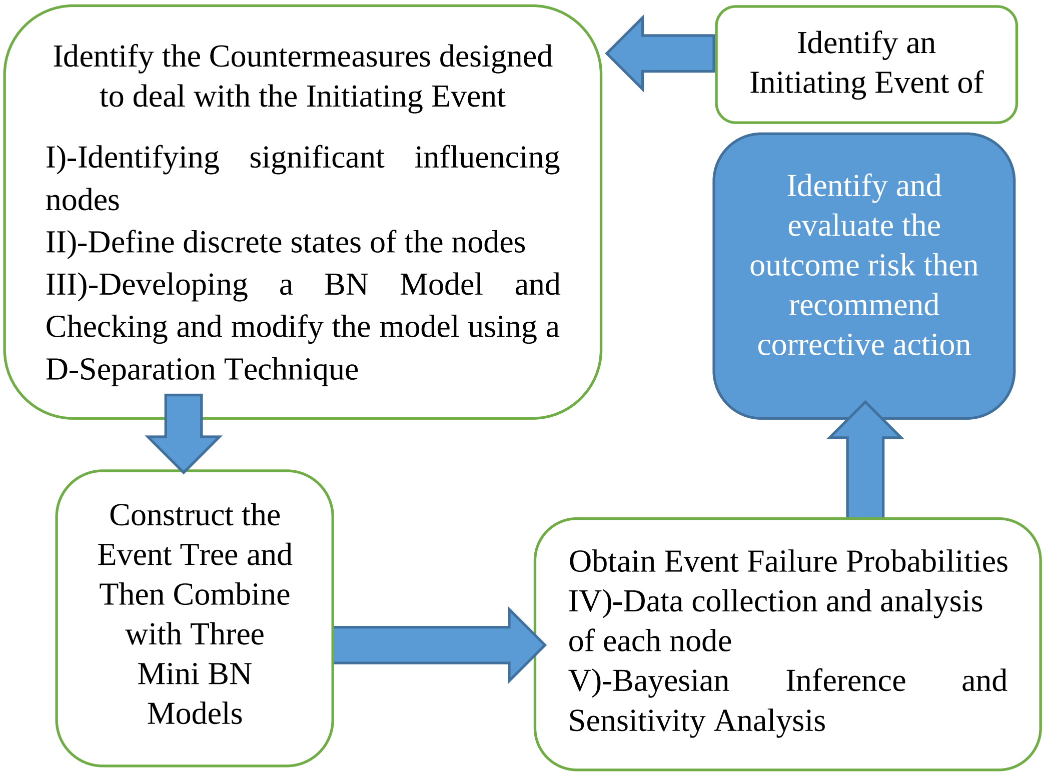

Identify an Initiating Event of
Identify the Countermeasures designed to deal with the Initiating Event
I)-Identifying significant influencing nodes
II)-Define discrete states of the nodes
III)-Developing a BN Model and Checking and modify the model using a D-Separation Technique
Construct the Event Tree and Then Combine with Three Mini BN Models
Obtain Event Failure Probabilities
IV)-Data collection and analysis of each node
V)-Bayesian Inference and Sensitivity Analysis
Identify and evaluate the outcome risk then recommend corrective action

Figure 4.4: The Assessment Procedure of BN and ETA Method

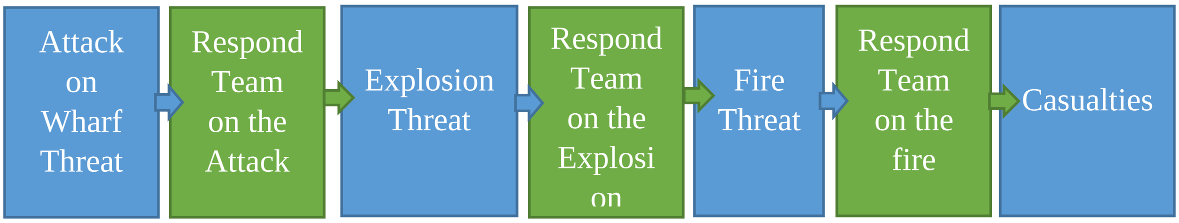


Figure 4.5: The Initiating Event (blue) versus the Countermeasure Effectiveness (green)

Step 2: Identify the Safety Functions Designed to Deal with the Initiating Event

The second step is to identify the countermeasures and in order to determine how effective is their involvement in countering the initial event. An interview was conducted and questionnaires distributed to the industrial and education experts. The data collected were then inserted into the BN software (NETICA) to analyse the probabilities of success and failure of the port security and safety measures.

Views from the industry and education experts were obtained through interviews in order to know the factors within the countermeasures that may lead to the probabilities of an attack from terrorists on the wharf. Three different threats were used which were attacks by collision, weapons attacks, and explosions and fires. The countermeasures against terrorist attacks would come from two departments, the Port Police Department (in charge of Port Security) and the Port's fire fighter Department (in charge of Port Safety). They are the experts and they specialise in saving people and handling dangerous situations. They are in a better position to reduce the effect of terrorist attacks compared to an average worker who is not specially trained in safety and security aspects and disaster mitigating measures.

I) Identifying significant nodes

Response team or countermeasure team is the team involved in taking actions to counter the terrorist attack. As a general concept, countermeasure implies precision in actions and refers to any tactical solutions or technological systems designed to prevent unwanted outcomes of a process. In this study, three different scenarios of countermeasure responses to the threat were listed, which were [1] countermeasures in response to terrorist attacks, [2] countermeasures in response to explosions, and [3] countermeasures in response to fires. All three scenarios (attacks, explosions, and fires) may happen separately, alone or in combination at the same time, but the scenarios were treated separately in order to allow the experts to make better assessments for the security and safety response team in countering the attack.

A-The countermeasures' efficient responses to the terrorist attack by collision and weapon

Seven nodes corresponding to the countermeasures against an attack to the wharf operation site are listed below:

Table 4.1: Nodes of BN Countermeasures to the Terrorist Attack by Collision and Weapon

Training (Attack)	Training is developing oneself or a team on the knowledge that relates to specific useful competencies, physically and spiritually. It has a specific goal of improving their capabilities and performance. In ISPS code 11, there is a compulsory training that requires port security officers, ship security officers, and other security personnel to attend vigorous training on operations (Gowsalya *et. al.,* 2017).
Experience (Attack)	Experience is the knowledge and mastery of an event gained through exposure to it. An experienced person is someone who has post-event knowledge and henceforth he/she gains a reputation as an expert. An expert has the know-how rather than merely the propositional/theoretical knowledge. Experienced port police and firefighters must have long

	service records, especially in security-related jobs prior to working at the port. Experience in military or police forces or prior involvement in rescue missions count (Gowsalya *et. al.,* 2017).
Skills (Attack)	Skills are the ability to do something at excellence level. It comes from one's knowledge, experience, and training. Experienced and well-trained Port Police personnel and Fire Fighters are considered skilful (Gowsalya *et. al.*, 2017).
Visual/ Hearing Awareness (Attack)	Visual and Hearing Awareness aims to equip the whole place with proper monitoring whether via technology (such as visible light cameras, fixed or pan video cameras, pinholes or fish-eye video cameras etc.) or non-technological assets (security posts/ booths with 360-degree views, or security patrols). These security measures provide fast first-hand information and help the security officers come out with the best countermeasures (Stanton *et. al.,* 2001).
Emergency Calls (Attack)	Unlike Visual/ Hearing Awareness (Information acquired within the seaport), Emergency Calls are information given by the port security from outside the seaport areas (such as coast guards in the Malacca Straits) giving warnings about possible attacks. Information such as distress signals from hijacked vessels, strange behaviours like vessel stopping mid-journey without reason, gunfire during the hijackings, and coast guard attacked before the hijack, are to be reported to the nearest seaport (Norman, 2010).
Situation Awareness (Attack)	Situation awareness is the knowledge, and attitude held by members of a group pertaining to the protection of the informational, and physical, assets of that group. Providing the right tools will enable the security officers to receive information faster and be aware of current situations. Many organizations require formal security awareness training for all workers when they join the organization and periodically after that, usually annually (Norman, 2010).
Armoury Defence Supply (Attack)	If the port comes under terrorist attack, it will immediately alert the military. However, the time lapse between the military being alerted to its arrival at the scene may require the port to also alert the local police for expediency. In some instances, the port also has some basic weapon supply to carry out the initial defence. In addition to the port police personnel, employees who have a military background or training can be supplied with weapons too.

B- The countermeasure efficient responses to explosions

Seven nodes corresponding to the countermeasures against possible explosions at the wharf operation site are listed below:

Table 4.2: Nodes of BN Countermeasures Against Possible Explosions

Training (Explosion)	Training the security staff in handling explosions-related attacks is very much different from combat training and use of weapons. The security staff need to be trained in matters and measures to be taken prior to an explosion such as recognising the types and features of a bomb, gas or chemical leaks and other hazards. In a situation that an explosion is imminent, they need to take measures to forewarn the people in the

	vicinity, provide covers to them, in order to avoid or minimise injuries or loss of life. Post-explosion, the security staff need to evaluate if there would be secondary explosions and institute measures in the same manner in handling explosions danger. Evacuation procedures is a must (Gowsalya *et. al.,* 2017).
Experience (Explosion)	Experience in handling situations related to an explosive material is mostly possessed by personnel whose previous jobs are firemen, military men, policemen or staff of security firms. Firemen usually have experience in handling dangerous goods, chemicals while military ex-servicemen know a lot about handling and defusing bombs (Gowsalya *et. al.,* 2017).
Skills (Explosion)	Skills in handling explosives involve the ability to predict if a collision/accident may lead to explosions, knowing the standard measures in ensuring the safety of people at the scene including evacuation procedures. Such skills are important in preventing injuries and/or loss of lives (Gowsalya *et. al.,* 2017).
Visual/ Hearing Awareness (Explosion)	Visual/Hearing awareness in this context is not the same as the ability of experienced and trained staff to detect an explosion. This node refers to the security staff having a visual awareness of an explosion when they see one (when an explosion happens). As soon as he sees an explosion, he takes the next step of reporting it (the event) to the response team (usually from the security post). In the case of “hearing awareness”, it occurs when the security staff hears an explosion but does not see it perhaps because the explosion happens at locations beyond his viewpoint or his view is blocked by objects or obstacles. In this respect, he has to contact any security facilities located nearest to the suspected explosion for confirmation and if the responses are in the negative (meaning no explosion), an explanation is required to identify the loud noise. If he receives no response, it is assumed that the explosion originates from the security facility near the explosion itself (Stanton *et. al.,* 2001).
Emergency Call (Explosion)	Since this study is related to the terrorist attack on the wharf scenario, the emergency calls are only meant for post-explosion. Emergency calls are not usually made prior to an explosion nor during explosions (Norman, 2010).
Situation Awareness (Explosion)	Situation awareness is important in handling situations involving explosions. It dictates that the security office assigns an appropriate response team to secure the area of the explosion, mobilise the rescue teams to save the victims and conduct an emergency evacuation (Stanton *et. al.,* 2001).
Explosion Defence Supply (Explosion)	The explosion defence supply to combat bomb/explosions are divided into two areas viz. detection and defuse. Detection involves the use of trained animals, detection aids and detection devices. Dogs are usually used in detecting a bomb and they work fine except that they tend to become tired and bored if used for too long in each mission. Detection aids are used to search for explosives by applying DMDNB* to the explosives. DMDNB produces a specific odour that dogs can smell or detect. Detection aids are usually used in commercial explosives to ensure every bomb set up is able to explode and none malfunctions. Detection devices vary from low-tech to high-tech ones such as X-ray Contena Machine (Cargo Scanner), Colorimetrics & Automated

	Colorimetrics (A chemical that detects explosive by observing colour reaction), Mechanical scent detection, and Silicon Nanowires for trace detection of explosives.
DMDNB is dimethyl and dinitrobutane where chemically names as 2,3-dimethyl-2,3-dinitrobutane, is an organic compound used as a detection taggant for explosives mostly use in United States (Thomas, *et al*. 2005).	

C- The countermeasures' efficient responses to fires

Eight nodes corresponding to the countermeasures against fires occurring at the wharf operation site are listed below:

Table 4.3: Nodes of BN Countermeasures Against Fires

Training (Fire)	Training for firefighters involves understanding how a fire starts, spreads and ways to control it. Staff have to be fully aware of fire risks in the workplace and prevent it from happening. In the event of fires due to terrorist attacks (whether they are caused by explosions, or by the terrorist from the vessel), the trained firefighting staff are able to handle hand-operated firefighting equipment and have practical knowledge on handling the situation (such as giving first-aid or temporary medical help to the victims) (Gowsalya *et. al.*, 2017).
Experience (Fire)	Experience in firefighting usually resides in senior staff who work and operate at different levels compared to the junior staff. The responsibility of handling fires that is entrusted to them makes them capable of making instant decisions during fires. The junior staff usually receive similar training but they lack experience and understanding of practical applications to be able to make split-second decisions like the senior staff. In other words, the junior staff have known only basic firefighting know-how, but not the strategic or tactical ones (Gowsalya *et. al.*, 2017).
Skills (Fire)	Skills are the ability to control fires, reduce damage and save lives at the excellence level. Skills come from one's knowledge, experience and training. In order to increase the number of skilled staff, senior staff can be asked to impart the required skills to the junior staff during training (Gowsalya *et. al.*, 2017).
Visual/ Hearing Awareness (Fire)	Visual and Hearing Awareness refers to putting the whole place under monitoring via technology. Since the port police is responsible for overseeing the security of the port, the task for which includes the visual and hearing awareness, providing a security post at the fire station would be redundant (Stanton *et. al.*, 2001).
Emergency Call (Fire)	Firefighting staff need to always be alert and ready in case of fires happening or possible disaster from fires. They are the first to receive a call when a fire breaks out at the port (Norman, 2010).
Fire Alarm (Fire)	A fire alarm system consists of some devices working together to detect and alert the people through audio appliances when fire, smoke, or other emergencies are present. These alarms can be activated automatically from smoke detectors and heat detectors or may also be activated via physical fire alarm activation devices such as manual call points/ pull stations or Magnetic lock on the emergency door (Norman 2010). Alarms

	can be either motorised bells or wall mountable sounders or horns (Norman, 2010).
Situation Awareness (Fire)	Situation awareness is the knowledge and attitude possessed by members of a group regarding the protection of the informational, and physical, assets of that group. Providing the right tools will help security officers receive information faster and become aware about the current situation. Many organisations require formal security awareness training for all workers when they join the organisation and periodically after that, usually annually (Norman 2010).
Fire Defence Supply (Fire)	In a firefighting list of supplies for fire control is basic firefighting items such as firefighter emergency suit, self-conditioned breathing apparatus, ground ladder, fire hose, first aid kit, power saw, hand tools and rescue tools (OSHA, 2019).

Table 4.4: Nodes List

Terrorist Attacks	Explosions	Fires
1.Training (Attack) 2.Experience (Attack) 3.Skills (Attack) 4.Visual/ Hearing Awareness (Attack) 5.Emergency Call (Attack) 6.Situation Awareness (Attack) 7.Armoury Defence Supply (Attack)	1.Training (Explosion) 2.Experience (Explosion) 3.Skills (Explosion) 4.Visual/ Hearing Awareness (Explosion) 5.Emergency Call (Explosion) 6.Situation Awareness (Explosion) 7.Explosion Defence Supply (Explosion)	1.Training (Fire) 2.Experience (Fire) 3.Skills (Fire) 4.Visual/ Hearing Awareness (Fire) 5.Emergency Call (Fire) 6.Fire Alarm (Fire) 7.Situation Awareness (Fire) 8.Fire Defence Supply (Fire Equipment)

Between these models, the only difference between the attack and explosion model and the fire model is the alarm. In the case study, the subjected port had two types of alarm, [1] fire alarms and [2] an emergency alarm. They emit different sound tones and their operation differs too. The fire alarm emits an alarm sound only for a particular facility (building) that is on fire, while the emergency alarm (used for incidents, involving terrorist attacks and explosions) will be blaring out throughout the whole port compound accompanied by emergency announcements. Therefore the “emergency alarm” was placed under the same node as the “emergency call”, but not the “fire alarm”, which was classified as a node of its own.

II) Define discrete states of the nodes

Listed below are three tables pertaining to the countermeasures efficient responses to the terrorist attacks, explosions and fires on the port (Table 4.5, Table 4.6, and Table 4.7).

Table 4.5: Nodes of Bayesian Network Countermeasures to the Terrorist Attack by Collision and Weapon

Training (Attack)	The states of training (attacks) are, (1) YES, the Security Response Team received training that enables them to counter terrorist attacks, (2) NO, the Security Response Team did not receive training that enables them to counter terrorist attacks (Gowsalya *et. al.*, 2017).
Experience (Attack)	The states of experience (attacks) are, (1) YES, the Security Response Team do have the experience that enables them to counter terrorist attacks, (2) NO, the Security Response Team do not have the experience that enables them to counter terrorist attacks (Gowsalya *et. al.*, 2017).
Skills (Attack)	The states of skills (attacks) are, (1) YES, the Security Response Team do have the skills that enable them to counter terrorist attacks, (2) NO, the Security Response Team do not have the skills that enable them to counter terrorist attacks (Gowsalya *et. al.*, 2017).
Visual/ Hearing Awareness (Attack)	The states of visual or hearing awareness (attacks) are, (1) YES, the Security Response Team do have visual or hearing awareness that enable them to counter terrorist attacks, (2) NO, the Security Response Team do not have visual or hearing awareness that enable them to counter terrorist attacks (Stanton *et. al.*, 2001).
Emergency Call (Attack)	The states of emergency call (attacks) are, (1) YES, the Security Response Team do have reliable and fast security information flow for emergency call that enables them to counter terrorist attacks, (2) NO, the Security Response Team do not have reliable and fast security information flow for emergency call that enables them to counter terrorist attacks (Norman, 2010).
Situation Awareness (Attack)	The states of situation awareness (attacks) are, (1) YES, the Security Response Team do have good situation awareness that enables them to counter terrorist attacks, (2) NO, the Security Response Team do not have good situation awareness that enables them to counter terrorist attacks (Stanton *et. al.*, 2001).
Armoury Defence Supply (Attack)	The states of armoury defence supply (attacks) are, (1) YES, the Security Response Team do have armoury defence supply that makes it capable of countering terrorist attacks, (2) NO, the Security Response Team do not have armoury defence supply that can make it capable of countering terrorist attacks.

Table 4.6: Nodes of Bayesian Network Countermeasures Against Possible Explosions

Training (Explosion)	The states of training (explosions) are, (1) YES, the Security Response Team receive training that enables them to counter or control explosions, (2) NO, the Security Respond Team do not receive training that enables them to counter or control explosions (Gowsalya *et. al.*, 2017).
Experience (Explosion)	The states of experience (explosions) are, (1) YES, the Security Response Team do have the experience that enables them to counter or control explosions, (2) NO, the Security Response Team do not have the experience that enables them to counter or control explosions (Gowsalya *et. al.*, 2017).
Skills (Explosion)	The states of skills (explosions) are, (1) YES, the Security Response Team do have the skills that enable them to counter or control explosions,

	(2) NO, the Security Response Team do not have the skills that enable them to counter or control explosion (Gowsalya *et. al.*, 2017).
Visual/ Hearing Awareness (Explosion)	The states of visual or hearing awareness (explosions) are, (1) YES, the Security Response Team do have visual or hearing awareness that enables it to counter or control explosion, (2) NO, the Security Response Team do not have visual or hearing awareness that enables it to counter or control explosions (Stanton *et. al.*, 2001).
Emergency Call (Explosion)	The states of emergency call (explosions) are, (1) YES, the Security Response Team do have reliable and fast security informant for emergency call that enables them to counter or control explosions, (2) NO, the Security Response Team do not have reliable and fast security informant for emergency call that enables them to counter or control explosions (Norman, 2010).
Situation Awareness (Explosion)	The states of situation awareness (explosions) are, (1) YES, the Security Response Team do have good situation awareness that enables them to counter or control explosions, (2) NO, the Security Response Team do not have good situation awareness that enables them to counter or control explosions (Stanton *et. al.*, 2001).
Explosion Defence Supply (Explosion)	The states of explosion defence supply (explosion) are, (1) YES, the Security Response Team do have explosion defence supply that is capable of being used to counter or control explosions, (2) NO, the Security Response Team do not have explosion defence supply that is capable of being used to counter or control explosions.

Table 4.7: Nodes of Bayesian Network Countermeasures Against Fires

Training (Fire)	The states of training (fires) are, (1) YES, the Security Response Team receive training that enables them to counter or control fires, (2) NO, the Security Response Team do not receive training that enables them to counter or control fires (Gowsalya *et. al.*, 2017).
Experience (Fire)	The states of experience (fires) are, (1) YES, the Security Response Team do have the experience that enables them to counter or control fires, (2) NO, the Security Response Team do not have the experience that enables them to counter or control fires (Gowsalya *et. al.*, 2017).
Skills (Fire)	The states of skills (fires) are, (1) YES, the Security Response Team do have the skills that enable them to counter or control fires, (2) NO, the Security Response Team do not have the skills that enable them to counter or control fires (Gowsalya *et. al.*, 2017).
Visual/ Hearing Awareness (Fire)	The states of visual or hearing awareness (fires) are, (1) YES, the Security Response Team do have visual or hearing awareness that helps to counter or control fires, (2) NO, the Security Response Team do not have visual or hearing awareness that helps to counter or control fires (Stanton *et. al.*, 2001).
Emergency Call (Fire)	The states of emergency call (fires) are, (1) YES, the Security Response Team do have reliable and fast security information flow for emergency call that helps to counter or control fires, (2) NO, the Security Response Team do not have reliable and fast security information flow for emergency call that helps to counter or control fires (Norman, 2010).

Emergency Fire Alarm (Fire)	The states of emergency fire alarm (fires) are, (1) YES, the Security Response Team do have reliable emergency fire alarms that help to counter or control fires, (2) NO, the Security Response Team do not have reliable emergency fire alarms that help to counter or control fires (Norman, 2010).
Situation Awareness (Fire)	The states of situation awareness (fires) are, (1) YES, the Security Response Team do have good situation awareness that helps to counter or control fires, (2) NO, the Security Response Team do not have good situation awareness that helps to counter or control fires (Stanton *et. al.*, 2001).
Fire Defence Supply (Fire)	The states of fire defence supply (fire) are, (1) YES, the Security Response Team do have equipment supply that is capable of being used to counter or control fires, (2) NO, the Security Response Team do not have equipment supply that is capable of being used to counter or control fires (OSHA, 2019).

A simple state definition mechanism is used to determine the state of all nodes in Table 4.8. The list below describes the nodes and their respective states: -

Table 4.8: The Total Nodes and Their States

Descriptions of Nodes	States
1.Training (Attacks)	Yes, No
2.Experience (Attacks)	Yes, No
3.Skills (Attacks)	Yes, No
4.Visual/ Hearing Awareness (Attacks)	Yes, No
5.Emergency Call (Attacks)	Yes, No
6.Situation Awareness (Attacks)	Yes, No
7.Armoury Defence Supply (Attacks)	Yes, No
8.Training (Explosions)	Yes, No
9.Experience (Explosions)	Yes, No
10.Skills (Explosions)	Yes, No
11.Visual/ Hearing Awareness (Explosions)	Yes, No
12.Emergency Call (Explosions)	Yes, No
13.Situation Awareness (Explosions)	Yes, No
14.Explosion Defence Supply (Explosions)	Yes, No
15.Training (Fires)	Yes, No
16.Experience (Fires)	Yes, No
17.Skills (Fires)	Yes, No
18.Visual/ Hearing Awareness (Fires)	Yes, No
19.Emergency Call (Fires)	Yes, No
20.Fire Alarm (Fires)	Yes, No
21.Situation Awareness (Fires)	Yes, No
22.Fire Defence Supply (Fires)	Yes, No

III) Developing a BN model to checking and modify the model by using a d-separation technique

After identifying the nodes and their states, the next step is to confirm the relationships between them and construct a qualitative network to represent all the nodes and their dependencies. The knowledge about understanding various dependencies is then used to construct the causal structure of the risk of terrorists attacking container port facilities. The graphical representation (a model) permits a direct expression of the fundamental qualitative relationships. After reviewing the model with experts and academicians, the researcher develops a set of questionnaires to get uniform responses instead of using direct interviews (see Step 4: Data collection and analysis of each node.

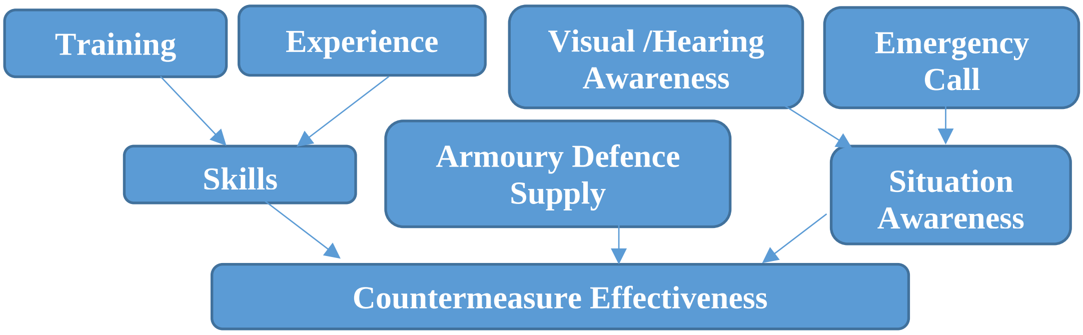


Figure 4.6: An Initial of a BN Model Representing Countermeasure Effectiveness in Responding to Terrorist Attack.

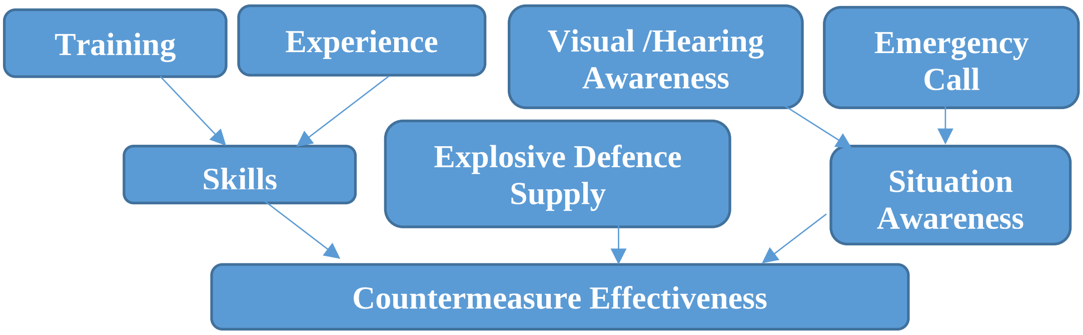


Figure 4.7: An Initial of a BN Model Representing Countermeasure Effectiveness in Responding to Explosions

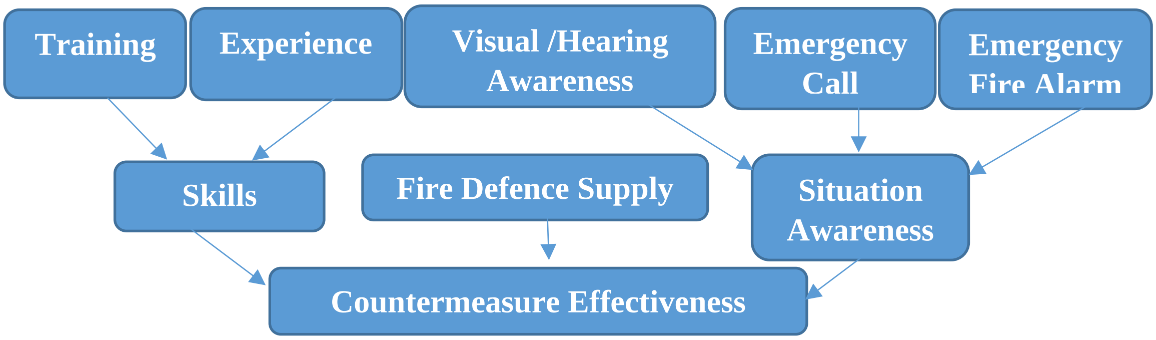


Figure 4.8: An Initial of a BN Model Representing Countermeasure Effectiveness in Responding to Fires

Figure 4.6, Figure 4.7 and Figure 4.8 are the initials of a BN model representing countermeasure effectiveness in response to terrorist attacks, explosions and fires, respectively. There are no changes after checking by using the d-separation technique.

Step 3: Construct the ETA and Then Combine with Three Mini BN Models

The third step is to build the ETA diagram by incorporating the horizontal and vertical lines. Horizontal lines are drawn between both functions, and vertical lines are drawn at each safety function that applies. ETA starts from left to the right, which begins with the initiating event, leads to another event called the intermediate event and on the rightmost is the consequence of the event. Horizontal lines connect each of the event stages with each branch splitting into two (one each for “success” and “failure”).

Table 4.9: Direction of Failure and Success

The direction of failure and success	
Failure	Upward
Success	Downward

After that, all the mini BN were combined on the newly construct ETA model. Those mini BN result were put at the countermeasure section right after the attack, explosion and fire. (See Figure 4.3).

Step 4: Obtain Event Failure Probabilities by Data Collection

To obtain the probabilities, two (2) different types of data collection were created, which were [1] the probability of safety function which was conducted by using BN and [2] the event probabilities. The probability of safety function was a lot more complex and required the use of BN since there are many factors to consider for the countermeasures against terrorist attacks, while the event probabilities were kept at basic.

[1] The probability of safety function which was conducted by using the Bayesian Network

This safety function is the continuation from Step 2: Developing a BN Model to check and modify the model by using a d-Separation Technique. Please refer to Figure 4.4 (The assessment procedure of BN and ETA method) for easier understanding of the whole picture.

IV) Data collection and analysis of each node

After reviewing the model with experts and academicians, a set of questionnaires was developed. The survey questionnaire starts with respondent information in regard to age, job expertise and experience. In the second section, the respondents answer the questions relating to the factors of the countermeasures in terms of percentage. This questionnaire was presented by using an eSurvey Creator from https://www.esurveycreator.co.uk/.

There were 71 qualitative data sets that the researcher managed to gather through the questionnaires (Appendix 6). These data sets were obtained from the selected experts who were from the maritime and security backgrounds. In the set of questionnaires, a set of guides of the probability rate is attached. Table 4.10 illustrates the range of the probability levels that would give an idea to the experts to help them state their judgments according to the situation(s) given in the questionnaires. Basically, the probability rate was divided into two parts, which were 1) Yes – the countermeasure can counter terrorist attacks (right-hand side) and 2) No – the countermeasure cannot counter terrorist attacks (left-hand side). This guide started from 50 as the middle value to differentiate the probability rate between the right and left-hand sides. However, the determination of what term should be used to express both sides was dependent on the state name for each node (Rahman, 2012).

All feedback received from the experts is transformed into a probability value (ranging from 0 and 1). 50 rating is the middle value that can be translated as 0.5 of the probability value, while the probability rating from 100 to 00 on both right-hand to left-hand sides can be transformed to the probability value of Yes and No, respectively (Table 4.10).

Table 4.10: The Transformation Process from the Probability Rate to the Probability Value

0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
→										
00 No	10	20	30	40	50	60	70	80	90	100 Yes

The total probability value of each node must sum up to 1.0, for instance 0.43 (highly unlikely) + 0.57 (highly likely) = 1.0. Due to the number of experts being more than 1, an average probability value for every single state of each node had to be calculated by using the average probability value for the state (Please refer to Chapter 3: Equation 3.6 and Table 3.6).

Result from the questionnaire (R1 until R6 – represent Respondent 1 to 6)

Table 4.11: The Demographics of Expert Interviewed

Result		R1	R2	R3	R4	R5	R6
1	Age	35	32	53	65	46	41
2	Experience	5	13	34	41	21	15
3	The Scope of Job	Security	Security	Security	Fire Fighter	Fire Fighter	Fire Fighter

Table 4.12: Result from Industry Expert for Event Success and Failure Probabilities (Attack Countermeasure)

Attack: The UCPT Data Collected from Expert Judgement on Given Nodes						
4	Training (Attacks)				State	Probability
					Yes	75.15
					No	24.83
5	Experience (Attacks)				State	Probability
					Yes	39.67
					No	60.33
10	Visual/ Hearing Awareness (Attacks)				State	Probability
					Yes	87.17
					No	12.83
11	Emergency Call (Attacks)				State	Probability
					Yes	94.50
					No	5.50
16	Armoury Defence Supply (Attacks)				State	Probability
					Yes	43.83
					No	56.17
Attack: The CPT Data Collected from Expert Judgement on Given Nodes						
6 to 9	Skills (Attacks)	Training		Experience	Yes	No
		No		No	0.17	99.83
				Yes	70.17	29.83
		Yes		No	77.33	22.67
				Yes	92.17	7.83
12 to 15	Situation awareness	Visual/ Hearing Awareness		Emergency call	Yes	No
		No		No	0.17	99.83
				Yes	92	8
		Yes		No	84.17	15.83
				Yes	98.17	1.83
17 to 24	Retaliation Effectiveness -1	Skills (Attacks)	Situation Awareness	Armoury Defence Supply	Yes	No
		No	No	No	0.5	99.5
				Yes	79.67	20.33
			Yes	No	79.33	20.67
				Yes	87.67	12.33

		Yes	No	No	79.67	20.33
				Yes	89.33	10.67
			Yes	No	89.5	10.5
				Yes	96.83	3.17

Table 4.13: Result from Industry Expert for Event Success and Failure Probabilities (Explosion Countermeasure)

Explosion: The UCPT Data Collected from Expert Judgement on Given Nodes						
25	Training (Explosion)				State	Probability
					Yes	87.17
					No	12.82
26	Experience (Explosion)				State	Probability
					Yes	57
					No	43
31	Visual/ Hearing Awareness (Explosion)				State	Probability
					Yes	87.33
					No	12.67
32	Emergency Call (Explosion)				State	Probability
					Yes	94.5
					No	5.5
37	Armoury Defence Supply (Explosion)				State	Probability
					Yes	41.33
					No	58.67
Explosion: The CPT Data Collected from Expert Judgement on Given Nodes						
27 to 30	Skills (Explosion)	Training		Experience	Yes	No
		No		No	0.17	99.83
				Yes	64.5	35.5
		Yes		No	71.33	28.67
				Yes	86.67	13.33
33 to 36	Situation Awareness	Visual/ Hearing Awareness		Emergency call	Yes	No
		No		No	0	100
				Yes	91.83	8.17
		Yes		No	15.67	15.67
				Yes	1.17	1.17
37 to 45	Retaliation Effectiveness - 2	Skills (Explosion)	Situation Awareness	Armoury Defence Supply	Yes	No
		No	No	No	0.33	99.67
				Yes	79.5	20.5
			Yes	No	79.5	20.5
				Yes	87.83	12.17
		Yes	No	No	79.67	20.33
				Yes	89.17	10.83
			Yes	No	89.33	10.67
				Yes	97.33	2.67

Table 4.14: Result from Industry Expert for Event Success and Failure Probabilities (Fire Countermeasure)

Fire: The UCPT Data Collected from Expert Judgement on Given Nodes						
46	Training (Fire)				State	Probability
					Yes	91.17
					No	8.83
47	Experience (Fire)				State	Probability
					Yes	46
					No	54
52	Visual/ Hearing Awareness (Fire)				State	Probability
					Yes	85
					No	15
53	Emergency Call (Fire)				State	Probability
					Yes	94.67
					No	5.33
54	Emergency Fire Alarm (Fire)				State	Probability
					Yes	80
					No	20
63	Armoury Defence Supply (Fire)				State	Probability
					Yes	44.17
					No	55.83
Fire: The CPT Data Collected from Expert Judgement on Given Nodes						
48 to 51	Skills (Fire)	Training		Experience	Yes	No
		No		No	0	100
				Yes	64.83	35.17
		Yes		No	71.33	28.67
				Yes	86.17	13.83
55 to 62	Situation Awareness	Visual/ Hearing Awareness	Emergency Call	Emergency Fire Alarm	Yes	No
		No	No	No	0	100
				Yes	78.33	21.67
			Yes	No	90.83	9.17
				Yes	96	4
		Yes	No	No	83.83	16.17
				Yes	93	7
			Yes	No	97.5	2.5
				Yes	98.5	1.5
64 to 71	Retaliation Effectiveness - 3	Skills (Fire)	Situation Awareness	Armoury Defence Supply	Yes	No
		No	No	No	0.17	99.83
				Yes	70.33	29.67
			Yes	No	70.67	29.33
				Yes	81.5	18.5
		Yes	No	No	70.5	29.5
				Yes	82.83	17.17
			Yes	No	83.17	16.83
				Yes	86.33	13.67

After calculating the average of experts' responses, the results were used as inputs for the BN model. The BN developed were the countermeasures for port security and safety capability and effectiveness. These models consist of three BN, with each model representing different situations (terrorist attacks, explosions, and fires).

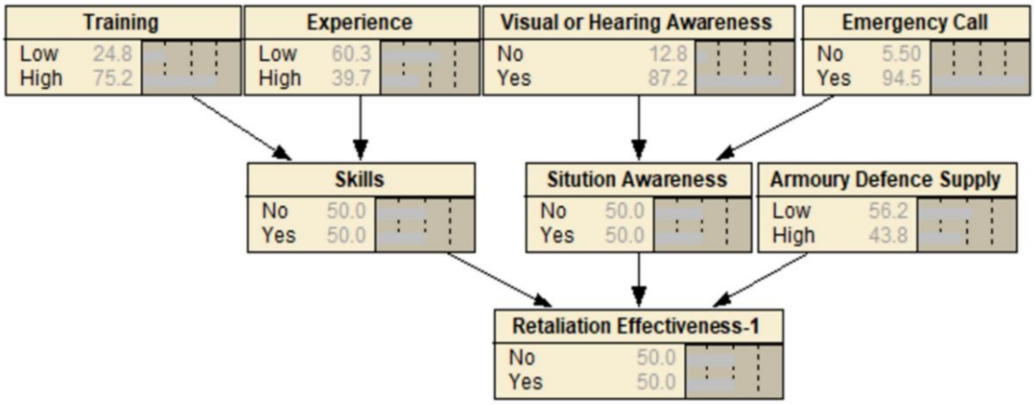


Figure 4.9: The BN model representing the Retaliation Effectiveness or Security Port Countermeasures - RE1 (Industry Expert)

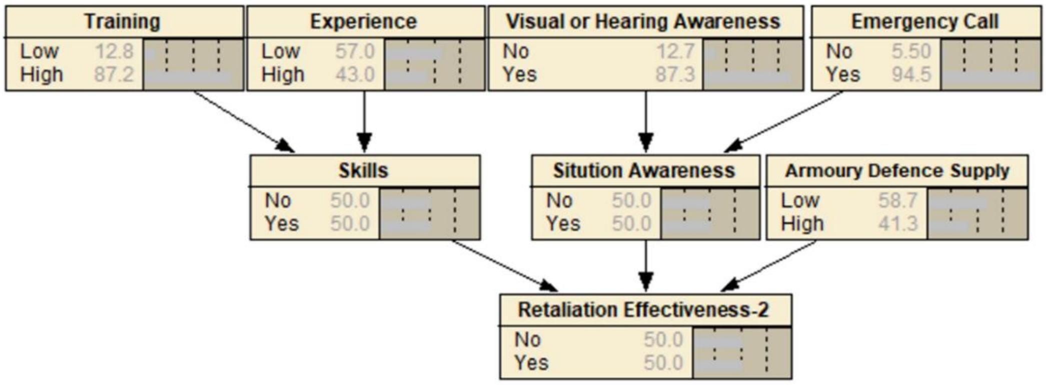


Figure 4.10: The BN model representing the Retaliation Effectiveness or Security Port Countermeasures – RE2 (Industry Expert)

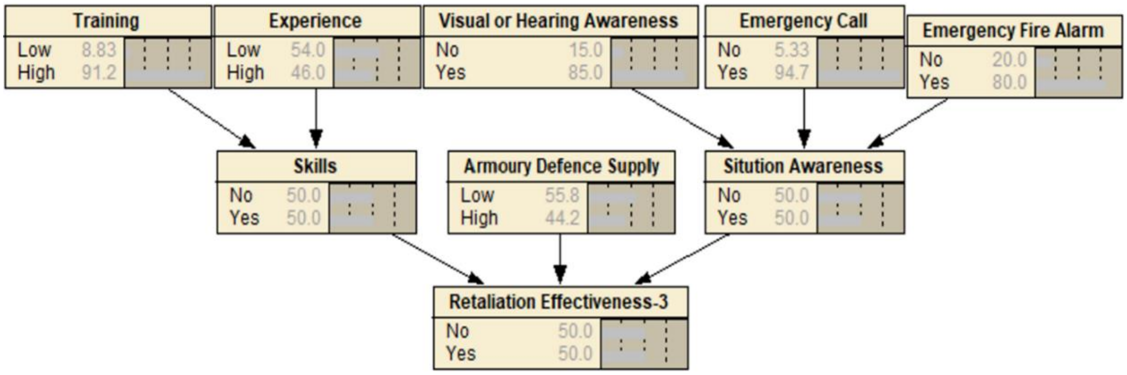


Figure 4.11: The BN model representing the Retaliation Effectiveness or Security Port Countermeasures – RE3 (Industry Expert)

A NETICA software (a BN method) was used to calculate the effectiveness of the port countermeasures. Figures 4.12 to 4.14 show the results after all the survey responses were keyed-in into the NETICA Software.

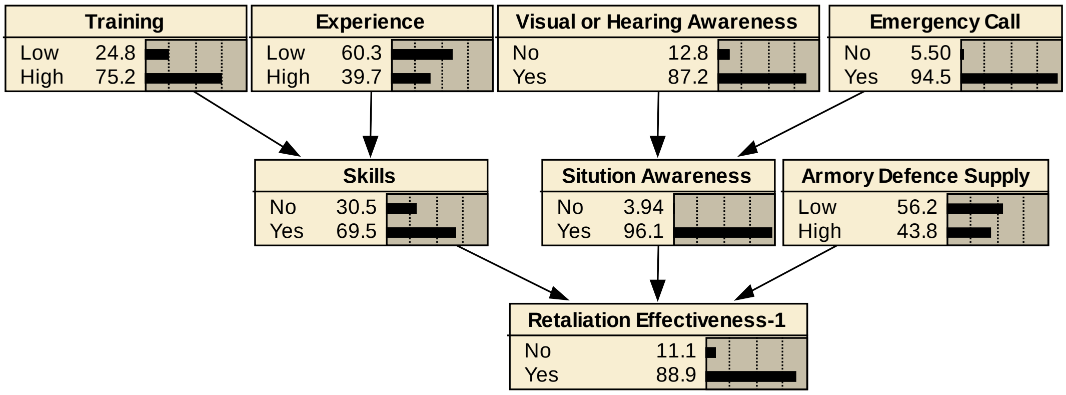


Figure 4.12: Result for Security Port Countermeasures - CM1 (Industry Expert)

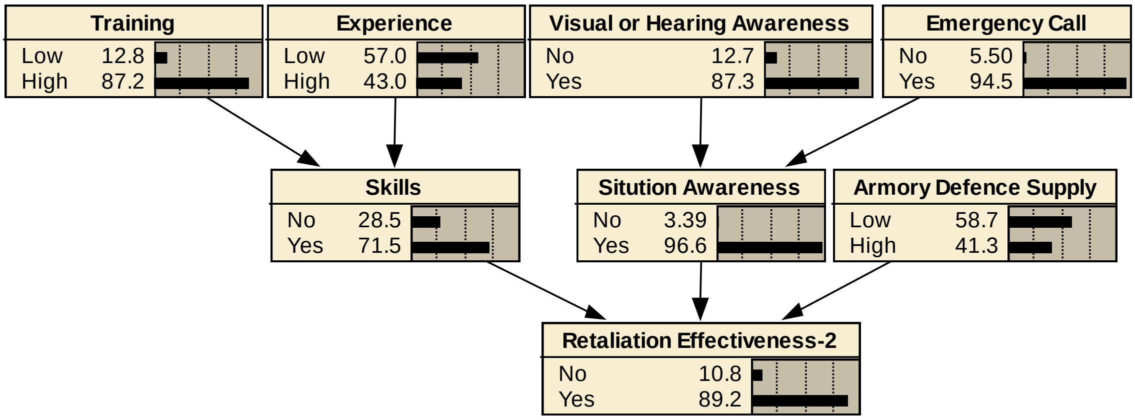


Figure 4.13: Result for Security Port Countermeasures - CM2 (Industry Expert)

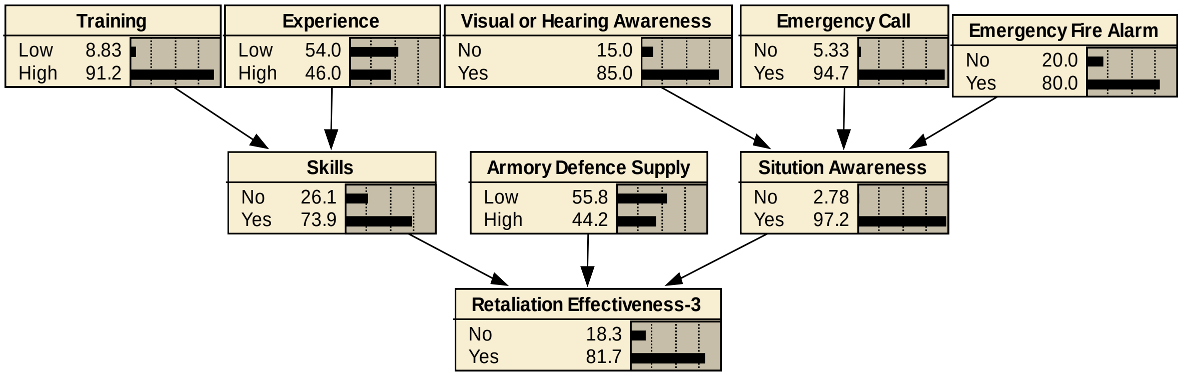


Figure 4.14: Result for Security Port Countermeasures - CM3 (Industry Expert)

The result of CM1 showed that 88.9% of retaliation effectiveness were YES (Figure 4.12). The port was not vulnerable to terrorist attacks, but there was a slight chance (11.1%) of the terrorist being able to attack the container wharf successfully. The CM2 result showed that

89.2% of retaliation effectiveness were YES (Figure 4.13). The port was not vulnerable to the danger of explosion; however, there was a slight chance (10.8%) that the terrorist will be able to attack the container wharf with explosion successfully. The CM3 result showed that 81.7% of retaliation effectiveness were YES (Figure 4.14). The port was not vulnerable to fires; however, there was a slight chance (18.3%) that the terrorist will be able to attack the container wharf by fire successfully.

Validation

If the model is sound and its reasoning logical, the results from the model must at least follow the following two axioms See 3.3 Methodology, Step 5 Sub-topic Validation.

Bayesian Inference for triple mini BN Models

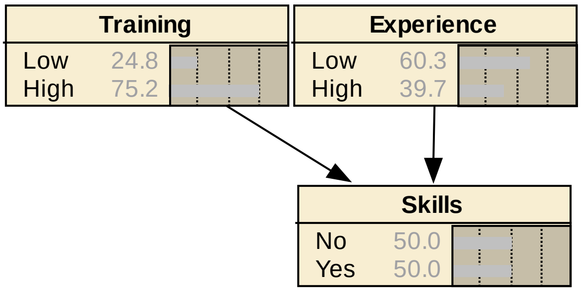


Figure 4.15: A Partial BN Model for Skills (Attack/Explosion/Fire), Training and Experience

R1 (Attack)

<table>
<tr>
<td>Training (Attack)
<table><tr><td>Low</td><td>0.2483</td></tr><tr><td>High</td><td>0.7517</td></tr></table>
For example, P (Training (Attack) - Low)
= 0.2483</td>
<td>Experience (Attack)
<table><tr><td>Low</td><td>0.6033</td></tr><tr><td>High</td><td>0.3967</td></tr></table>
For example, P (Experience (Attack) - Low)
= 0.6033</td>
</tr>
</table>

By using the conditional probability values given in the CPT for each node, the prior probability values can be obtained.

Table 4.15: R1-Skills (Conditional Probability)

	Training	Low		High	
	Experience	Low	High	Low	High
Skills	No	0.9983	0.2983	0.2267	0.0783
	Yes	0.0017	0.7017	0.7733	0.9219

For example, the prior probability value of the node “R1-Skills: No” is calculated as follows:

R1 - P (Skills: No) = ∑P (Training - Low, Training - High, Experience - Low, Experience - High) (4.3)

P (Skills: No) = (0.9983 × Training – Low × Experience - Low) + (0.2983 × Training – Low × Experience - High) + (0.2267 × Training – High × Experience - Low) + (0.0783 × Training – High × Experience - High)

P (Skills: No) = (0.9983 × 0.2483 × 0.6033) + (0.2983 × 0.2483 × 0.3967) + (0.2267 × 0.7517 × 0.6033) + (0.0783 × 0.7517 × 0.3967)

P (Skills: No) = 0.3050851

The same result obtained from Netica = Skills-No =0.305 thus 0.305≈0.3050851

The probability value of the node “Skills-No” is known to be 0.305 while the one for “Skills-Yes” is 1.000- 0.305=0.695. Such values can also be calculated using the Netica software tool, as shown in Figure 4.16- R1.

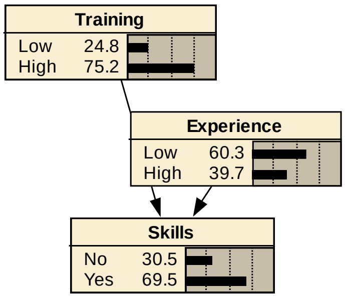


Figure 4.16: R1 - A Partial BN Model for R1- Skills: No, Training (Attack) and Experience (Attack)

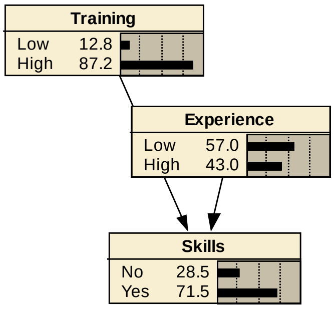


Figure 4.17: R2 - A Partial BN Model for R2- Skills: No, Training (Explosion) and Experience (Explosion)

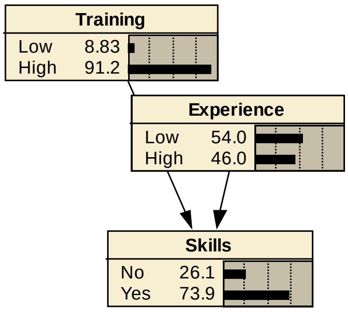


Figure 4.18: R3 - A Partial BN Model for R3- Skills: No, Training (Fire) and Experience (Fire)

R2 (Explosion)

Training (Explosion)		Experience (Explosion)	
Low	0.1283	Low	0.57
High	0.8717	High	0.43

For example, P (Training (Attack) - Low) = 0.1283	For example, P (Experience (Explosion) - Low) = 0.57

By using the conditional probability values given in the CPT for each node, the prior probability values can be obtained.

Table 4.16: R2-Skills (Conditional Probability)

	Training	Low		High	
	Experience	Low	High	Low	High
Skills	No	0.9983	0.355	0.2867	0.1333
	Yes	0.0017	0.645	0.7133	0.8667

For example, the prior probability value of the node "R2-Skills: No" is calculated as follows:

R2 - P (Skills: No) = ∑P (Training - Low, Training - High, Experience - Low, Experience - High) (4.4)

P (Skills: No) = (0.9983 × Training - Low × Experience - Low) + (0.355 × Training - Low × Experience - High) + (0.2867 × Training - High × Experience - Low) + (0.1333 × Training - High × Experience - High)

P (Skills: No) = (0.9983 × 0.1283 × 0.57) + (0.355 × 0.1283 × 0.43) + (0.2867 × 0.8717 × 0.57) + (0.1333 × 0.8717 × 0.43)

P (Skills: No) = 0.285009

The same result obtained from Netica = Skills-No =0.285 thus 0.285≈0.285009

The probability value of the node "Skills-No" is known to be 0.285 while the one for "Skills-Yes" is 1.000- 0.285=0.715. Such values can also be calculated using the Netica software tool, as shown in Figure 4.17-R2.

R3 (Fire)

<table>
<tr>
<td>Training (Fire)
<table><tr><td>Low</td><td>0.0883</td></tr><tr><td>High</td><td>0.9117</td></tr></table>
For example, P (Training (Attack) - Low) = 0.0883</td>
<td>Experience (Fire)
<table><tr><td>Low</td><td>0.54</td></tr><tr><td>High</td><td>0.46</td></tr></table>
For example, P (Experience (Fire) - Low) = 0.54</td>
</tr>
</table>

By using the conditional probability values given in the CPT for each node, the prior probability values can be obtained.

Table 4.17: R3-Skills (Conditional Probability)

	Training	Low		High	
	Experience	Low	High	Low	High
Skills	No	1.00	0.3517	0.2867	0.1383
	Yes	0.00	0.6483	0.7133	0.8617

For example, the prior probability value of the node "R3-Skills: No" is calculated as follows:

R3 - P (Skills: No) = ∑P (Training - Low, Training - High, Experience - Low, Experience - High) (4.5)

P (Skills: No) = (1.00 × Training - Low × Experience - Low) + (0.3517 × Training - Low × Experience - High) + (0.2867 × Training - High × Experience - Low) + (0.1383 × Training - High × Experience - High)

P (Skills: No) = (1.00 × 0.0883 × 0.54) + (0.3517 × 0.0883 × 0.46) + (0.2867 × 0.9117 × 0.54) + (0.1383 × 0.9117 × 0.46)

P (Skills: No) = 0.2611155

The same result obtained from Netica = Skills-No =0.261 thus 0.261≈0.2611155

The probability value of the node "Skills-No" is known to be 0.261 while the one for "Skills-Yes" is 1.000- 0.261=0.739. Such values can also be calculated using the Netica software tool, as shown in Figure 4.18-R3.

R1 – result

The process of computing the prior probability value of node Skill is called pre-posterior analysis. To continue, a piece of evidence is entered to the node "Training (Attack) *absolute High*" with the purpose of determining the updated posterior probability values of the node "Skills". The posterior probability value of the node "Skills-*NO*" given "Training (Attack) *absolute High*" is computed using Equation 4.6.

1. Training (Attack) *absolute High*

Low	0.0
High	1.0

2. Experience (Attack)

Low	0.6033

High	0.3967

For example, P (Experience -High (Attack)) =0.3967

3. Skills (Attack)

Training	Low		High	
Experience	Low	High	Low	High
No	0.9983	0.2983	0.2267	0.0783
Yes	0.0017	0.7017	0.7733	0.9219

Equation 4.2-R1

$$\text{P (Skills} - \text{Yes} \mid \text{Training absolute High)} = \frac{\text{P (Training}-\text{High,Skills}-\text{Yes)}}{\text{P (Training}-\text{High)}} \tag{4.6}$$

$$\text{P (Skills} - \text{Yes} \mid \text{Training absolute High)}$$
$$= \frac{\sum \text{P (Training} - \text{High, Experience} - \text{Low, Experience} - \text{High)}}{\text{P (Training} - \text{High)}}$$

$$\text{P (Skills} - \text{Yes} \mid \text{Training absolute High)}$$
$$= \frac{(0.7017 \times \text{Training} - \text{High} \times \text{Experience} - \text{Low}) + (0.9219 \times \text{Training} - \text{High} \times \text{Experience} - \text{High})}{1.0}$$

$$\text{P (Skills} - \text{Yes} \mid \text{Training absolute High)}$$
$$= \frac{(0.7733 \times 1 \times 0.6033) + (0.9219 \times 1 \times 0.3967)}{1.0}$$

$$\text{P (Skills} - \text{Yes} \mid \text{Training absolute High)} = 0.83225$$

After giving a piece of evidence to the node Training absolute High in Figure R1-3.17, the result shows that the new posterior probability value of the node “Skills − Yes” increased from 0.695 (See Figure 4.19) to 0.832≈0.83225.

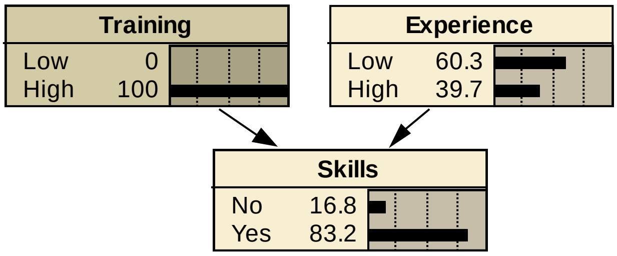


Figure 4.19: A Partial BN Model for Skills Attack, Absolute-High Training and Experience

R2 – result

The process of computing the prior probability value of node Skill is called pre-posterior analysis. To continue, a piece of evidence is entered to the node "Training (Explosion) *absolute High*" with the purpose of determining the updated posterior probability values of the node "Skills". The posterior probability value of the node "Skills-*NO*" given "Training (Explosion) *absolute High*" is computed using Equation 4.7.

1. Training (Attack) *absolute High*

Low	0.0
High	1.0

2. Experience (Attack)

Low	0.57
High	0.43

For example, P (Experience -High (Attack)) =0.43

3. Skills (Attack)

Training	Low		High	
Experience	Low	High	Low	High
No	0.9983	0.355	0.2867	0.1333
Yes	0.0017	0.645	0.7133	0.8667

Equation 4.2-R1

$$\mathrm{P\ (Skills - Yes} \mid \mathrm{Training\ absolute\ High)} = \frac{\mathrm{P\ (Training{-}High, Skills{-}Yes)}}{\mathrm{P\ (Training{-}High)}} \qquad (4.7)$$

$$\mathrm{P\ (Skills - Yes} \mid \mathrm{Training\ absolute\ High)}$$
$$= \frac{\sum \mathrm{P\ (Training - High, Experience - Low, Experience - High)}}{\mathrm{P\ (Training - High)}}$$

$$\mathrm{P\ (Skills - Yes} \mid \mathrm{Training\ absolute\ High)}$$
$$= \frac{(0.7133 \times \mathrm{Training - High} \times \mathrm{Experience - Low}) + (0.8667 \times \mathrm{Training - High} \times \mathrm{Experience - High})}{1.0}$$

$$\mathrm{P\ (Skills - Yes} \mid \mathrm{Training\ absolute\ High)} = \frac{(0.7133 \times 1 \times 0.57) + (0.8667 \times 1 \times 0.43)}{1.0}$$

$$\mathrm{P\ (Skills - Yes} \mid \mathrm{Training\ absolute\ High)} = 0.779262$$

After giving a piece of evidence to the node Training absolute High, the result shows that the new posterior probability value of the node "Skills − Yes" increased from 0.715 (See Figure 4.20) to 0.779≈0.779262

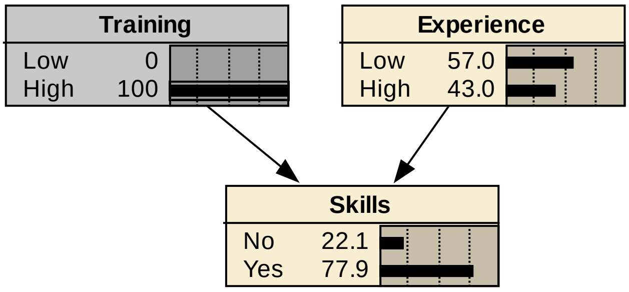


Figure 4.20: A Partial BN Model for Skills Explosion, Absolute-High Training and Experience

R3-Result

The process of computing the prior probability value of node Skill is called pre-posterior analysis. To continue, a piece of evidence is entered to the node “Training (Fire) *absolute High*” with the purpose of determining the updated posterior probability values of the node “Skills”. The posterior probability value of the node “Skills-*NO*” given “Training (Fire) *absolute High*” is computed using Equation 4.8.

1. Training (Attack) *absolute High*

Low	0.0
High	1.0

2. Experience (Attack)

Low	0.54
High	0.46

For example, P (Experience -High (Attack)) =0.46

3. Skills (Attack)

Training	Low		High	
Experience	Low	High	Low	High
No	1.00	0.3517	0.2867	0.1383
Yes	0.00	0.6483	0.7133	0.8617

Equation 4.2-R1

$$\mathrm{P}\ (\mathrm{Skills}-\mathrm{Yes}\,|\,\mathrm{Training\ absolute\ High}) = \frac{\mathrm{P}\ (\mathrm{Training}-\mathrm{High},\mathrm{Skills}-\mathrm{Yes})}{\mathrm{P}\ (\mathrm{Training}-\mathrm{High})} \qquad (4.8)$$

$$\mathrm{P}\ (\mathrm{Skills}-\mathrm{Yes}\,|\,\mathrm{Training\ absolute\ High})$$
$$= \frac{\sum \mathrm{P}\ (\mathrm{Training}-\mathrm{High},\mathrm{Experience}-\mathrm{Low},\mathrm{Experience}-\mathrm{High})}{\mathrm{P}\ (\mathrm{Training}-\mathrm{High})}$$

$$P\ (\text{Skills} - \text{Yes} \,|\, \text{Training absolute High}) = \frac{(0.7133 \times \text{Training} - \text{High} \times \text{Experience} - \text{Low}) + (0.8617 \times \text{Training} - \text{High} \times \text{Experience} - \text{High})}{1.0}$$

$$P\ (\text{Skills} - \text{Yes} \,|\, \text{Training absolute High}) = \frac{(0.7133 \times 1 \times 0.54) + (0.8617 \times 1 \times 0.46)}{1.0}$$

$$P\ (\text{Skills} - \text{Yes} \,|\, \text{Training absolute High}) = 0.781564$$

After giving a piece of evidence to the node Training absolute High, the result shows that the new posterior probability value of the node "Skills − Yes" increased from 0.739 (See Figure 4.21) to 0.782≈0.781564.

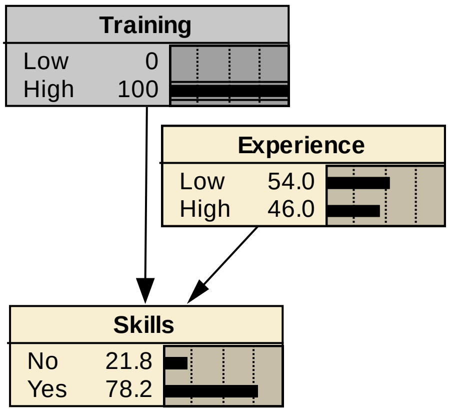


Figure 4.21: A Partial BN Model for Skills Fire, Absolute-High Training and Experience

Sensitivity Analysis

Detail of Sensitivity Analysis for Bayesian Network can be seen in 3.3 Methodology, Step 7 Sub-topic Sensitivity Analysis.

This step discusses the robustness of the BN model through sensitivity analysis. This is a very useful technique to identify the most sensitive parameter of a network. Besides, the sensitivity analysis also describes the functional relation between the parameter and the probability of the hypothesis. This can be used to compute the impact of different variations in the parameter value. The purpose of this step is to analyse how sensitive is the terrorist model about an attack on the port when there are changes in parameters or inputs.

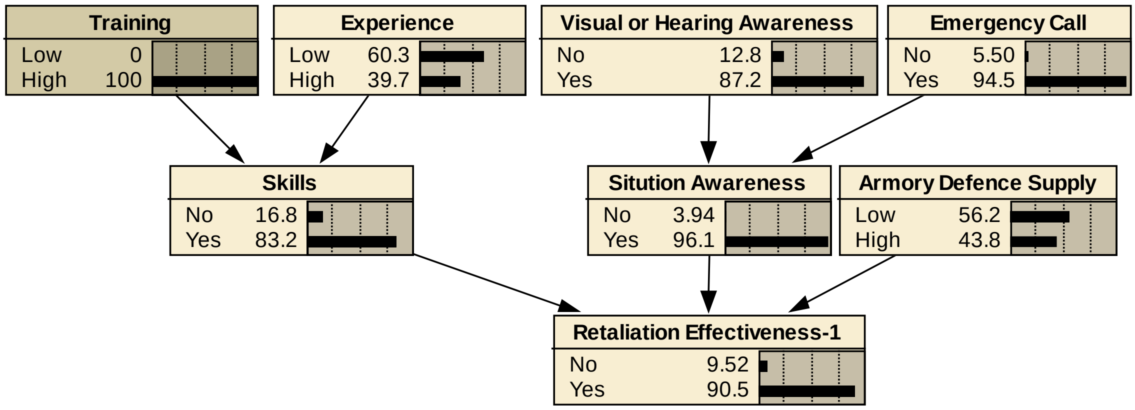


Figure 4.22: The BN model representing the Retaliation Effectiveness or Security Port Countermeasures - R1 (Absolute-Yes)

To conduct the sensitivity analysis, one output node "Skills" and two input nodes "Training", and "Experience" were used. One of the input nodes will be given different variations in probability values. If the output node is not influenced by an input node, then the input node is considered to be insignificant and has to be eliminated. Thus, further investigation is required for this situation. For example, by giving 100% of probability of High to the node "Training" = [Absolute "High"], the posterior probability value of the node "Skills -Yes" increases from 69.5% to 83.2%. This means that the output node of this model was sensitive to the probability changes of the input nodes.

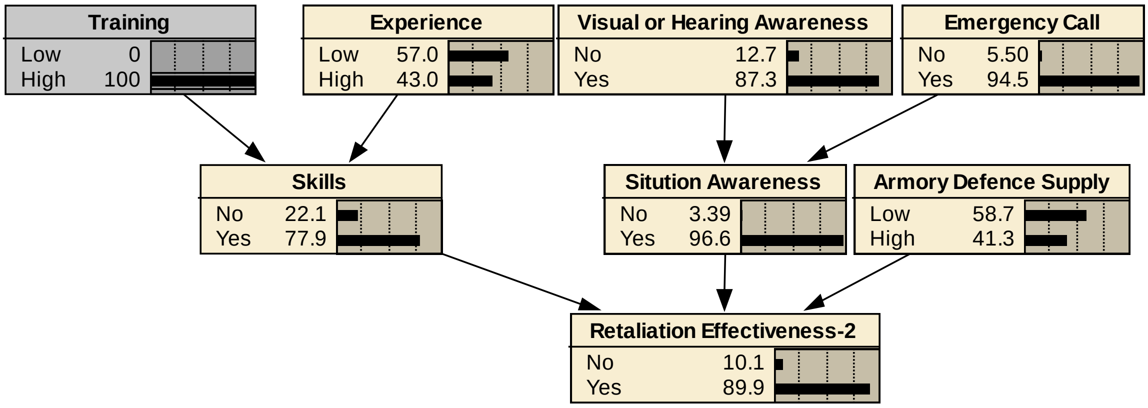


Figure 4.23: The BN model representing the Retaliation Effectiveness or Security Port Countermeasures – R2 (Absolute-Yes)

By giving 100% of probability of High to the node "Training" =[Absolute "High"], the posterior probability value of the node "Skills -Yes" increases from 71.5% to 77.9%. This means that the output node of this model was sensitive to the probability changes of the input nodes.

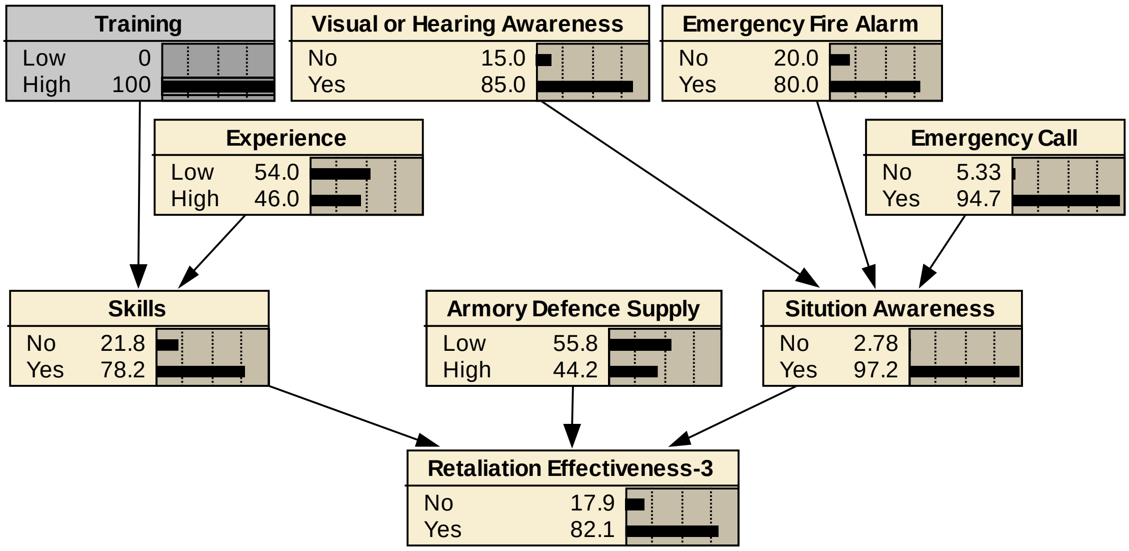


Figure 4.24: The BN model representing the Retaliation Effectiveness or Security Port Countermeasures – R3 (Absolute-Yes)

By giving 100% of probability of High to the node "Training" = [Absolute "High"], the posterior probability value of the node "Skills -Yes" increases from 73.9% to 78.2%. This means that the output node of this model was sensitive to the probability changes of the input nodes.

[2] The event probabilities

In this study, the researcher also co-opts three academician who specialise in maritime studies and have working experience in or with the maritime industries for more than 5 to 20 years. They agree to answer the questionnaires except for the section on opinions related to security since they did not have the information sought for. However, their opinions were still valued as a counterweight to the opinion of industry experts.

Table 4.18: The demographic and result for event success and failure probabilities (academician)

Result		R1	R2	R3
1	Age	42	32	51
2	Experience	16	4	30
3	The Scope of Job	Academic	Academic	Academic

Table 4.19: Result from Academic Expert for Countermeasure success and failure probabilities

No		Arithmetic average	[Negative average]
4	Explosion	63.00	37.00
5	Fire	43.00	57.00
6.1	Damages Injuries	42.67	57.33
6.2	Damages Death	36.33	63.67

Results from the survey and questionnaire showed that the chance of explosions happening was 63% and the chance that it will not happen was 37%. As for fires, there was 43% chance that it will happen and 57% chance that it will not happen. In the case of damage, injuries and loss of life, damage to properties were not calculated or included due to time constraints and the inability on the part of the Port under study to grant access to the related financial information. Damage arising from injuries were put as the first followed by the loss of life. Hence, there is no loss of life if there is no injury. The probability of injuries happening was 42.67% and 57.33% not happening. The probability of damage arising out of loss of life was 36.33% that it will happen and 63.67% that it will not.

Step 5: Identify and evaluate the outcome risk then recommend corrective action

The next step in the qualitative part of the analysis is to describe the different event sequences arising from the initiating event and calculate the overall probability of the event paths, and hence determine the risks. Another sequence represents a retaliation effectiveness or countermeasure effectiveness.

The first initiating event was not included in the questionnaires since the study was conducted under the assumption that the terrorists will attack the port with 100% surety. However, the countermeasures gave very interesting results that there would be minimal damage if the terrorists attack the wharf operation site since the port police and security are capable of thwarting the attack (with 88.9% probability of success). This high probability may come from training and experience event-states in which skills come up to 69.5% and situation awareness comes to 96.1%, both compensating the low score in the armoury defence supply (43.8%). If the port operator decides to have a high volume of armoury defence supply, it might boost up the success of countermeasures even higher.

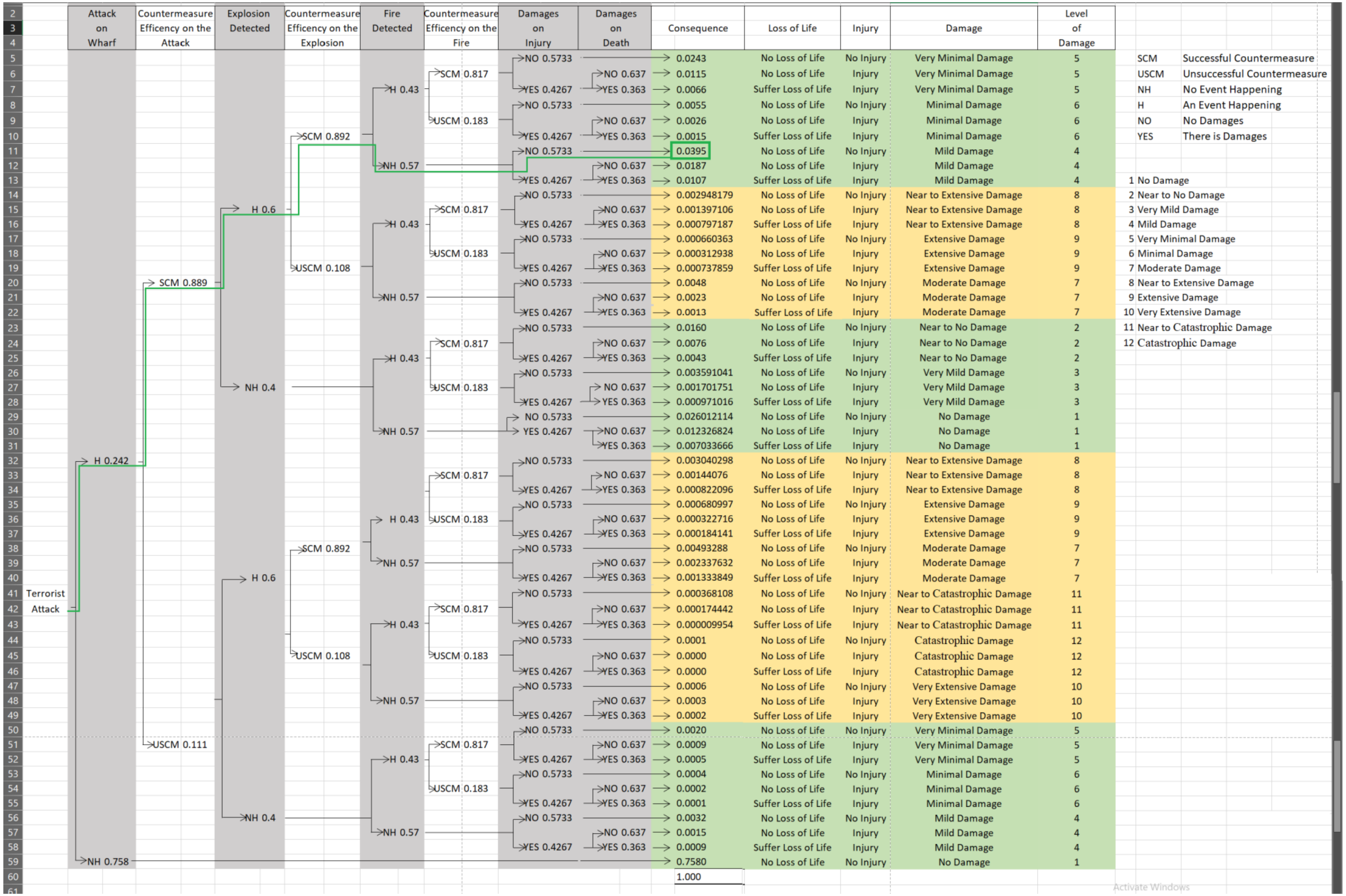
Furthermore, the strategic location of the port contributes to the ‘success’ percentage too since it is difficult for an outsider to enter the port without help from locals. If they come in without local captains, the vessel may be easily grounded since the sea depths at the port are unpredictable.

This particular port also has a unique requirement in staff recruitment, that is, priorities for employment were given to ex-servicemen from the military or candidates with military training or experience. Around 35% of its employees had training in using firearms and were able to act if any attacks were to happen. This port was also located near a police station (about 20 minutes away) and a military camp (about 38 minutes away). The fact that the port is near a military camp also explains why it has moderate armoury defence supply. Being in close proximity to the police station and the military camp, the port police and employees can afford to hold on for up to 30 minutes in a terrorist attack before assistance comes. Oversupply in the armoury may become a double edge sword in case the terrorists break into the port armoury defence supply and use the seized weapons to inflict damage to the port facilities and people.

The normal ETA is not as complex as this pioneer and huge ETA. Normally, an ETA has the initiating event such as fire, then the countermeasures coming. The first countermeasure starts with fire being detected, then the fire alarms start blaring, the sprinkler system starts, and in the end minimising the consequence of the fire.

In constructing this complex ETA, three initiating events were incorporated in one ETA. Events are [1] attacks from terrorists, [2] explosions and [3] fires. The countermeasures were so big that they must be calculated separately by using BN. However, the ETA was still too complex and may confuse readers. To overcome this problem, two colours were incorporated inside the ETA to allow easier understanding. Green consequence indicates "successful" security countermeasure facing all these initial events and orange-yellow indicates "failed" (or failure in) security countermeasure facing all these initial events (Figure 4.25).

The second and the third initiating events which were the explosions and fires were put in that sequence because explosions are far more deadly than fires. The difference between explosions and fires is the rates of physical and chemical processes happening during explosions are much faster than those happening during fires. This is because, during a fire, air and fuel are separated, while in an explosion the air and fuel are pre-mixed. Even though explosions have similar properties to fire such as producing flames, intense heat and high temperatures, explosions produce blasts, damaging and destructive pressure or shock waves, and sometimes they produce high-velocity fragments (that scatter to every directions) caused by bursting equipment (Lemkowitz, 2014).



Consequence	Loss of Life	Injury	Damage	Level of Damage
0.0243	No Loss of Life	No Injury	Very Minimal Damage	5
0.0115	No Loss of Life	Injury	Very Minimal Damage	5
0.0066	Suffer Loss of Life	Injury	Very Minimal Damage	5
0.0055	No Loss of Life	No Injury	Minimal Damage	6
0.0026	No Loss of Life	Injury	Minimal Damage	6
0.0015	Suffer Loss of Life	Injury	Minimal Damage	6
0.0395	No Loss of Life	No Injury	Mild Damage	4
0.0187	No Loss of Life	Injury	Mild Damage	4
0.0107	Suffer Loss of Life	Injury	Mild Damage	4
0.002948179	No Loss of Life	No Injury	Near to Extensive Damage	8
0.001397106	No Loss of Life	Injury	Near to Extensive Damage	8
0.000797187	Suffer Loss of Life	Injury	Near to Extensive Damage	8
0.000660363	No Loss of Life	No Injury	Extensive Damage	9
0.000312938	No Loss of Life	Injury	Extensive Damage	9
0.000737859	Suffer Loss of Life	Injury	Extensive Damage	9
0.0048	No Loss of Life	No Injury	Moderate Damage	7
0.0023	No Loss of Life	Injury	Moderate Damage	7
0.0013	Suffer Loss of Life	Injury	Moderate Damage	7
0.0160	No Loss of Life	No Injury	Near to No Damage	2
0.0076	No Loss of Life	Injury	Near to No Damage	2
0.0043	Suffer Loss of Life	Injury	Near to No Damage	2
0.003591041	No Loss of Life	No Injury	Very Mild Damage	3
0.001701751	No Loss of Life	Injury	Very Mild Damage	3
0.000971016	Suffer Loss of Life	Injury	Very Mild Damage	3
0.026012114	No Loss of Life	No Injury	No Damage	1
0.012326824	No Loss of Life	Injury	No Damage	1
0.007033666	Suffer Loss of Life	Injury	No Damage	1
0.003040298	No Loss of Life	No Injury	Near to Extensive Damage	8
0.00144076	No Loss of Life	Injury	Near to Extensive Damage	8
0.000822096	Suffer Loss of Life	Injury	Near to Extensive Damage	8
0.000680997	No Loss of Life	No Injury	Extensive Damage	9
0.000322716	No Loss of Life	Injury	Extensive Damage	9
0.000184141	Suffer Loss of Life	Injury	Extensive Damage	9
0.00493288	No Loss of Life	No Injury	Moderate Damage	7
0.002337632	No Loss of Life	Injury	Moderate Damage	7
0.001333849	Suffer Loss of Life	Injury	Moderate Damage	7
0.000368108	No Loss of Life	No Injury	Near to Catastrophic Damage	11
0.000174442	No Loss of Life	Injury	Near to Catastrophic Damage	11
0.000009954	Suffer Loss of Life	Injury	Near to Catastrophic Damage	11
0.0001	No Loss of Life	No Injury	Catastrophic Damage	12
0.0000	No Loss of Life	Injury	Catastrophic Damage	12
0.0000	Suffer Loss of Life	Injury	Catastrophic Damage	12
0.0006	No Loss of Life	No Injury	Very Extensive Damage	10
0.0003	No Loss of Life	Injury	Very Extensive Damage	10
0.0002	Suffer Loss of Life	Injury	Very Extensive Damage	10
0.0020	No Loss of Life	No Injury	Very Minimal Damage	5
0.0009	No Loss of Life	Injury	Very Minimal Damage	5
0.0005	Suffer Loss of Life	Injury	Very Minimal Damage	5
0.0004	No Loss of Life	No Injury	Minimal Damage	6
0.0002	No Loss of Life	Injury	Minimal Damage	6
0.0001	Suffer Loss of Life	Injury	Minimal Damage	6
0.0032	No Loss of Life	No Injury	Mild Damage	4
0.0015	No Loss of Life	Injury	Mild Damage	4
0.0009	Suffer Loss of Life	Injury	Mild Damage	4
0.7580	No Loss of Life	No Injury	No Damage	1
1.000				

SCM	Successful Countermeasure
USCM	Unsuccessful Countermeasure
NH	No Event Happening
H	An Event Happening
NO	No Damages
YES	There is Damages

1	No Damage
2	Near to No Damage
3	Very Mild Damage
4	Mild Damage
5	Very Minimal Damage
6	Minimal Damage
7	Moderate Damage
8	Near to Extensive Damage
9	Extensive Damage
10	Very Extensive Damage
11	Near to Catastrophic Damage
12	Catastrophic Damage

Figure 4.25: The ETA Result and the Outcomes

The percentage of explosions happening was high at 63% chance of happening and 37% of not happening at all. This may be factored by the fact that terrorist attacks are not familiar occurrences but the port authorities have confidence in the ability of the countermeasures to tackle explosions with 89% "successful" in controlling the explosions and 11% "failed". This latter figure may be due to the experience they already possess in handling chemicals and dangerous goods. For fires, the chance of them happening was moderate, at 43% and 57% chance of not happening. The countermeasures were high too with 82% "successful" and only 18% chance of failure.

Table 4.20: The ETA's Descriptions of Element State

Different Elements in ETA	Abbreviation	Descriptions of The Element State
Countermeasure	SCM	Successful Countermeasure
	USCM	Unsuccessful Countermeasure
Initiating Event	NH	No Event Happening
	H	An Event Happening
Damages	NO	No Damages
	YES	There is Damage

Table 4.21: The Level and Description of Level of Damage

Level of Damage	Description of Level of Damage
1	No Damage
2	Near to No Damage
3	Very Mild Damage
4	Mild Damage
5	Very Minimal Damage
6	Minimal Damage
7	Moderate Damage
8	Near to Extensive Damage
9	Extensive Damage
10	Very Extensive Damage
11	Near to Catastrophic Damage
12	Catastrophic Damage

Table 4.22: The Outcomes % Successful Security Counter Measure Facing All Initial Events versus Failure Security Counter Measure Facing All Initial Events

The Successful Security Counter Measure Facing All Initial Events	The Failure Security Counter Measure Facing All Initial Events	Total
(0.889+0.892+0.817)÷3=0.866	1 - 0.866 = 0.134	1.00

Below is an example of how to calculate the ETA manually, where P_7represents probability of consequence number 7, $P_{1\mathrm{E}}, P_{2\mathrm{E}}$ and $P_{3\mathrm{E}}$ represent probability of the three initiating events (which were initiating event for an attack, initiating event for explosion and initiating event for fire), $P_{1\mathrm{S}}$and$P_{2\mathrm{S}}$ represent the successful countermeasure probability ($P_{3\mathrm{S}}$ was not included in the probability of consequence number 7, where it does not need countermeasure for fire since the fire event does not happen, see Figure 4.25) and $P_{1\mathrm{D}}$and$P_{2\mathrm{D}}$ represent probability of the damage of injury and loss of life.

$$P_7 = (P_{1\mathrm{E}} \times P_{1\mathrm{S}} \times P_{2\mathrm{E}} \times P_{2\mathrm{S}} \times P_{3\mathrm{E}} \times P_{1\mathrm{D}} \times P_{2\mathrm{D}}) \quad (4.9)$$

$$P_7 = (\text{Terrorist Attack} \times \text{CEA} *\times \text{Explosion} \times \text{CEE} **\times \text{Fire} \times \text{DOI} ***\times \text{DOD} ****)$$

$$P_7 = (0.242 \times 0.889 \times 0.63 \times 0.892 \times 0.57 \times 0.5733)$$

$$P_7 = 0.0395074799368 \approx 0.0395$$

Tables 4.23: The Description of Example on How to Calculate the ETA Manually

*, **, ***, ****	Description
CEA*	Countermeasure Efficiency on the Terrorist Attack
CEE**	Countermeasure Efficiency on the Explosion
DOI***	Damage on Injury
DOD****	Damage on Death

Based on the results from the ETA Model of countermeasure effectiveness, the highest result showed that there was 75.8% chance the subjected port receives no damage with no injury and no loss of life (Figure 4.25). The chances were high in the beginning since the results were taken from the previous chapter. The second highest result was the 3.95% chance the subjected port receives mild damage with no injury and no loss of life.

4.4 Conclusion

The structure of the diagram, which clearly showed the progression of the attack and countermeasures, helps the researcher to specify where security or safety systems will be most effective in protecting against these accidents. However, the result from this chapter revealed that the countermeasures were excellent, and there were small chances of damage, injury and death occurring should the terrorists decide to attack this seaport.

In the previous chapter, the study conducted on the probability of a terrorist attack at port facilities showed that wharf-on-site [WOS] had the highest likelihood of getting attacked by terrorists with the highest possible damages inflicted on the port and the state economy.

There were a few possible attack methods, such as hijacking a vessel and crashing it onto the wharf or installing explosives on the vessel that will explode when it crashes. That chapter also took the next logical step by listing three possible main events that may cause high damages to the sea port. Those damaging events were terrorist attacks (ram into the wharf and an attack using weapons), explosions (install an explosive on the vessel that will set-off during a collision, rocket-propelled grenades or hand grenades) and fires (flame thrower, fire after an explosion or arson). The port operator is expected to counter the attacks via countermeasures, which are called attack security countermeasures, explosion security countermeasures and fire security countermeasures, respectively. These events can happen independently, or a combination of any of them. To measure the consequences experienced by the port facilities, the BN and ETA were used. The results showed how little damage the port may experience if attacked by terrorists. This showed the effectiveness of the port security system based on expert judgements.

Chapter 5: Ranking the Security Effectiveness by Using Analytic Hierarchy Process and Evidential Reasoning

Summary

This chapter focuses on estimating the cost and benefits of port security by ranking up the security countermeasures listed by using an Analytic Hierarchy Process (AHP) approach and synthesising the outcome by using an Evidential Reasoning (ER) approach. This chapter is an extension from the previous chapter which estimates the consequences of a terrorist attack and the role of the existing security countermeasures. Since the previous result indicated the success of the existing countermeasures, this chapter will further explore the security effectiveness as a whole and not just countermeasures on the terrorist attack at the wharf. The countermeasures will be listed in hierarchical order starting with the main criteria followed by the sub-criteria. Most of the items in the main criteria are from a combination of general security functions coupled with security costs. Sub-criteria items are the equipment, training, programmes, expenses and methods used in security operations. All criteria (and the sub-criteria) will be ranked according to the order of their importance. After the experts decided on the ranking in descending order of their importance, each criteria and sub-criteria will be assigned with three alternative countermeasures (High-Tech, Low-Tech and No-Tech categories of security measures) and these alternatives are chosen according to the belief degree on which is the best for the port safety.

5.1 Introduction

This chapter consists of an understanding of what makes a security countermeasure effective or not, the function of security countermeasures, the elements of specific security countermeasures, and how to rank specific countermeasures using AHP and ER approaches to help decision makers a choice. Security countermeasures are not very popular from the seaport stakeholders' point of view since they (countermeasures) cost a lot of money and the higher the degree of security measures employed, the longer will be the operations time and possible delay. On the other hand, having an effective security system would decrease the monthly insurance expenses, conform to the government safety requirements, increase customer confidence and keep the company reputation intact.

5.1.1 The Function of Security Countermeasure

There are seven things that security countermeasures, in general, hope to do (security countermeasure functions) which are access control, deterrence, detection, assessing the attack, delaying the attack, responding to the attack and collecting evidence of the attack (Norman, 2010).

All security countermeasures had a few goals of manipulating the behaviour of potential threats in order to eliminate the threats directed at the organisation. There are three main goals and the first one is to actively identify the threat and deny any possible access to the organisation, such as identifying unresponsive and suspicious vessels (that may indicate them being hijacked by terrorists) and deny them access, or stop them from coming close to the port. Secondly, to deny any party access to weapons, explosives and dangerous chemicals except for legitimate purposes and for that, the items should be well controlled and monitored. The third and last goal is to make the environment suitable for appropriate behaviour, unsuitable for inappropriate or terroristic behaviour, and mitigate any hostile actions or threats. If all these three goals are achieved then the security measures of the port are considered effective.

There are strategies that can be implemented to achieve the stated goals such as to control the access to the port compound at the port gate (using high security barriers such as deployable bollards, phalanx barriers, and crash rated barriers). Wherever possible, deterring a threat from becoming reality would be the best way of any security countermeasure. As an example, Malaysia, Indonesia and Singapore have between them an agreement to fight piracy within their shared sea parameter such as the Straits of Malacca (Bradford, 2004, See 3.3 step 3.1). A good counter-surveillance is important to deter a terrorist attack and such surveillance includes ample use of boat surveillance on the seaward parameter near the wharf and the exterior spaces outside the port compound.

When a threat of an attack is detected, it is important to assess whether that threat is real, or just a false alarm. Video surveillance cameras can be used to confirm an alarm when the presence of an intruder can be seen on camera. Once the threat of an attack is confirmed, a response is needed. Responses to the threats (for the port security staff) may be in the form of not taking any direct action against the actors, in countering the threats, or trying to minimise any potential harm to innocent people, or calling others, such as the military and external police forces, for help and to intervene directly against the attack including capturing the threat actors when the situation allows.

To establish an appropriate response for non-security staff, workers who are not involved in security countermeasures should have prior knowledge on what to do and where to go in the event of an attack (since they have undergone emergency drills for such an event and got information from announcements after the emergency alarm). This helps to create a scenario where people feel reassured and secure (since they know what to do to stay safe) and the security office can focus on protecting them. The next function is gathering evidence for an investigation into an attack and for the post event analysis resulting in scenario planning and training for later use.

5.1.2 Priority of the Security Programme

Before choosing the most effective security countermeasure, some issues need to be addressed. First, is the investment budget for the security which the port operator is willing to invest. The port management needs to consider the values of the assets and containers it is protecting. In addition to that, the security manager needs to gauge the willingness of, and to influence the upper management of the port to allocate the required finances for the port security. It is sometimes essential for the security office to have a direct reporting line (to the CEO) in order to succeed in achieving its goals. If for example, the security office is placed under the facilities management department, it will likely be treated as a normal unimportant department, similar to housekeeping and supplies, with the department heads struggling and competing among themselves for the small departmental budgets, regardless of the risks involved.

Second, the manager of the security department should be a trained security professional. This is important because the manager needs to understand the challenges of security management and its role in protecting the organisation. For any organisation with high security risks, the security department should have a direct line of reporting to the CEO. If not, communication between the CEO and the security office takes a longer and more indirect route through the departmental head and sometimes must pass through unnecessary filters that may dilute, distort, or delay its importance and hence its risks.

Finally, the head of security needs to have good communications with the IT department to ensure that smooth security systems and programmes are actually helping the security department. Both the IT and the security departments need to work together and share their concerns on the security systems to eliminate any confusion and insecure systems. Any glitches or system malfunctions need to be reported immediately since it may be an attack disguised as a system having a breakdown (Norman, 2010).

5.1.3 Security Countermeasure Alternatives

For the purpose of determining the effectiveness of security countermeasures, the countermeasures are classified into three types, namely the High-Technology Security Countermeasures (High-Tech), Low-Technology Security Countermeasures (Low-Tech) and No-Technology Security Countermeasures (No-Tech).

A. High Technology Security Countermeasure (High-Tech)

High-tech countermeasure focuses more on the electronic section of security countermeasures, commonly including access control systems, digital video systems, security alarm systems, two-way voice communications system, and the information technology security (Norman, 2010). Except for the guards, Hi-Tech elements are the most visible portions of the security countermeasure. It is possible to maximise the efficiency of High-Tech countermeasures if they are correctly designed. A well-designed security video system can support video surveillance, video guard "routine tours" (many more routine tours of the facility each hour than a walking guard can perform), and video pursuits (following a subject through the building). Besides providing or performing video surveillance, the system can also save thousands of dollars annually in guard costs in respect to control and alarm systems access.

B. Low Technology Security Countermeasure (Low-Tech)

Low-Tech countermeasures use non-digital and medium level of technology equipment, commonly used are locks, barriers, lighting, revolving doors and deployable barriers (Norman, 2010). They are cheaper than High-Tech and do not require much training to use or operate since they are not complex.

C. No Technology Security Countermeasure (No-Tech)

No-Tech countermeasures use rules and non-technology equipment to create an environment that discourages criminal activities and encourages safe and secure environment (Norman, 2010). No-Tech solutions include policies and procedures, security staffing, training, awareness programmes, emergency preparedness programmes, investigations, and security dogs.

These three types of solutions should be used in combination to address vulnerability issues in order to achieve multiple layers of protection. The most valuable assets should be protected by multiple layers of protection, from the outermost perimeter inwards. Listed below are the security countermeasure functions arranged according to the three security alternatives:

Table 5.1: Security Functions According to Countermeasure Alternatives

Security Countermeasure Function	High-Tech	Low-Tech	No-Tech
Access Control	• Card Technologies • Access Credential Reader Technologies • Consoles/Receptions • Security Command	• Locks • Revolving Doors • Mechanical and Electronic Turnstiles • Vehicle Gates	• Policies • Procedures • Trained Dogs • Law Enforcement

Deterring an Attack	• Photo Id Detectors • Security Management Office-Interview Room • Incorporate sensors in the layout	• Deployable Barriers • Lighting in the layout • Signage's	• CPTED Element • Deterrence Programmes
Detecting an Attack	• Property Perimeter Detection Systems • Building Perimeter Detection Systems • Interior Space Detection Systems • Point Detection Systems • Video Detection Systems • Security System Infrastructures • Security Digital Infrastructure	• Visual Device – binocular scope • Communication Device – Walkie Talkie • Vehicles Patrols – Surveillance Boat, Cars And Motorcycle	• Security Post • Routine Patrols • Routine Checks • Security Awareness Programmes
Assessing the Attack			
Delay the Attack	• Non-Lethal Weapon -Long Range Acoustic Device (LRAD) -Anti-Piracy Laser Beam -Tasers Guns –Electric Shock -Active Denial System – Pain Ray (Electromagnetic Wave) -Advanced Bomb Suit	• Non-Lethal Weapon -Water Cannon -Net- Boat Trap -Foul-Smelling Liquid -Rear Wire Canisters -Stun Grenade -Fire Engine -Explosive Ordnance Disposal (EOD) Suit -Bullet Proof Vehicles • Lethal Weapon -Armed Guard -Grenade (Bomb)	• Guard (Armed/Unarmed) • Security Vehicles Training Programmes • Emergency Preparedness Programmes • Disaster Recovery Programmes • Security Staffing
Responding to the Attack			
Collecting Evidence of the Attack.	•Record an audio and a video of an attack •Collect evidence of the attack for further legal action against the attackers and for insurance purposes		

5.1.4 Security Functions Novelty

In risk assessment and security countermeasure selection book (Norman, 2010) chapter 17 on subtopic of selection and budgeting tools, Norman has categorized the countermeasure into 7 function in which is access control, deterrence, detect attack, assessment, delay, respond and collecting the evidence. Given in the chapter, two illustration about the function of specific countermeasure's effectiveness measured based upon the threat it is against. In the simplistic examples below the category of countermeasures against generic criminal or terrorist threats.

Table 5.2: Criminal Threat Countermeasure Functions

Security Function	Alarm	Access Control	CCTV	Intercom	Barriers	Locks	Lighting	Landscape
Access Control		X			X	X		X
Deterrence	X	X	X		X	X	X	X
Detections	X	X	X					
Assessment		X	X	X			X	
Delay		X			X	X		X
Response		X	X	X			X	
Evidence	X	X	X					
Functions	3	6	5	2	2	2	3	2

Table 5.2 shows countermeasures that are effective against a terrorist threat with the more specific the threat, the more specific countermeasure can be estimated. Plus, specific countermeasure on specific location have varying degrees of effectiveness (Norman, 2010).

Table 5.3: Terrorist Threat Countermeasure Functions

Security Function	Alarm	Access Control	CCTV	Intercom	Barriers	Locks	Lighting	Landscape
Access Control					X			X
Deterrence					X			X
Detections	X		X					
Assessment			X	X			X	
Delay		X			X	X		X
Response			X				X	
Evidence	X	X	X					
Functions	2	2	4	1	2	1	2	2

There is a different score that can come out from the figure where in criminal threat most of the function score were high compare to the terrorist threat. This is because this countermeasure were not design specifically to counter terrorist on maritime but to counter terrorist in general. Thus, a new novel security function was developed to countermeasure the terrorist threat to maritime (See Figure 5.1). Further explanation will be directed to table 5.6 in this chapter and sub-topic 6.3.2 in chapter 6.

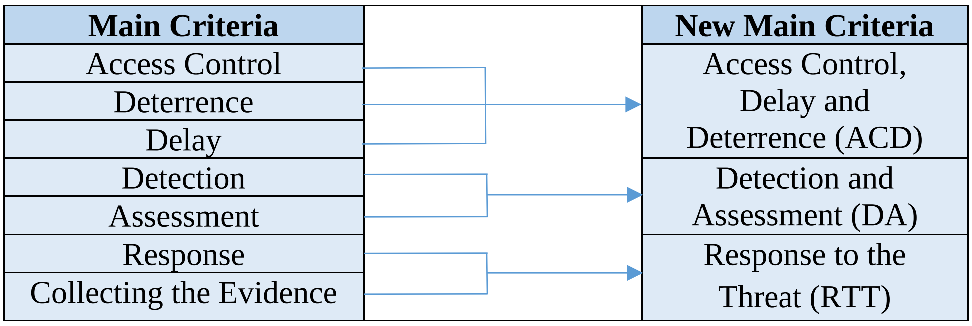


Figure 5.1: New Novel Security Function Was Developed To Countermeasure The Terrorist Threat

5.2 Background to the AHP and ER

The methods will be used in ranking the most effective countermeasures for the port. There are two main methods to be applied in this study, which are the AHP and the ER methods.

5.2.1 Analytic Hierarchy Process (AHP)

The basic scale adopted is a scale that captures individual preferences either in quantitative or qualitative forms (Saaty, 1980 and 1994). The scales compare the alternatives in respect of the criteria by using a fundamental scale such as "1" is "equally important", "2*", "3" is "a little important", "4*", "5" is "important", "6*", "7 is "very important", "8*", and "9 is "extremely important" and *(2, 4, 6, and 8 are intermediate values of "important"). The paired comparison scale between the comparing pair of two items (item i and item j) is as follows:

Table 5.4: Example of Scales Uses in AHP

item i	$^1/_9$	$^1/_8$	$^1/_7$	$^1/_6$	$^1/_5$	$^1/_4$	$^1/_3$	$^1/_2$	1	2	3	4	5	6	7	8	9	item j

A pair-wise comparison technique was used to find the weight of each of the criteria, by first, setting up n criteria in the row and column of a $n \times n$ matrix. Then, making comparisons to all the criteria by applying a ratio scale assessment (as shown in Table 5.5). This table contains two parts described in numerical numbers (together with their linguistic meanings). The left side explains the degree of "importants", while the right side explains the "unimportants" (Rahman, 2012).

Table 5.5: The Ratio Scales of Pair-Wise Comparison

Numerical Assessment	Linguistic Meanings	Numerical Assessment	Linguistic Meanings
1	Equally Important	1	Equally Important
2	Intermediate Values of Importance	1/2	Intermediate Values of Unimportance
3	A Little Important	1/3	A Little Unimportant
4	Intermediate Values of Importance	1/4	Intermediate Values of Unimportance
5	Important	1/5	Unimportant
6	Intermediate Values of Importance	1/6	Intermediate Values of Unimportance
7	Very Important	1/7	Very Unimportant
8	Intermediate Values of Importance	1/8	Intermediate Values of Unimportance
9	Extremely Important	1/9	Extremely Unimportant

The equation below shows the qualified judgements on pairs of attributes Ai and Aj are represented by a n×n matrix *A*.

$$\mathrm{A} = a_{ij} = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ a/a_{12} & 1 & \cdots & a_{2n} \\ . & . & \cdots & . \\ 1/a_{1n} & 1/a_{2n} & \cdots & 1 \end{bmatrix} \qquad (5.1)$$

Where, i=1,2,3,…,n and each aij relates to attribute Ai to attribute Aj.

For a matrix of order n, (n×(n−1)/2) comparisons are required. According to Pam (2010), the weight vector indicates the priority of each element in the pair-wise comparison matrix in terms of its overall contribution to the decision-making process. Such a weight value can be calculated by using Equation 5.2.

$$w_k = \frac{1}{n}\sum_{j=1}^{n}\left(\frac{a_{kj}}{\sum_{i=1}^{n} a_{ij}}\right) (k = 1,2,3, \ldots., n) \qquad (5.2)$$

Where, aij stands for the entry of row *i* and column *j* in a comparison matrix of order *n*.

The weight values obtained in the pair-wise comparison matrix were checked for consistency purposes by using Consistency Ratio (*CR*). The *CR* value was computed by using the following equations (Saaty, 1990):

$$CR=\frac{CI}{RI} \quad (5.3)$$

$$CI=\frac{\lambda_{max}-n}{n-1} \quad (5.4)$$

$$\lambda_{max} = \frac{\sum_{j=1}^{n}\frac{\sum_{k=1}^{n} w_k a_{jk}}{w_j}}{n} \quad (5.5)$$

Where, n is the number of items being compared, λmax stands for maximum weight value of the n×n comparison matrix, *RI* stands for average random index (Table 5.6) and *CI* stands for consistency index.

Table 5.6: Random Index (RI) Values

n	1	2	3	4	5	6	7	8	9	10
RI	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

CR is designed in such a way that a value greater than 0.10 indicates an inconsistency in pair-wise comparison. If *CR* is 0.10 or less, the consistency of the pair-wise comparisons is considered reasonable (Saaty, 1980).

5.2.2 Evidential Reasoning (ER) Overview

According to Yang and Xu (2002), supposedly there is a simple two-level hierarchy of attributes with a general attribute at the top level and a number of basic attributes at the bottom level. Supposed there are *L* basic attributes (i=1,2,…,L) associated with a general attribute y. Define a set of *L* basic attributes as follows:

$$E=\{e_1, \dots, e_i, \dots, e_L\} \quad (5.6)$$

Given weights (i=1,2,…,L) of the basic attributes, where, w_i is the relative weight of the i^{th} basic attribute (e_i) with $0 \leq w_i \leq 1$. Such weight values can be established through a pair-wise comparison involving the AHP approach as described in Step 6 of Section 5.3.

A given assessment for e_i(i=1,2,…,L) can be mathematically represented as shown in Equation 5.7 (Yang & Xu, 2002).

$$SC\,(e_i) = \{(M_n, \beta_{n,i}), n = 1,2, \dots, N\}, i=1,2,\dots,L, \quad (5.7)$$

Table 5.7: A Degree of Belief Level of Satisfying

E1	E2	E3	E4	E5
Worse	Poor	Average	Good	Best

Where, En is the nth evaluation grade and βn denotes a degree of belief satisfying, $\beta_{n,i} \geq 0$ and $\sum_{n=1}^{N} \beta_{n,i} \leq 1$. An assessment SC (e_i) is called complete (relatively, incomplete) if $\sum_{n=1}^{N} \beta_{n,i} = 1$ (respectively, $\sum_{n=1}^{N} \beta_{n,i} \leq 1$). For example, the three assessments are given as follows for demonstrating complete and incomplete assessments:

SC Security Staff Training of High-Tech = E1-0.00, E2-0.00, E3-0.06, E4-0.26, E5-0.68

SC Hiring Experience Staff of High-Tech = 1-0.00, E2-0.00, E3-0.24, E4-0.34, E5-0.42

SC Non-Security Staff Training of High-Tech = E1-0.00, E2-0.16, E3-0.44, E4-0.34, E5-0.00

Next, let mn be a basic probability mass representing the degree to which the ith basic attribute ei supports the hypothesis that the attribute y is assessed to the nth grade $E\ n$. mn, can be calculated as follows (Yang & Xu, 2002):

$$m_{n,i} = w_i \beta_{n,i} \quad n = 1,2, \dots, N \;\; i = 1,2, \dots, L \tag{5.8}$$

Where, w_i needs to be normalised. $m_{E,i}$ is given by:

$$m_{E,i} = 1 - \sum_{n=1}^{N} m_{n,i} \quad i = 1,2, \dots, L \tag{5.9}$$

The remaining probability mass $m\ E$, is split into two parts, $\bar{m}_{E,i}$ and $\tilde{m}_{E,i}$, and can be calculated by using the following equations (Yang & Xu, 2002):

$$\bar{m}_{E,i} = 1 - w_i \quad i = 1,2, \dots, L \tag{5.10}$$

$$\tilde{m}_{E,i} = w_i (1 - \sum_{n=1}^{N} \beta_{n,i}) \quad i = 1,2, \dots, L \tag{5.11}$$

Where, $m_{E,i}$=$\bar{m}_{E,i}$+$\tilde{m}_{E,i}$. $\bar{m}_{E,i}$ is a basic probability mass representing the belief degree of the basic attributes e_i, while $\tilde{m}_{E,i}$ is the incompleteness of the belief degree assessment.

The recursive evidential reasoning algorithm can be summarised as follows (Yang & Xu, 2002):

$$m_n = K[m_{n,i} m_{n+1,i} + m_{n,i} m_{E,i+1} + m_{E,i} m_{n+1,i}] \quad n = 1,2, \dots, N \tag{5.12}$$

$$\widetilde{m}_E = K[\widetilde{m}_{E,i}\widetilde{m}_{E,i+1} + \overline{m}_{E,i}\widetilde{m}_{E,i+1} + \widetilde{m}_{E,i}\overline{m}_{E,i+1}] \quad n = 1,2,\dots,N \tag{5.13}$$

$$K = [1 - \textstyle\sum_{t=1}^{N}\sum_{\substack{j=1 \\ j\neq t}}^{N} m_{t,i}m_{j,i+1}]^{-1}$$

$$i = 1,2,\dots, \mathrm{L}\text{-}1 \tag{5.14}$$

Where, K is a normalising factor so that $\sum_{n=1}^{N} m_n + \widetilde{m}_E = 1$. Note that the attributes in E are arbitrarily numbered. The results of m_n and $\widetilde{m}_E$do not depend on the other in which the basic attributes are aggregated.

The normalisation of the probability $\overline{m}_E$ in Equation 5.13 can be computed by using Equation 5.15.

$$\overline{m}_E = K\,[\overline{m}_{E,i}\overline{m}_{E,i+1}] \tag{5.15}$$

The normalisation of the probability m_H can be computed by using Equation 5.16.

$$m_E = \widetilde{m}_E + \overline{m}_E \tag{5.16}$$

In the ER approach, the combined degree of belief βn is directly given by (Yang & Xu, 2002):

$$\beta n = \frac{m_n}{1-\overline{m}_E} \qquad n = 1,2,\dots, N \tag{5.17}$$

$$\beta_E = \frac{\widetilde{m}_E}{1-\overline{m}_E} \tag{5.18}$$

Where, βn will be a degree of belief to which the general attribute y is assessed to the grade

En. βE is the degree of belief unassigned to any individual evaluation grade after all the L basic attributes have been assessed. It denotes the degree of incompleteness in the overall assessment.

5.3 Methodology

The selection of the most effective security countermeasure will be examined to construct the model. A flow chart of a test case is illustrated in Figure 5.2 where it shows the steps of the process illustrated by the rectangular boxes. The flow chart begins with identifying the problem and setting up the goal that needs to be achieved, followed by the identification of the evaluation criteria and alternatives that are conducted by using a brainstorming technique, literature and expert discussions. The third box represents the next step that is to determine the alternative solutions which will be mostly taken from the literatures and discussions with experts. The fourth is developing the model by using an AHP approach and then collecting the data for all criteria by using a set of questionnaires. The sixth step is assigning weightage to each of the criteria by using a pair wise comparison. An assessment on each of the alternatives is conducted by using an ER method and finally the proposed model will be validated by using a sensitivity analysis process. Further details of the process will be presented together with the case study in Section 5.3.

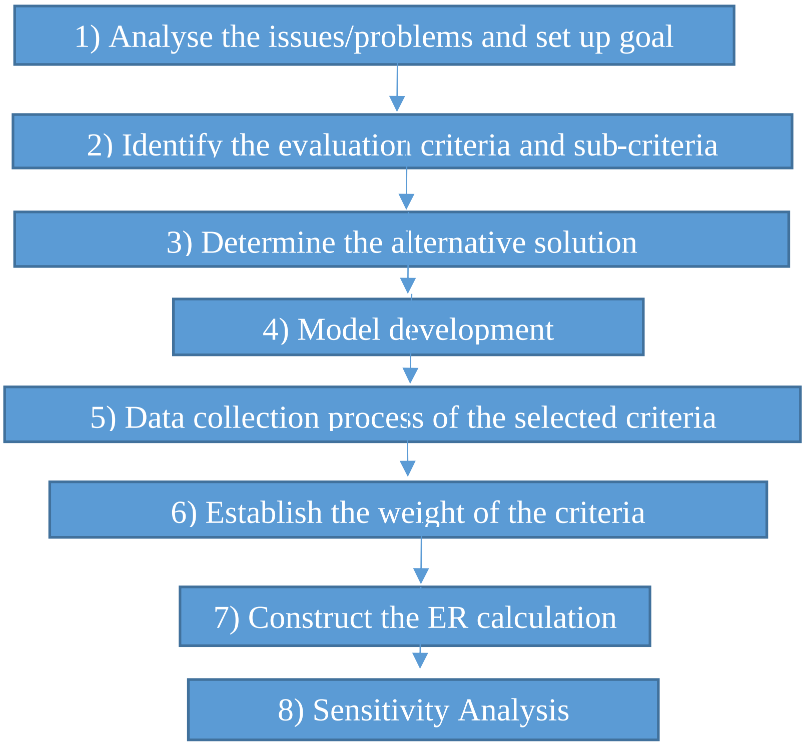

1) Analyse the issues/problems and set up goal
2) Identify the evaluation criteria and sub-criteria
3) Determine the alternative solution
4) Model development
5) Data collection process of the selected criteria
6) Establish the weight of the criteria
7) Construct the ER calculation
8) Sensitivity Analysis

Figure 5.2: The Flow Chart of the Study Development

Step 1: Set up a goal

In the previous chapter, the security countermeasures touch only on the security effectiveness in tackling terrorist attacks if and when they occurred and if the attacks were towards the wharfs and the consequences of such attacks. The chapter takes into consideration the security staff but not the non-security staff, the equipment supplies but not their costs and technology. The chapter does not highlight the access controls, deterrence, detection and assessment since the assumption is that the attacks would be on the wharfs. In this chapter, a generic security countermeasure study is applied in full force.

Step 2: Identify the evaluation criteria and sub-criteria

The literature surveys, discussion with experts and brainstorming technique will be used in the process of identifying the evaluation criteria and sub-criteria of this study. From these approaches, several criteria and sub-criteria can be obtained, but only some of them will be selected as criteria to comply with the security countermeasures for terrorist attack.

The parameters are divided into the main criteria and sub-criteria, which can be called Level 1 and Level 2, respectively. In general, there are four main criteria in this study, namely 1) Access Control, Delay and Deterrence, 2) Detection and Assessment, 3) Response to The Threat, and 4) Personnel and Equipment Security Cost. Each has its associated evaluation sub-criteria, as listed in Table 5.8. Below is the list of security countermeasures of terrorist attack on ports (main criteria and sub-criteria).

Table 5.8: Main Criteria and Sub-Criteria

Main Criteria	Sub-Criteria
Access Control and Deterrence (ACD)	Landscaping and Layout (LL)
	Gate and Barrier (GB)
	Screening and Check-up (SCU)
	Flexibility (FLX)
Detection and Assessment (DA)	Hearing Detection and Assessment (HDA)
	Visual Detection and Assessment (VDA)
	Other Detection and Assessment (ODA)
Response to the Threat (RTT)	Security Staff Training (SST)
	Hiring Experience Staff (HES)
	Non-security Staff Training (NST)
Personnel and Equipment Security Cost (PESC)	Drill Training Cost (DTC)
	Experienced Staff Salary (ESS)
	Procurement Equipment Cost (PEC)
	Security Equipment Maintenance Cost (SEMC)

Table 5.9: The Meaning of the Main Criteria and Sub-Criteria

Criteria	Meaning
Access Control, Delay and Deterrence	Is about limiting access to vulnerable assets only to those who have legitimate need to access them and creating a psychological impression that the risk of acting as a threat actor could be greater than the reward, either through creating the possibility that the threat action may not succeed, or that the threat actor may be caught and penalised.
Detection and Assessment	Is about utilising detection technologies that can alert the security staff of any unwanted or inappropriate activity within their compounds (seaport compound) and assess what has been detected to determine if it is a real threat or just a false alarm.
Response to the Threat	Is about people's actions. When the attack event occurs, they need to know what they should do (such as giving a warning to the threat actors, deploying a barrier to delay the threat and aggressive responses like automated

	weapons when needed). The people that will be included will be the security staff, security expert and non-security staff.
Personnel and Equipment Security Cost	The cost of security consists of Fixed Costs (High-Tech: annual payment for system licences, Low-Tech: Electricity payment for the techs, or guards' monthly payroll for No-Tech), and Installation Costs (payment for one off installation of the system for example the Hi-Tech item, installation of the Electronic Turnstiles, or policy enforcement for No-Tech).
Sub-Criteria	
Landscaping and Layout	Reshaping the layout of the port compound into a secure environment without affecting its operation. (No-Tech - the physical shape of the port facilities such as CPTED element, Low-Tech – the lighting in the layout and High-Tech – installing security sensor along port layout)
CPTED (crime prevention through environmental design) is a scientifically proven architectural discipline that helps reduce criminal behaviour by creating spaces that encourage appropriate behaviour and reducing the likelihood of criminal activity.	
Gate and Barrier	Control the access from outside to prevent unwanted visitors from entering the compound. (No-Tech – Policies and Procedures, Low-Tech - Deployable Barriers/ Vehicle Gates/ Revolving Doors, and High-Tech - Card Technologies System/ Access Credential Reader Technologies).
Screening and Check-up	Conduct a check-up and screening to prevent any illegal item from entering the facilities (weapons and bomb). (No-Tech guard search/trained dog's inspection, Low-Tech - Mechanical and Electronic Turnstiles, High Tech - Photo ID Detectors).
Flexibility	A flexibility sub-criterion has one purpose, which is to take into consideration customer satisfaction. While having a good access control and deterrence security would be good to prevent threats and ensure the customers that their merchandise/containers are well-protected such measures come with a huge cost and tighter security would cause delays, bottlenecks and discomfort to the customers since port operations deal with a lot of outsiders from the land and the sea.
Hearing Detection and Assessment	Creating detection methods using hearing that can alert the security staff of any unwanted or inappropriate activity within their compound then assess what has been detected to determine if it is a real threat or just a false alarm. (No-Tech – Security Posts/ Routine Patrols, Low-Tech – Emergency Alarms/Fire Alarms/ Communication Devices – Walkie Talkie, and High-Tech - Seismic Detection Systems/ Ultrasonic Sensors/ Duress Alarms).
Visual Detection and Assessment	Creating detection methods using visual that can alert the security staff of any unwanted or inappropriate activity within their compound then assess what has been detected to determine if it is a real threat or just a false alarm. (No-Tech – Security Posts/ Routine Patrols, Low-Tech – Visual Devices – binocular scopes/ Pan and Tilt CCTVs, and High-Tech Capacitance Detection Systems/ Infrared and Laser Detection Systems / Ground-Based Radar).
Other Detection and Assessment	Creating detection methods using others that can alert the security staff of any unwanted or inappropriate activity within their compound then assess what has been detected to determine if it is a real threat or just a false alarm. (No-Tech – Security Posts/ Routine Patrols, Low-Tech – Vehicular Patrols – Surveillance Boats, Cars And Motorcycles, and High-Tech - Fibre-Optics Detection Systems/ Thermal Imaging Sensors such as x-ray and Chemical residue detection systems).

Security Staff Training	After the security team confirms a threat based on their assessment, they are responsible for protecting the lives and the assets. This is done by delaying the threat actors from starting to take action or mitigating the threat while waiting for outside help and back-up. No-Tech – consist of security guards (armed/Unarmed) training program. Low-Tech – training security guards with Non-Lethal Weapons such as Water Cannon, Nets - Boat Traps, Fire Engines, Bomb Diffused programmes, and High-Tech– training security guards with an Advanced Non-Lethal Devices (such as -Long Range Acoustic Device (LRAD), Advanced Bomb Suits) and training to familiarise them with advanced High-Tech security systems for detection and assessment.
Hiring Experience Staff	Definition of experienced staff in this aspect does not reflect only for experience in security works. It also includes persons having military background, experts in bomb disposal, previous work as firemen and persons with experience as medical personnel in the military. In here, their role is to train the security staff in using No-Tech, Low-Tech and High-Tech items.
Non-security Staff Training	All non-security staff are required to have some knowledge about security countermeasures. This includes being familiar with the security system High-Tech and Low-Tech installed in the facilities compound and avoid any behaviour that may exploit those security items. On No-Tech areas, non-security staff should be involved in emergency preparedness programmes, and disaster recovery programmes.
Drill Training Cost	Drills and Training Costs cover both security staff and non-security staff. High-Tech would require more expense since it requires costly equipment, and hiring experts to train security staff and explain to non-security staff. Low-Tech and No Tech costs would be lower than High-Tech.
Experienced Staff Salary	Determining the salaries of experienced staff would be a little bit tricky since a lot of things need to be considered such as how many years has the expert work in such a field, their accomplishment before being hired into the company, their current conditions whether they still perform the same as before or even better, and were they just hired to became an instructor to train new bloods or do they need to be involved in security operations. The experts' extra payment as security staff will be considered due to their expertise in handling the items of security countermeasures (High-Tech, Low-Tech, No-Tech). [Justification – to measure the effectiveness of countermeasures]
Procurement Equipment Cost	Purchase of equipment for safety depends on the technology levels, while High-Tech has good technology (it can protect the building area with a bigger range) it costs a lot of money. On the other hand, No-Tech does not use technology (such as security staff and dogs - they cannot protect the compound as a whole and if the organization wants to cover the whole area of the building, it may increase the cost of hiring additional employees and the possibility of security controls being compromised due to the risk of unethical and treacherous workers).
Security Equipment Maintenance Cost	Equipment maintenance for security also depends on technology level. For High-Tech, it may be cheaper since it requires a small number of employees to protect the entire port area. In the case of No-Tech, maintenance costs may be higher as it requires a large number of security personnel to monitor

	the entire port area. They also need to be protected with life and health insurance and provided with training from time to time.

Step 3: Determine the alternative solutions

There are three types of possible alternatives in this study. All of them have their own advantages and limitations, and that will be the main focus when the experts make judgments in answering the survey questionnaires during the data collection period. The goal of each of the alternatives is to select the most effective security countermeasure against terrorist attack at the seaport (however, these alternatives can be adopted together). The three alternatives for this case study are: 1) The High-Tech security countermeasures, 2) The Low-Tech security countermeasures, and 3) The No-Tech security countermeasures as described in Table 5.10. Further in-depth explanations on the three alternatives are given in Section 5.1.3: Security Countermeasure Alternatives.

Table 5.10: Three Alternatives, Their Definitions and Meanings

Alternatives	**Meaning**
High-Tech Security Countermeasure	Hi-tech (electronic) countermeasures employ electronic systems to deter, detect, assess, and assist in the responses to the threats and to collect evidence.
Low-Tech Security Countermeasure	Lo-tech solutions include locks, barriers, lighting, and architectural solutions.
No-Tech Security Countermeasure	No-tech solutions include policies and procedures, security staffing, training, awareness programmes, investigations, and security dogs

Table 5.11: Alternatives Countermeasure and Their Possible Equipment and Security Staff Used

Main Criteria	**High-Tech**	**Low-Tech**	**No-Tech**
ACD	• Card Technologies • Access Credential Reader Technologies* • Consoles/Receptions • Security Command • Photo ID Detectors • Security Management Office-Interview Room • Incorporate sensors in the layout	• Locks • Revolving Doors • Mechanical and Electronic Turnstiles • Vehicle Gates • Deployable Barriers • Lighting in the layout • Signage	• Policies • Procedures • Trained Dogs • Law Enforcement • CPTED Element • Deterrence Programmes
DA	• Property Perimeter Detection Systems • Building Perimeter Detection Systems	• Visual Device – binocular scopes	• Security Posts • Routine Patrols

	• Interior Space Detection Systems • Point Detection Systems • Video Detection Systems • Security System Infrastructures • Security Digital Infrastructure	• Communication Devices – Walkie Talkie • Vehicular Patrols – Surveillance Boats, Cars And Motorcycles	• Routine Check-Up • Security Awareness Programmes
RTT	• Non-Lethal Weapons -Long Range Acoustic Device (LRAD) -Anti-Piracy Laser Beam -Tasers Guns –Electric Shock -Active Denial System – Pain Ray (Electromagnetic Wave) -Advanced Bomb Suits	• Non-Lethal Weapons -Water Cannons -Net- Boat Traps -Foul Smelling Liquid -Rear Wire Canisters -Stun Grenades -Fire Engines -Explosive Ordnance Disposal (EOD) Suits -Bullet Proof Vehicles • Lethal Weapons -Guard Firearms -Grenades (Bombs)	• Guards (Armed/Unarmed) • Security Vehicles Training Programmes • Emergency Preparedness Programmes • Disaster Recovery Programmes • Security Staffing
PESC	Higher Cost	Medium Cost	Lower Cost

Step 4: Model development

The model developed contains the goal, main criteria, sub-criteria and the alternatives for the solutions. All information will be illustrated in hierarchical structure starting with the goal, linked to the main criteria then spread up to sub-criteria and finally end up on the alternatives as the solutions. The scientific model assists the port organisation in selecting or choosing for their security countermeasure the alternative that is most effective in facing a terrorist attack on the seaport.

By combining all the information in Step 1, Step 2 and Step 3, an analytical model was developed, as shown in Figure 5.3. Basically, it has three levels of information where at the first level (at the top) is the goal, followed by the criteria (at the second level) and the sub-criteria (at the third level after the criteria), while all the alternatives are at the bottom of the model. The main goal of this study is to select the most effective security countermeasure to counter a terrorist attack at the port.

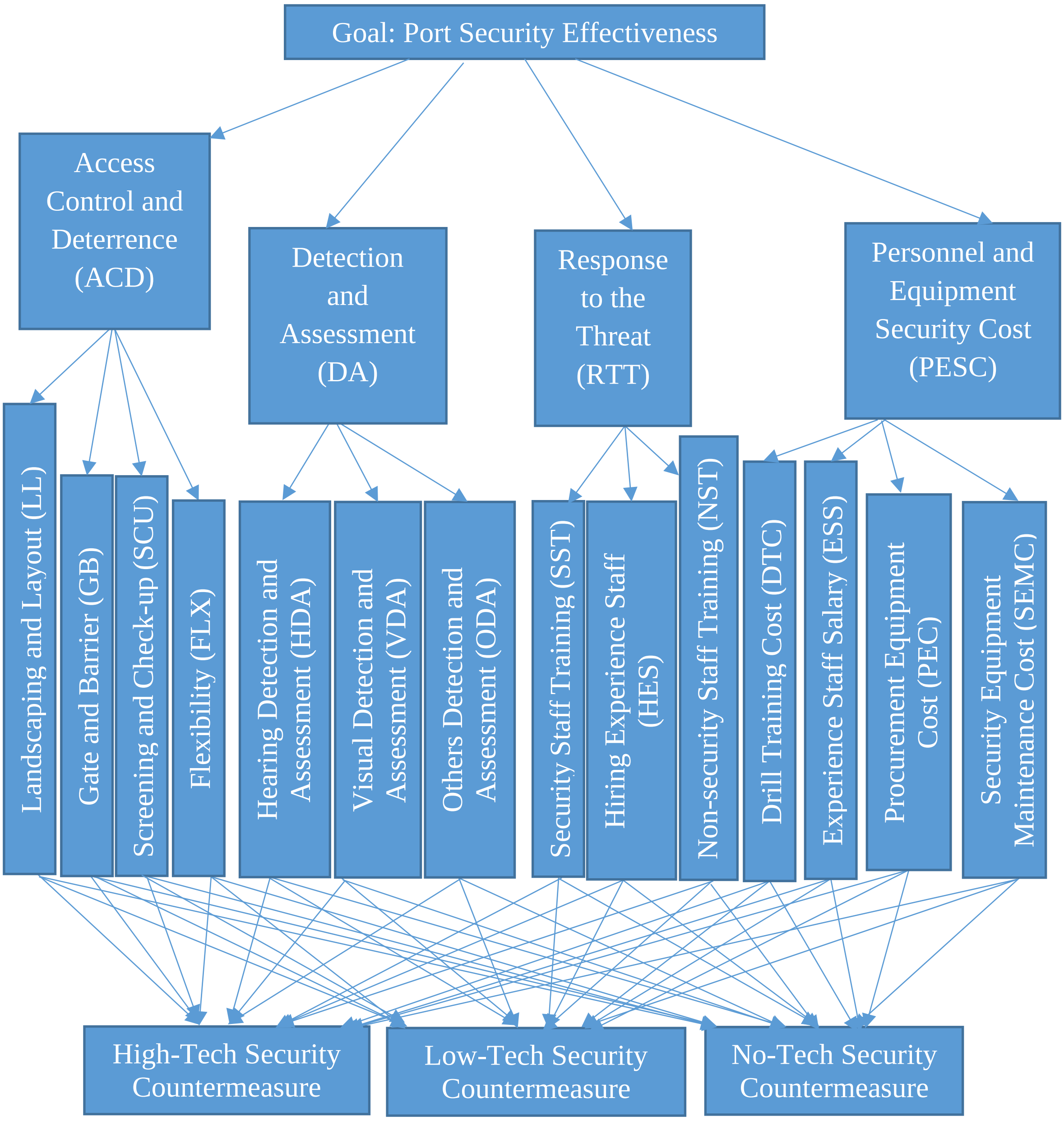

Goal: Port Security Effectiveness
Access Control and Deterrence (ACD)
Detection and Assessment (DA)
Response to the Threat (RTT)
Personnel and Equipment Security Cost (PESC)
Landscaping and Layout (LL)
Gate and Barrier (GB)
Screening and Check-up (SCU)
Flexibility (FLX)
Hearing Detection and Assessment (HDA)
Visual Detection and Assessment (VDA)
Others Detection and Assessment (ODA)
Security Staff Training (SST)
Hiring Experience Staff (HES)
Non-security Staff Training (NST)
Drill Training Cost (DTC)
Experience Staff Salary (ESS)
Procurement Equipment Cost (PEC)
Security Equipment Maintenance Cost (SEMC)
High-Tech Security Countermeasure
Low-Tech Security Countermeasure
No-Tech Security Countermeasure

Figure 5.3: The Model of the Most Effective Alternative of Security Countermeasure

There are four main criteria as described in Table 5.9 namely: 1) Access Control, Delay and Deterrence (ACD), 2) Detection and Assessment (DA), 3) Response To the Threat (RTT), and 4) Personnel and Equipment Security Cost (PESC). Each of the criteria has a few sub-criteria attached to it, which are: 1) LL, GB, SCU, FLX for criteria ACD, 2) HDA, VDA, ODA for criteria DA, 3) SST, HES, NST for criteria RTT, AND 4) DTC, ESS, PEC, SEMC for criteria PESC. All the main criteria and sub-criteria are linked to the three alternatives which are High-tech security countermeasures, Low-tech security countermeasures and No-tech security countermeasures.

Step 5: Data collection process

Data collection was conducted by getting expert judgement on the subject of the study. A set of questionnaires was given to each of the selected experts and they were expected to respond based on their expert opinions. Discussions were held with the experts through scheduled interview sessions.

In this case study, all the necessary qualitative data were obtained from expert judgments by using the said questionnaires (Appendix 8). Five experts were selected based on their knowledge, expertise and experience in the maritime industry of more than 10 years. All the experts contributed their opinion and judgements in developing a novel model, determining parameters and answering questionnaires. Below are their responses on the main criteria effectiveness of the countermeasures' (Table 5.12).

Table 5.12: Respondents' (Experts') Opinion on the main criteria Effectiveness of the Countermeasures

Q	Criteria's	R 1	R 2	R 3	R 4	R 5	TOTAL	AVERAGE
5	ACD versus DA	2	2	3	2	2	11	11/5
	ACD versus RTT	3	3	3	2	2	13	13/5
	ACD versus PESC	4	4	2	2	4	16	16/5
6	DA versus RTT	2	3	2	2	2	11	11/5
	DA versus PESC	3	4	2	3	2	14	14/5
7	RTT versus PESC	2	4	2	3	2	13	13/5

Step 6*: *Estimate the weightage of each criterion by using the AHP approach

The weightage estimation process of the evaluation criteria can be conducted by using a pair-wise comparison technique. The implementation of this technique is associated with a number of selected expert judgments for analysing the priority of each criterion to another by incorporating the ratio scale of pair-wise comparison in Table 5.5. To continue, firstly, a level of criteria needs to be identified. There are two levels of criteria in this test case as shown in Figure 5.3. Level 1 is known as the main criteria, while Level 2 is called sub-criteria.

$$\text{Average Rating Value}=\frac{\substack{Total\ rate\ given\ by\ the\ experts\\ for\ the\ same\ criterion}}{Total\ number\ of\ experts} \tag{5.19}$$

A set of questionnaires (Appendix 9) was sent to each of the selected experts for their evaluation and their feedback was investigated accordingly based on their judgments on the criteria under discussion. Referring to the four main criteria as mentioned earlier and together with Equation 5.19, a 4×4 pair-wise comparison matrix was developed to obtain the weightage of these criteria. *A(ACDDARTTPESC)* is a pair-wise comparison matrix expressing the qualified judgement with regard to the relative priority of ACD, DA, RTT, and PESC (Table 5.13).

By using the ratio scale of pair-wise comparison listed in Table 5.5, given the four main criteria as an example (ACD, DA, RTT, and PESC), a 4×4 pair-wise comparison matrix is used for obtaining the weightage of each of them Equation 5.1). *A* (ACD, DA, RTT, and PESC) is a matrix expressing the qualified judgement with regard to the relative priority of the Access Control, Delay and Deterrence (ACD), Detection and Assessment (DA), Response to The Threat (RTT), and Personnel and Equipment Security Cost (PESC).

Table 5.13: The Total of 4×4 Pair-Wise Comparison Matrix Main Criteria

A(ACDDARTTPESC) =

	ACD	DA	RTT	PESC
ACD	1	11/5	13/5	16/5
DA	5/11	1	11/5	14/5
RTT	5/13	5/11	1	13/5
PESC	5/16	5/11	5/13	1
TOTAL	2.15	4.11	6.18	9.60

The performance ratio rate of *A (ACDDARTTPESC)* was calculated as follows:

Table 5.14: The Performance Ratio of Each Main Criterion

ACD	(1)÷ 2.15 =0.465	(11/5) ÷4.11 =0.535	(13/5) ÷6.18 =0.420	(16/5) ÷9.6 =0.333
DA	(5/11) ÷2.15 =0.211	(1) ÷4.11 =0.243	(11/5) ÷6.18 =0.356	(14/5) ÷9.6 =0.290
RTT	(5/13) ÷2.15 =0.179	(5/11) ÷4.11 =0.111	(1) ÷6.18 =0.162	(13/5) ÷9.6 =0.271
PESC	(5/16) ÷2.15 =0.145	(5/11) ÷4.11 =0.111	(5/13) ÷6.18 =0.062	(1) ÷9.6 =0.104

The weightage of the main criteria and sub-criteria was calculated by using a pair-wise comparison technique. It is an AHP approach, by sending a set of questionnaires to the selected experts for them to analyse the importance of each criterion to another by placing a ratio scale of the pairwise comparison. The weightage values of all the main criteria were determined by using Equation 5.2. Given the criterion "ACD" as an example, the weightage value is computed as follows:

$$W_{ACD} = \frac{0.465+0.535+0.42+0.333}{4} = 0.438 \tag{5.20}$$

Where, the weightage value of the criterion ACD is known to be 0.438, similarly, the weightage calculation algorithm was applied to all other main criteria. Table 5.15 summarises all output values of the weightage calculation.

Table 5.15: The Weightage Value of Evaluation Criteria

					Weight Value (Average)
ACD	0.465	0.535	0.420	0.333	0.438
DA	0.211	0.243	0.356	0.292	0.276
RTT	0.179	0.111	0.162	0.271	0.180
PESC	0.145	0.111	0.062	0.104	0.106

After obtaining the weightage value of each criterion, the consistency ratio needs to be measured (if the inconsistency is smaller than or equal to 10%). Saaty (1980) allowed some measures of inconsistency (common with subjective human judgement) when applied to the logic of preferences. Inconsistencies arise when three items were compared, such as A, B, and C. For example, if Item A is more preferred over Item B, and Item B is more preferred over Item C, then by transitive property, Item A should be more preferred over Item C. If not, then the comparisons are not consistent.

Any inconsistency that is greater than 10% will be rejected and the subjective judgement needs to be revised. The calculation of the consistency ratio of the pair-wise comparison was conducted. Firstly, each value in the column of the pair-wise comparison matrix (Table 5.13) was multiplied by the weightage value of each criterion as follows:

$$0.438 \begin{array}{|c|} \hline \text{ACD} \\ \hline 1 \\ \hline 5/11 \\ \hline 5/13 \\ \hline 5/16 \\ \hline \end{array} + 0.276 \begin{array}{|c|} \hline \text{DA} \\ \hline 11/5 \\ \hline 1 \\ \hline 5/11 \\ \hline 5/11 \\ \hline \end{array} + 0.180 \begin{array}{|c|} \hline \text{RTT} \\ \hline 13/5 \\ \hline 11/5 \\ \hline 1 \\ \hline 5/13 \\ \hline \end{array} + 0.106 \begin{array}{|c|} \hline \text{PESC} \\ \hline 16/5 \\ \hline 14/5 \\ \hline 13/5 \\ \hline 1 \\ \hline \end{array}$$

Consequently, Table 5.16 summarises the calculation below.

Table 5.16: The Total Value of the Calculation

					TOTAL
ACD	0.438	0.606	0.469	0.338	1.852
DA	0.199	0.276	0.397	0.296	1.167
RTT	0.169	0.125	0.180	0.274	0.749
PESC	0.137	0.125	0.069	0.106	0.437

In order to calculate the $\frac{\sum_{k=1}^{n} w_k a_{jk}}{w_i}$ value as described in Equation 5.5, the total value of each main criterion described in Table 5.16 needs to be divided with the weightage value of the corresponding main criteria as follows:

$$\frac{1.852}{0.438} = 4.223; \frac{1.167}{0.276} = 4.237; \frac{0.749}{0.180} = 4.149; \frac{0.437}{0.106} = 4.142$$

The λ_{max} is calculated as follows:

$$\lambda_{max} = \frac{4.223 + 4.237 + 4.149 + 4.142}{4} = 4.188$$

Next, the *CI* is computed by using Equation 5.4 as follows:

$$CI = \frac{4.188 - 4}{4 - 1} = 0.063$$

Subsequently, the consistency ratio (*CR*) is calculated by using Equation 5.3. There are four criteria in Level 1, therefore the random index (*RI*) is 0.9000 since the n is 4 (Table 5.6) and the *CR* value of the main criteria is obtained as follows:

$$CR = \frac{0.063}{0.9} = 0.07$$

The *CR* value of the main criteria is known to be 0.07. This means that the degree of consistency in the pairwise comparison is acceptable because the *CR* value is less than 0.10. The similar calculation process of the weighting vector described previously was applied to determine the priority of each sub-criterion as compared to others at Level 2. There are four groups of sub-criteria which are: 1) ACD, 2) DA, 3) RTT and 4) PESC that need to be evaluated.

The weighting values of all the sub-criteria under ACD group are as follows:

Table 5.17: The Total of 4×4 Pair-Wise Comparison Matrix Sub-Criteria under ACD

A(LLGBSCUFLX) =

	LL	GB	SCU	FLX
LL	1	3/4	1/2	10/7
GB	4/3	1	1	3/2
SCU	2	1	1	11/6
FLX	2/3	2/3	1/2	1
TOTAL	5.00	3.42	3.00	5.76

The weightage values of *A (LLGBSCUFLX)* are 0.201 (LL), 0.283 (GB), 0.341 (SCU) and 0.175 (FLX), while the *CR* value is 0.01.

The weighting vector values of all the sub-criteria under DA group are summarised as follows:

Table 5.18: The Total of 4×4 Pair-Wise Comparison Matrix Sub-Criteria under DA

A(HADVDAODA) =

	HAD	VDA	ODA
HAD	1	1	3/2
VDA	1	1	3
ODA	2/3	1/3	1
TOTAL	2.67	2.33	5.50

The weightage values of *A (HADVDAODA)* are 0.391 (HAD), 0.417 (VDA) and 0.192 (ODA), while the *CR* value is 0.067.

The weighting vector values of all the sub-criteria under RTT group are summarised as follows:

Table 5.19: The Total of 4×4 Pair-Wise Comparison Matrix Sub-Criteria under RTT

A(SSTHESNST) =

	SST	HES	NST
SST	1	10/7	19/7
HES	2/3	1	5/2
NST	3/8	2/5	1
TOTAL	2.04	2.83	6.21

The weightage values of *A (SSTHESNST)* are 0.483 (SST), 0.353 (HES) and 0.164 (NST), while the *CR* value is 0.008.

The weighting vector values of all the sub-criteria under PESC group are summarised as follows:

Table 5.20: The Total of 4×4 Pair-Wise Comparison Matrix Sub-Criteria under PESC

A(ACDDARTTPESC) =

	DTC	ESS	PEC	SEMC
DTC	1	4/7	2/3	3/4
ESS	12/7	1	5/6	2
PEC	3/2	11/9	1	8/7
SEMC	11/8	1/2	7/8	1
TOTAL	5.59	3.29	3.38	4.89

The weightage values of *A (DTCESSPECSEMC)* are 0.178 (DTC), 0.309 (ESS), 0.301 (PEC) and 0.212 (SEMC), while the *CR* value is 0.022.

Table 5.21: Weight of Main criteria and Sub criteria

Main Criteria		**Sub-Criteria**	
Access Control, Delay and Deterrence (ACD)	0.438	Landscaping and Layout (LL)	0.201
		Gate and Barrier (GB)	0.283
		Screening and Check-up (SCU)	0.341
		Flexibility (FLX)	0.175
Detection and Assessment (DA)	0.276	Hearing Detection and Assessment (HDA)	0.391
		Visual Detection and Assessment (VDA)	0.417
		Other Detection and Assessment (ODA)	0.192
Response to the Threat (RTT)	0.180	Security Staff Training (SST)	0.483
		Hiring Experience Staff (HES)	0.353
		Non-security Staff Training (NST)	0.164
Personnel and Equipment Security Cost (PESC)	0.106	Drill Training Cost (DTC)	0.178
		Experienced Staff Salary (ESS)	0.309
		Procurement Equipment Cost (PEC)	0.301
		Security Equipment Maintenance Cost (SEMC)	0.212

Step 7: Construction of the ER calculation

The ER approach assessment was conducted by using IDS software tools and to demonstrate the assessment, an example of manual calculation is shown (the example was taken from one of the sub-criteria of the case study which was the criterion “response to threats in respect to the alternative the High-Tech Security Countermeasure”). Then, the ranking of the alternatives was calculated from the result of the assessment value. For more details regarding the ER algorithm, refer to Section 5.2.2.

Let y=$e_1 \oplus e_2 \oplus e_3$

Table 5.22: The Belief Degree Values of the Criterion “Response to Threats” with Respect to the Alternative “High-Tech Security Countermeasures”

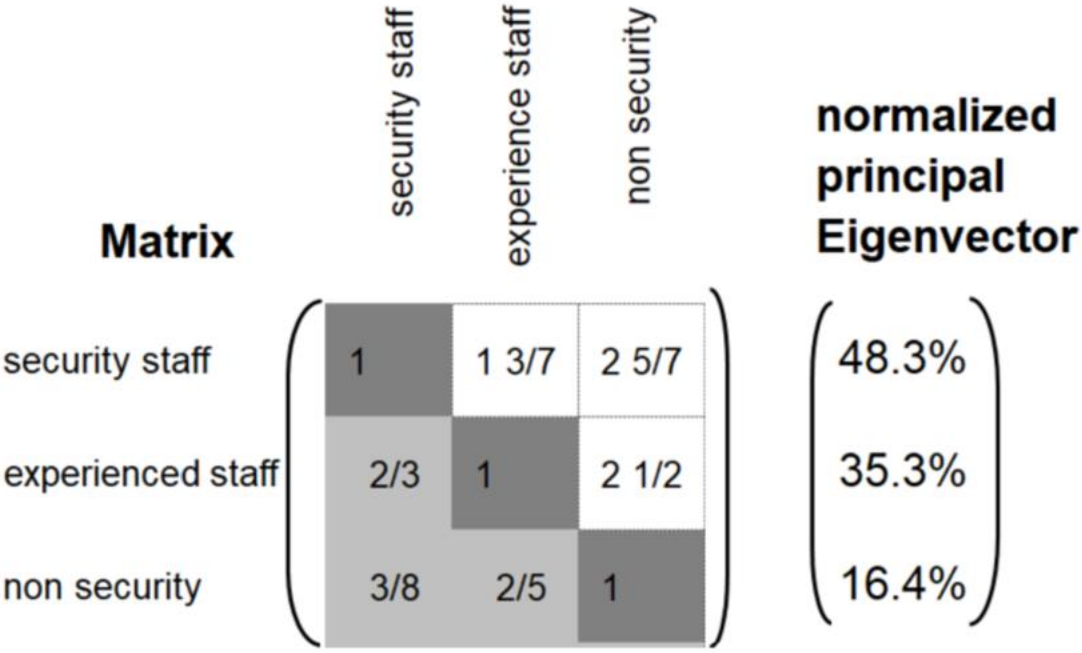
Belief Degree ($\boldsymbol{\beta}$)		Assessment Grades				
		Poor	Reasonably Poor	Average	Reasonably Good	Good
RTT	SST	0.00	0.00	0.06	0.26	0.68
	HES	0.00	0.00	0.24	0.34	0.42
	NST	0.00	0.16	0.44	0.34	0.06

By using Equation 5.7, the belief degree values of SST, HES and NST were formed as follows:

SC(*SST*) = {(*Poor, 0.00*), (*Reasonably Poor, 0.00*), (*Average, 0.06*), (*Reasonably Good, 0.26*), (*Good, 0.68*)}.

SC(HES) = {*(Poor, 0.00)*, (*Reasonably Poor, 0.00*), (*Average, 0.24*), (*Reasonably Good, 0.34*), (*Good, 0.42*)}.

SC(NST) = {*(Poor, 0.00)*, (*Reasonably Poor, 0.16*), (*Average, 0.44*), (*Reasonably Good, 0.34*), (*Good, 0.06*)}.



Matrix	security staff	experience staff	non security	normalized principal Eigenvector
security staff	1	1 3/7	2 5/7	48.3%
experienced staff	2/3	1	2 1/2	35.3%
non security	3/8	2/5	1	16.4%

Figure 5.4: The Weight Values of the Criterion 'Respond to Threat'

The weight values of SST, HES and NST were 0.483, 0.353 and 0.164 as described in Figure 5.3. By using the information given in Table 5.19 and the weight values, the basic probability masses *mn,* were calculated by using Equation 5.8 as follows:

The $m_{n,i}$ of SST

	Equation 5.8					Equation 5.10	Equation 5.11	Equation 5.9
SST × 0.483	$m_{1,1}$ =0	$m_{2,1}$ =0	$m_{3,1}$= 0.02898	$m_{4,1}$= 0.12558	$m_{5,1}$= 0.32844	$\overline{m}_{E,1}$= 1-0.483 =0.517	$\widetilde{m}_{E,1}$= 0.483(1-1) =0	$m_{E,1}$= 0.517+0 =0.517

The $m_{n,i}$ of HES

HES × 0.353	$m_{1,2}$ =0	$m_{2,2}$ =0	$m_{3,2}$= 0.08472	$m_{4,2}$= 0.12002	$m_{5,2}$= 0.14826	$\overline{m}_{E,2}$= 1-0.353 =0.647	$\widetilde{m}_{E,2}$= 0.353(1-1) =0	$m_{E,2}$= 0.647+0 =0.647

The $m_{n,i}$ of NST

NST × 0.164	$m_{1,3}$ =0	$m_{2,3}$= 0.02624	$m_{3,3}$= 0.07216	$m_{4,3}$= 0.05576	$m_{5,3}$= 0.00984	$\overline{m}_{E,3}$= 1-0.164 =0.836	$\widetilde{m}_{E,3}$= 0.164(1-1) =0	$m_{E,3}$= 0.836+0 =0.836

	M1	M2	M3	M4	M5	m̄	m̃	m
1	0.00	0.00	0.02898	0.12558	0.32844	0.517	0.00	0.517
2	0.00	0.00	0.08472	0.12002	0.14826	0.647	0.00	0.647

The $m_{E,i}$ values for both $m_{E,1}$ and $m_{E,2}$ were calculated using Equation 5.9. $\overline{m}_{E,i}$, can be calculated using Equation 5.10, while $\widetilde{m}_{E,i}$ can be computed by using Equation 5.11. To continue calculating using the equation, those steps were shown below.

The equation below refers to equation 5.14 to calculate the normalized factor of (K).

$$\text{K}=\left[1-\begin{pmatrix} m_{1,1} & m_{2,2} & +m_{1,1} & m_{3,2} & +m_{1,1} & m_{4,2} & +m_{1,1} & m_{5,2} \\ m_{2,1} & m_{1,2} & +m_{2,1} & m_{3,2} & +m_{2,1} & m_{4,2} & +m_{2,1} & m_{5,2} \\ m_{3,1} & m_{1,2} & +m_{3,1} & m_{2,2} & +m_{3,1} & m_{4,2} & +m_{3,1} & m_{5,2} \\ m_{4,1} & m_{1,2} & +m_{4,1} & m_{2,2} & +m_{4,1} & m_{3,2} & +m_{4,1} & m_{5,2} \\ m_{5,1} & m_{1,2} & +m_{5,1} & m_{2,2} & +m_{5,1} & m_{3,2} & +m_{5,1} & m_{4,2} \end{pmatrix}\right]^{-1} \tag{5.21}$$

$$\text{K}=\left[1-\begin{pmatrix} 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.02898\times0.12002 & 0.02898\times0.14826 \\ 0.0 & 0.0 & 0.12558\times0.08472 & 0.12558\times0.14826 \\ 0.0 & 0.0 & 0.32844\times0.08472 & 0.32844\times0.12002 \end{pmatrix}\right]^{-1}$$

$$\text{K}=\left[1-\begin{pmatrix} 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.003478 & 0.004297 \\ 0.0 & 0.0 & 0.010639 & 0.018618 \\ 0.0 & 0.0 & 0.027825 & 0.039419 \end{pmatrix}\right]^{-1}$$

$\text{K}=[1-(0.104276)]^{-1}$ $=[0.895724]^{-1}$ =1.116415324 ≈1.1164

The normalised factor (K) can be further calculated using Equation 5.12 as follows:

(1+2)

$m_1 \;= K_{I(1+2)}(m_{1,1}m_{1,2} + m_{1,1}m_{E,2} + m_{E,1}m_{1,2})$	=1.1164 ([0.00000×0.000000] + [0.00000×0.647] + [0.517×0.00000])	= 0
$m_2 \;= K_{I(1+2)}(m_{2,1}m_{2,2} + m_{2,1}m_{E,2} + m_{E,1}m_{2,2})$	=1.1164 ([0.00000×0.00000] + [0.00000×0.647] + [0.517×0.00000])	= 0
$m_3 \;= K_{I(1+2)}(m_{3,1}m_{3,2} + m_{3,1}m_{E,2} + m_{E,1}m_{3,2})$	=1.1164 ([0.02898×0.08472] + [0.02898×0.647] + [0.517×0.08472])	= 0.072573217
$m_4 \;= K_{I(1+2)}(m_{4,1}m_{4,2} + m_{4,1}m_{E,2} + m_{E,1}m_{4,2})$	=1.1164 ([0.12558×0.12002] + [0.12558×0.647] + [0.517×0.12002])	= 0.176809957
$m_5 \;= K_{I(1+2)}(m_{5,1}m_{5,2} + m_{5,1}m_{E,2} + m_{E,1}m_{5,2})$	=1.1164 ([0.32844×0.14826] + [0.32844×0.647] + [0.517×0.14826])	= 0.377176521
$\overline{m}_E \;= K_{I(1+2)}(\overline{m}_{E1}\,\overline{m}_{E2})$	=1.1164 (0.647×0.517)	= 0.373440305
$\widetilde{m}_E \;= K_{I(1+2)}(\widetilde{m}_{E,1}\widetilde{m}_{E,2} + \overline{m}_{E,1}\,\widetilde{m}_{E,2} + \widetilde{m}_{E,1}\overline{m}_{E,2})$	=1.1164 ([0.00000×0.000000] + [0.647×0.00000] + [0.00000×0.517])	= 0

The normalisation of the probability $\widetilde{m}_E$ (calculated by using Equation 5.13), $\overline{m}_E$ (calculated using Equation 5.15), and m_E (calculated by using Equation 5.16) as follows:

$m_{1,1+2}$=0.00	$m_{2,1+2}$=0.00	$m_{3,1+2}$=0.072572123	$m_{4,1+2}$=0.176807295
$m_{1,3}$=0.00	$m_{2,3}$=0.02624	$m_{3,3}$ =0.07216	$m_{4,3}$ =0.05576

$m_{5,1+2}$=0.377170843	$\bar{m}_{E,1+2}$= 0.373434684	$\tilde{m}_{E,1+2}$=0.00	$m_{E,1+2}$=0.373434684
$m_{5,3}$ =0.00984	$\bar{m}_{E,3}$=0.836	$\tilde{m}_{E,3}$=0.00	$m_{E,3}$=0.836

To calculate the normalised factor (K) [1+2+3], Equation 5.14 was again applied. This equation can be further expressed as follows:

$$\text{K}=\left[1-\begin{pmatrix} m_{1,1+2} & m_{2,3} & +m_{1,1+2} & m_{3,3} & +m_{1,1+2} & m_{4,3} & +m_{1,1+2} & m_{5,3} \\ m_{2,1+2} & m_{1,3} & +m_{2,1+2} & m_{3,3} & +m_{2,1+2} & m_{4,3} & +m_{2,1+2} & m_{5,3} \\ m_{3,1+2} & m_{1,3} & +m_{3,1+2} & m_{2,3} & +m_{3,1+2} & m_{4,3} & +m_{3,1+2} & m_{5,3} \\ m_{4,1+2} & m_{1,3} & +m_{4,1+2} & m_{2,3} & +m_{4,1+2} & m_{3,3} & +m_{4,1+2} & m_{5,3} \\ m_{5,1+2} & m_{1,3} & +m_{5,1+2} & m_{2,3} & +m_{5,1+2} & m_{3,3} & +m_{5,1+2} & m_{4,3} \end{pmatrix}\right]^{-1} \tag{5.22}$$

$$\text{K}=\left[1-\begin{pmatrix} 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0726\times0.02624 & 0.0726\times0.05576 & 0.0726\times0.00984 \\ 0.00 & 0.1768\times0.02624 & 0.1768\times0.07216 & 0.1768\times0.00984 \\ 0.00 & 0.3772\times0.02624 & 0.3772\times0.07216 & 0.3772\times0.05576 \end{pmatrix}\right]^{-1}$$

$$\text{K}=\left[1-\begin{pmatrix} 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.001904 & 0.004047 & 0.000714 \\ 0.0 & 0.004639 & 0.012759 & 0.00174 \\ 0.0 & 0.009897 & 0.027217 & 0.021031 \end{pmatrix}\right]^{-1}$$

$$\text{K}=[1-(0.083948566)]^{-1} \quad =[0.916051434]^{-1} \quad =1.09$$

(1+2+3)

m_1	$= K_{II(I+3)}(m_{1,I}m_{1,3} + m_{1,I}m_{E,3} + m_{E,I}m_{1,3})$	=1.09 ([0.00000×0.000000] + [0.00×0.836] + [0.373440305×0.00])	= 0.00
m_2	$= K_{II(I+3)}(m_{2,I}m_{2,3} + m_{2,I}m_{E,3} + m_{E,I}m_{2,3})$	=1.09 ([0.00000×0.02624] + [0.0×0.836] + [0.373440305×0.02624])	= 0.01068099
m_3	$= K_{II(I+3)}(m_{3,I}m_{3,3} + m_{3,I}m_{E,3} + m_{E,I}m_{3,3})$	=1.09 ([0.072573217×0.07216] + [0.072572123×0.836] + [0.373440305×0.07216])	= 0.101212544
m_4	$= K_{II(I+3)}(m_{4,I}m_{4,3} + m_{4,I}m_{E,3} + m_{E,I}m_{4,3})$	=1.09 ([0.176809957×0.05576] + [0.176807295×0.836] + [0.373440305×0.05576])	= 0.194559636
m_5	$= K_{II(I+3)}(m_{5,I}m_{5,3} + m_{5,I}m_{E,3} + m_{E,I}m_{5,3})$	=1.09 ([0.377176521×0.00984] + [0.377176521×0.836] + [0.373440305×00.00984])	= 0.351749149

$\bar{m}_E \quad = K_{II(I+3)}(\bar{m}_{E,I}\,\bar{m}_{E,3})$	=1.09 (0.373440305×0.836)	= 0.340293 744
$\tilde{m}_E \quad = K_{II(I+3)}(\tilde{m}_{E,I}\tilde{m}_{H,3} + \bar{m}_{EI}\ \tilde{m}_{E,3} + \tilde{m}_{E,I}\bar{m}_{E,3})$	=1.09 ([0.00000×0.000000] + [0.373440305×0.00000] + [0.00000×0.836])	= 0.00

The result calculated from above were simplifies as follows:

$m_{1,1+2+3}$=0	$m_{2,1+2+3}$=0.01068099	$m_{3,1+2+3}$=0.101212544	$m_{4,1+2+3}$=0.194559636

$m_{5,1+2+3}$=0.351749149	$\bar{m}_{E,1+2+3}$=0.340293744	$\tilde{m}_{E,1+2+3}$=0	$m_{E,1+2+3}$=0.340293744

The combined degrees of belief values are calculated using Equation 5.17 as follows:

$$(Poor)\beta_1 = \frac{m_1}{1-\bar{m}_E} = \frac{0}{1-0.34029} = 0.00$$

$$(Reasonably\ Poor)\beta_2 = \frac{m_2}{1-\bar{m}_E} = \frac{0.01068099}{1-0.34029} = 0.016190524$$

$$(Average)\beta_3 = \frac{m_3}{1-\bar{m}_E} = \frac{0.101212544}{1-0.34029} = 0.153420622$$

$$(Reasonably\ Good)\beta_4 = \frac{m_4}{1-\bar{m}_E} = \frac{0.194559636}{1-0.34029} = 0.294918586$$

$$(Good)\beta_5 = \frac{m_5}{1-\bar{m}_E} = \frac{0.351749149}{1-0.34029} = 0.533190561$$

The belief degree value for β_E is computed using Equation 5.18 as follows:

$$\beta_E = \frac{\tilde{m}_E}{1-\bar{m}_E} = \frac{0}{1-0.34029} = 0$$

The aggregated assessment for the criterion "response to the threats" in respect of the alternative "high-tech security countermeasures" is therefore given by the following distribution:

SC (Respond to Threat) = SC (SST ⊕ HES ⊕ NST)

= {(Worst,0), (Poor, 0.016), (Average, 0.153), (Good,0.295), (Best,0.533)}

Such aggregated assessment values can also be calculated by using the Intelligent Decision System (*IDS*) software tool as shown in Figure 5.5.

All other calculations will be conducted by using IDS software together with the weight value of the same main criteria and sub-criteria. As a result, the output values of the three alternative strategies are summarised in Figure 5.6 (High-Tech Security), Figure 5.7 (Low-Tech Security) and Figure 5.8 (No-Tech Security).

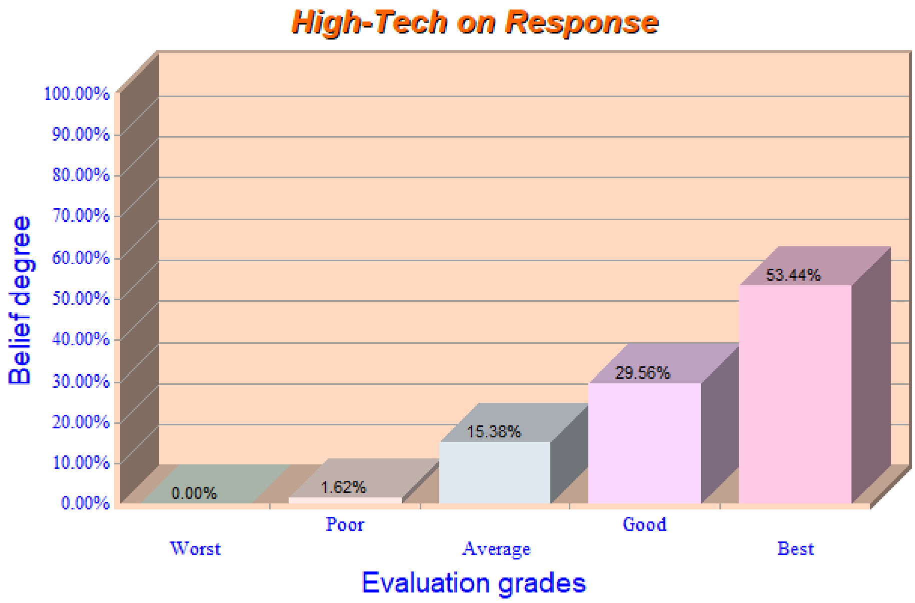


Figure 5.5: The Alternative "High-Tech Security Countermeasures in Response to Threat"

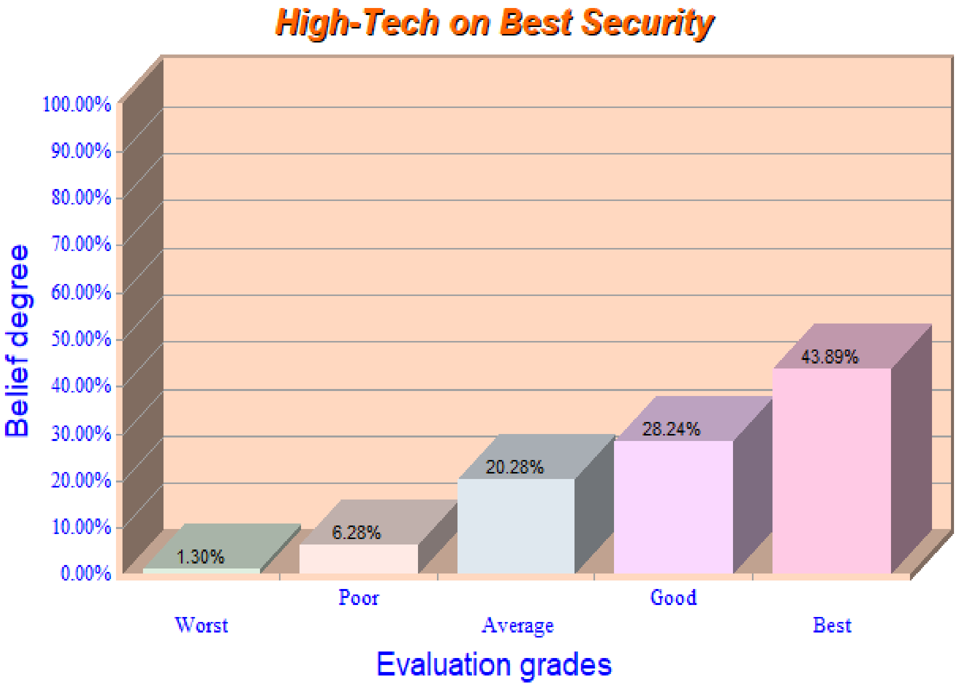


Figure 5.6: The Output Values of the Alternative "High Tech Security"

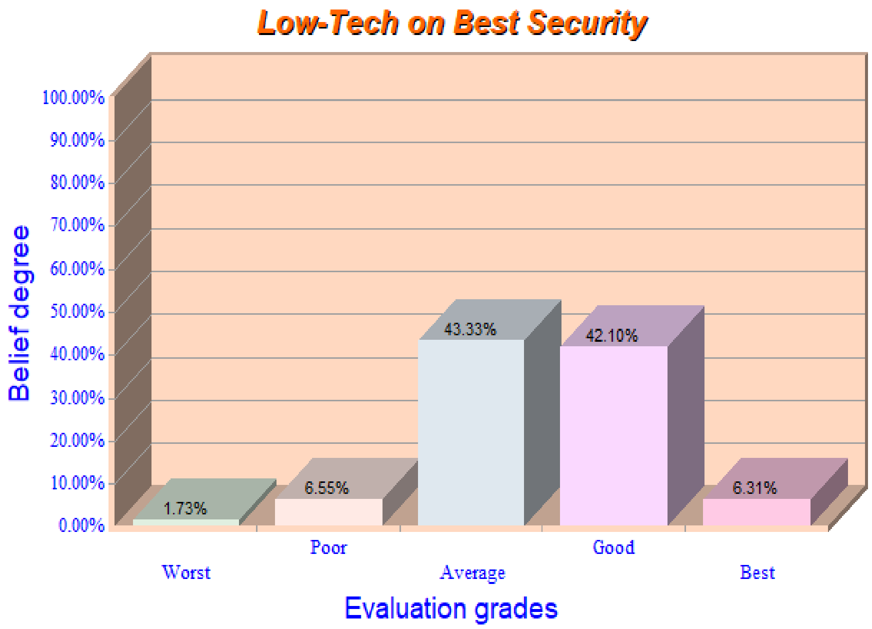


Figure 5.7: The Output Values of the Alternative "Low Tech Security"

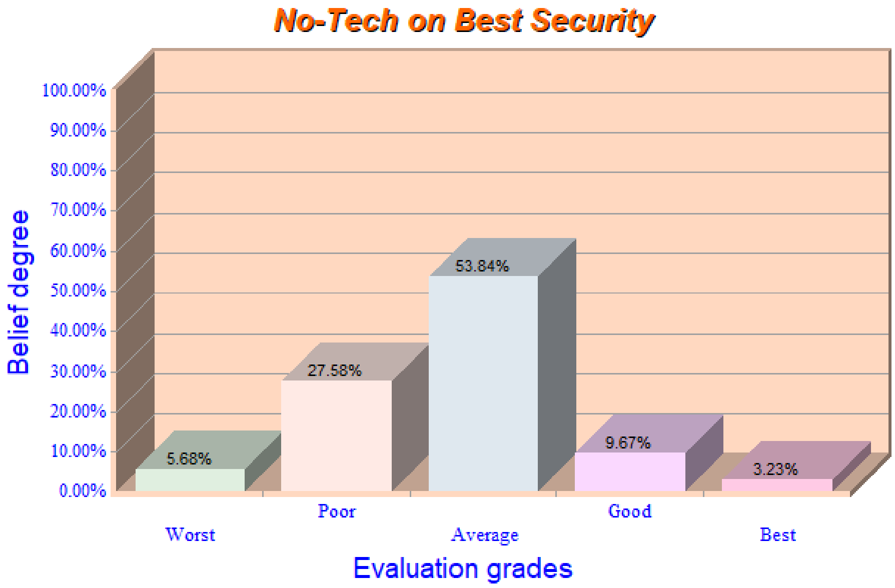
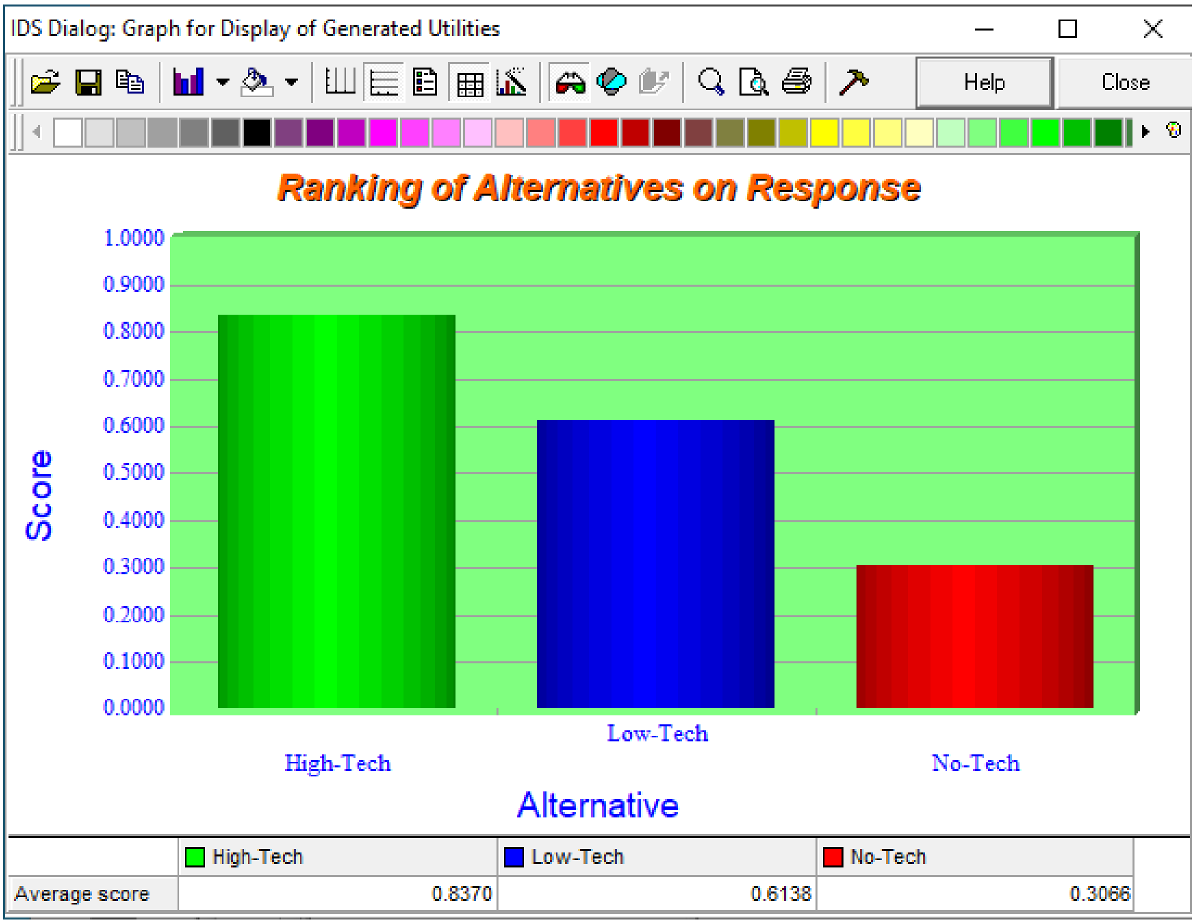


Figure 5.8: The Output Values of the Alternative "No Tech Security"

In the end, to determine the best security countermeasure for terrorist attacks, the three alternatives were ranked. To construct such a rank, a utility concept was used in this study and a set of utility values was given to the evaluation grades of the parent "High-Tech Security countermeasures in response to threat" as follows: {(*Best*, *1.00*), (Good, *0.75*), (*Average*, *0.50*), (*Poor*, *0.25*) and (*Worst*, *0.00*). By using the belief degree values described in Figure 5.5 for the alternative "High-Tech Security countermeasures in response to threat", the assessment value of this alternative was computed as follows:

Best	:	53.3% ×1.00	=0.533
Good	:	29.5%×0.75	=0.221
Average	:	15.3%×0.50	=0.077
Poor	:	01.6%×0.25	=0.004
Worst	:	00.00%×0.00	=0.000
Total			=0.835

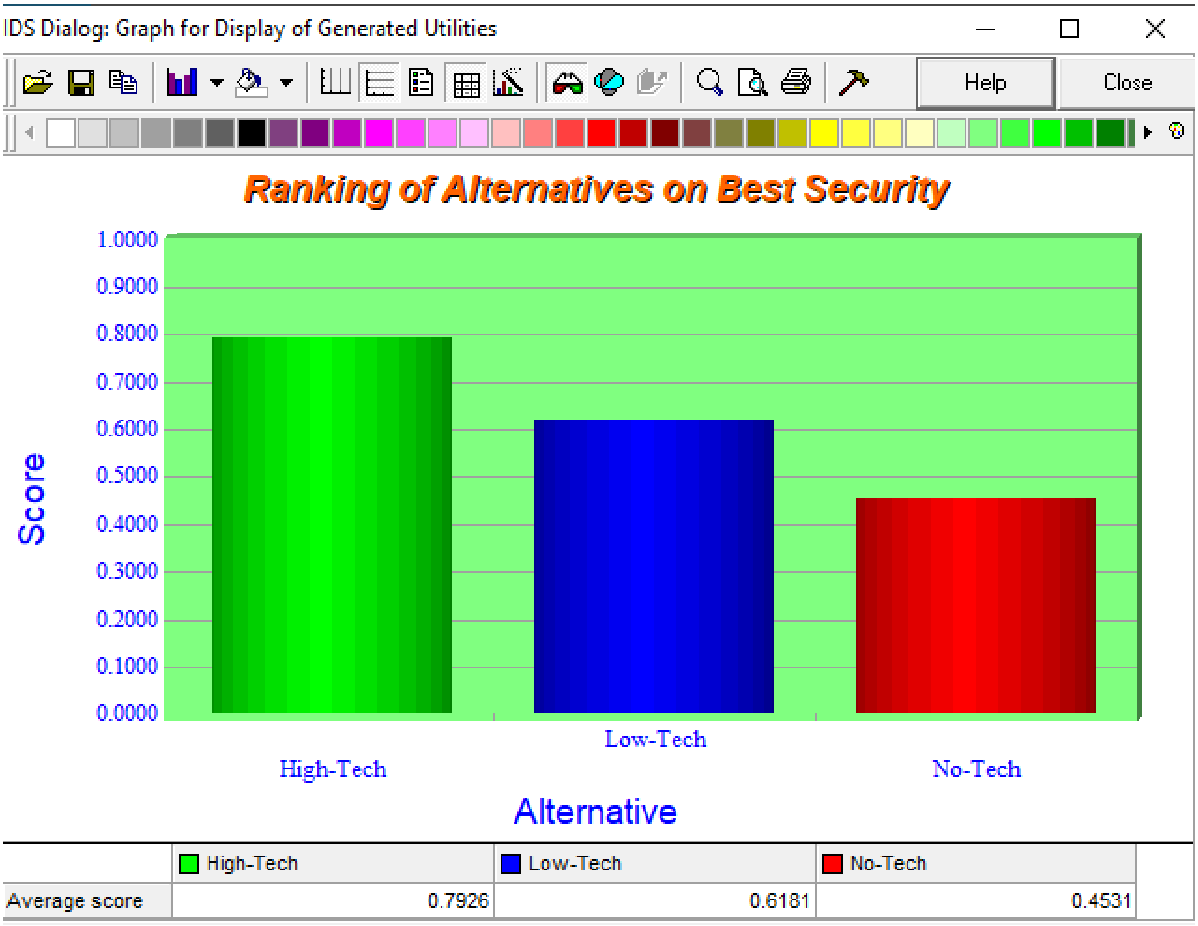


	🟩 High-Tech	🟦 Low-Tech	🟥 No-Tech
Average score	0.8370	0.6138	0.3066

Figure 5.9: The Ranking of the RTT

The assessment value of the alternative “High-Tech security countermeasures in response to threat” is known to be 0.835. A similar calculation technique was applied for determining the assessment values of the alternatives “Low-Tech security countermeasures in response to threat” and “No-tech security countermeasures in response to threat”. Figure 5.9 summarises the assessment values/average scores associated with the ranking of all alternatives in selecting the best security countermeasure for countering a terrorist attack. The alternative “High-tech Security

Countermeasure” was ranked in the first place (0.8370) followed by the alternative “Low-Tech Security Countermeasure” in the second place (0.6138) and the alternative “No-tech Security Countermeasure” in the last place (0.3066).



	🟩 High-Tech	🟦 Low-Tech	🟥 No-Tech
Average score	0.7926	0.6181	0.4531

Figure 5.10: The Ranking of the Best Security Countermeasures

Step 8: Sensitivity analysis

A sensitivity analysis process for this study is conducted using two axioms with the purpose of validating the proposed model. Such axioms are described as follows: **Axiom 1**: A slight increase/decrease of any sub-criterion should certainly result in the effect of a relative increase/decrease of the belief degree values of the evaluation grades of the alternatives. **Axiom 2**: Given the variation increase of subjective belief degree values of the least evaluation grade for any sub-criterion by percentages and decreasing the value of the highest evaluation grade by the same amount, its influence magnitude to the overall assessment score values should keep consistency.

Referring from above, there are two axioms used in this step as a mechanism for the model validation process. To validate the model using the axiom 1, the weight values of the main criteria under the column “0.0” in Table 5.23 are obtained using the AHP technique as described in Step 6 of Section 5.3 and they are considered as the original weight values in the sensitivity analysis process. From the original weight values, a new set of weight values is obtained using the percentage increase of 10%, 20% and 30%. As a result, the new weight values of the main criteria are summarised as shown in Table 5.23.

Table 5.23: Weight values of the main criteria for different percentages

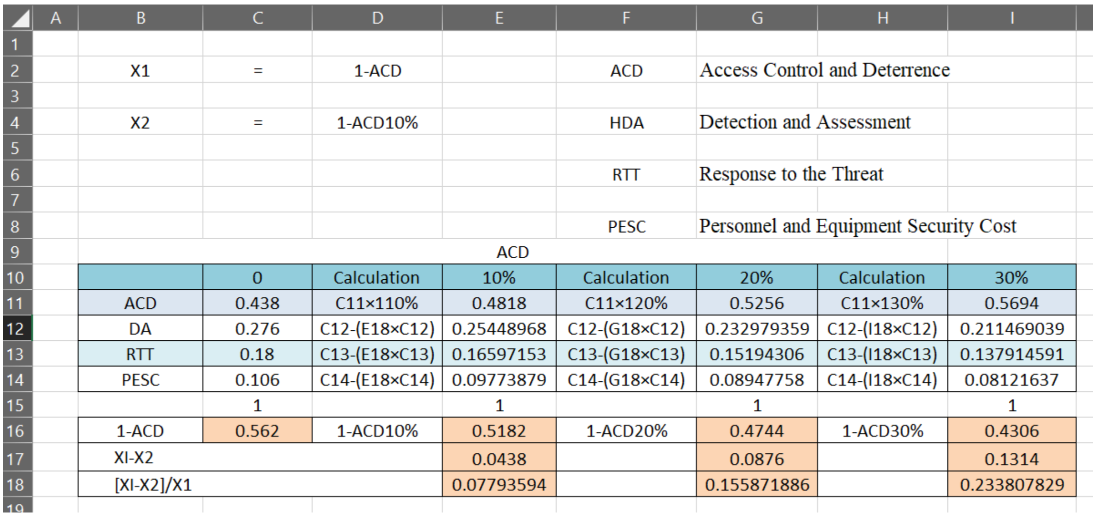
	Original Weight	New Weight		
	0.0%	10%	20%	30%
ACD	0.438	0.4818	0.5256	0.5694
DA	0.276	0.3036	0.3312	0.3588
RTT	0.180	0.198	0.216	0.234
PESC	0.106	0.1166	0.1272	0.1378

To validate the proposed model, a sensitivity analysis process is conducted using the *IDS* software. The alternative “No-Tech” is demonstrated as an example in this process. By using the new weight values of the four main criteria under the columns “10%”, “20%” and “30%” in Table 5.23, it is shown that the belief degree values of the evaluation grades of the parent node “Best Countermeasure” associated with the alternative “No-Tech” have certainly changed as shown in Table 5.24. By giving 10% of the weight change to the criterion “ACD” as an example, the evaluation grade “Poor” decreases from 5.69% to 4.88%. In a similar way, the same observation technique is applied in order to validate this model. Consequently, it shows that the proposed model is sensitive to the change of the weight values of the main criteria. In a similar way, the same technique is applied to construct the sensitivity analysis process to the other two alternatives. Further detailed outputs of this process are given in Figure 5.11. From the above, Axiom 1 is satisfied.

Table 5.24: A sensitivity analysis of the alternative “No-Tech” Weight value of the main criteria

Weight value of the main criteria		Evaluation Grades					
		Poor	Reasonably Poor	Average	Reasonably Good	Good	
0.00%	Main	5.69%	26.97%	52.09%	10.89%	4.36%	100.00%
10%	ACD	4.88%	26.75%	54.44%	10.22%	3.72%	100.00%
	DA	5.94%	26.82%	50.80%	11.44%	4.99%	100.00%
	RTT	5.96%	27.41%	51.63%	10.70%	4.29%	100.00%
	PESC	5.76%	26.83%	52.04%	11.05%	4.33%	100.00%

20%	ACD	4.10%	26.53%	56.68%	9.58%	3.11%	100.00%
	DA	6.20%	26.67%	49.46%	12.02%	5.66%	100.00%
	RTT	6.25%	27.88%	51.15%	10.50%	4.22%	100.00%
	PESC	5.83%	26.67%	51.98%	11.21%	4.30%	100.00%
30%	ACD	3.36%	26.34%	58.77%	8.99%	2.54%	100.00%
	DA	6.46%	26.49%	48.07%	12.62%	6.36%	100.00%
	RTT	6.54%	28.36%	50.66%	10.29%	4.14%	100.00%
	PESC	5.90%	26.52%	51.93%	11.38%	4.26%	100.00%



X1	=	1-ACD		ACD	Access Control and Deterrence		
X2	=	1-ACD10%		HDA	Detection and Assessment		
				RTT	Response to the Threat		
				PESC	Personnel and Equipment Security Cost		

ACD

	0	Calculation	10%	Calculation	20%	Calculation	30%
ACD	0.438	C11×110%	0.4818	C11×120%	0.5256	C11×130%	0.5694
DA	0.276	C12-(E18×C12)	0.25448968	C12-(G18×C12)	0.232979359	C12-(I18×C12)	0.211469039
RTT	0.18	C13-(E18×C13)	0.16597153	C13-(G18×C13)	0.15194306	C13-(I18×C13)	0.137914591
PESC	0.106	C14-(E18×C14)	0.09773879	C14-(G18×C14)	0.08947758	C14-(I18×C14)	0.08121637
	1		1		1		1
1-ACD	0.562	1-ACD10%	0.5182	1-ACD20%	0.4744	1-ACD30%	0.4306
XI-X2			0.0438		0.0876		0.1314
[XI-X2]/X1			0.07793594		0.155871886		0.233807829

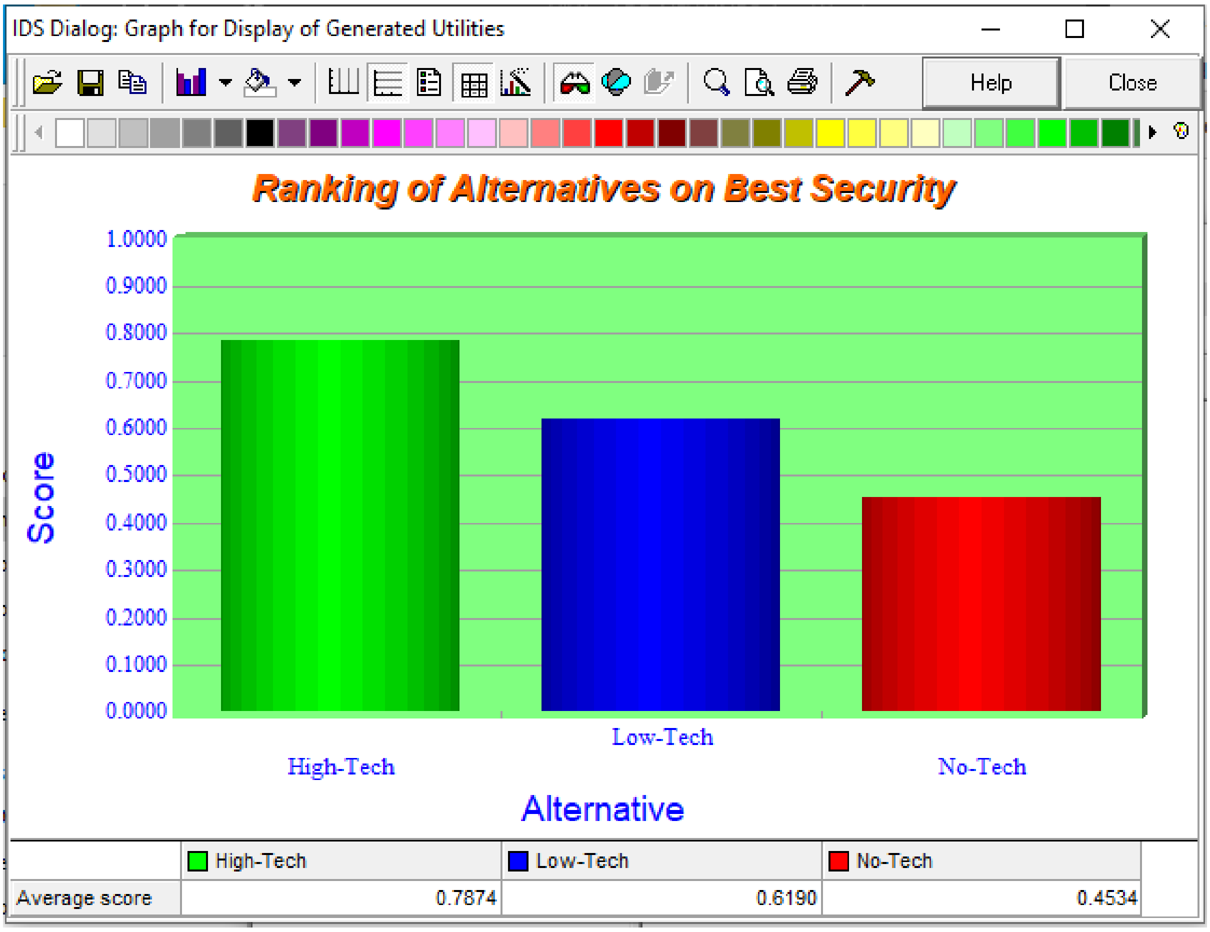
Figure 5.11: How to calculate the weight if ACD increase at 10%, 20%, and 30%

To demonstrate the validation process of this model using the Axiom 2, three sub-criteria “LL”, “HDA” and “Security” with respect to the alternative “No-Tech” are used as an example. The overall assessment score for this alternative is 45.31% (Figure 5.10). Given 30% increase of the belief degree values of the least evaluation grade for the three sub-criteria mentioned and increasing the value of the highest evaluation grade by the same amount, it shows that the overall assessment score for this alternative is changed. Two symbols are used for differentiating the original and new belief degree values. β_0 represents the original belief degree value for each evaluation grade, while β_1 describes the new belief degree values of the evaluation grade after applying the 30% increase of the least grade and increasing the value of the highest grade by the same amount. Tables 5.25, 5.26 and 5.27 show the belief degree values of $\beta 0$ and $\beta 1$ for the three different sub-criteria.

Table 5.25 shows the belief degree values of β_0 and β_1 for the sub-criterion “LL” with respect to the alternative “No TECH”. For such a criterion, the least evaluation grade is “*Poor*” and the highest evaluation grade is “*Good*”. By increasing 30% of the belief degree value of the grade “Reasonably Poor” change from 0.2554 to 0.2532, “Average” change from 0.6788 to 0.6814, and “Reasonably Good” change from 0.0657 to 0.0653. It shows that the overall assessment score for this alternative increase from 45.31% to 45.34%.

Table 5.25: LL for the alternative “No-TECH”

Weight value of the sub-criteria			Evaluation Grades					
%	Sub-Criteria		Poor	Reasonably Poor	Average	Reasonably Good	Good	
0%	LL	*β0*	0.00%	25.54%	67.88%	6.57%	0.00%	100.00%
30%	LL	*β1*	0.00%	25.32%	68.14%	6.53%	0.00%	100.00%



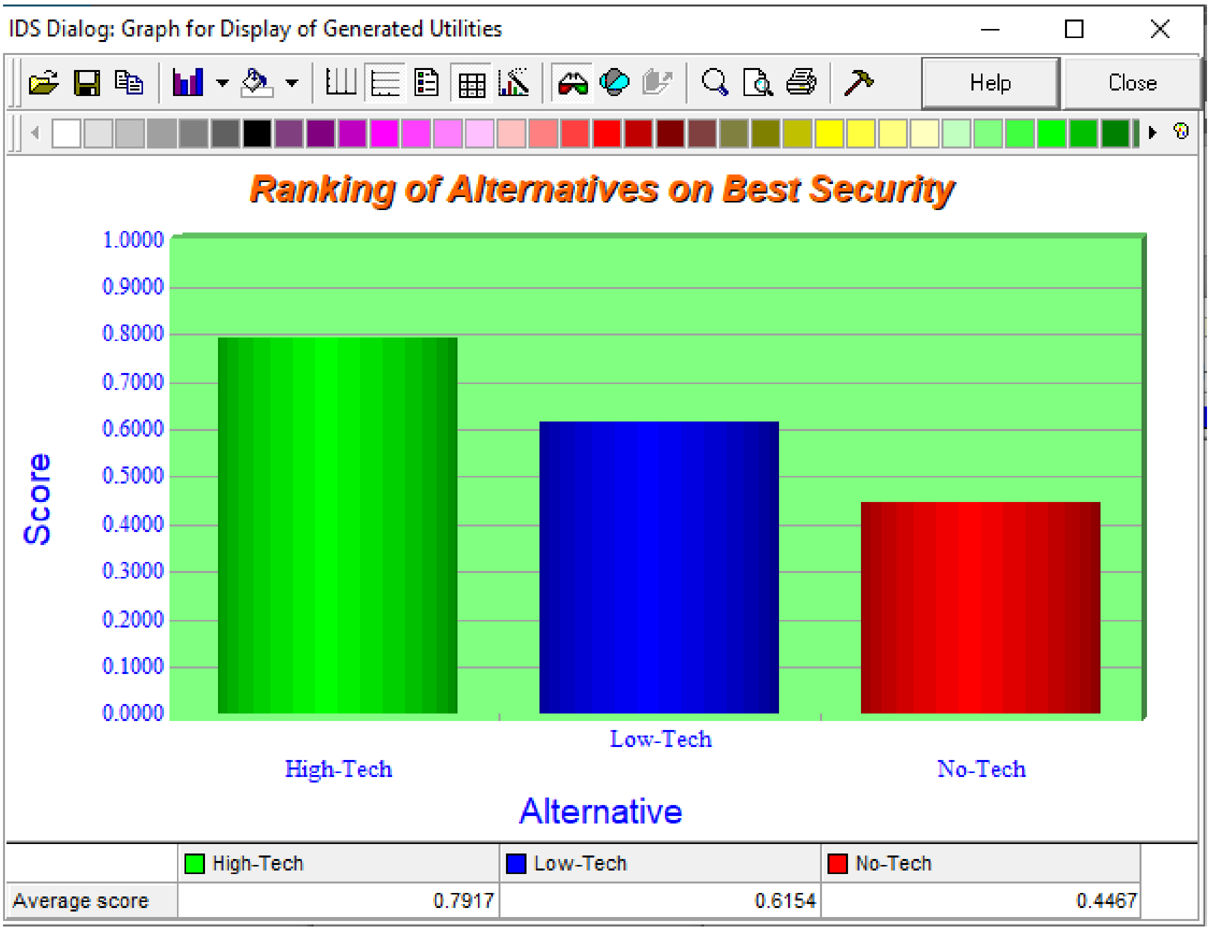
	🟩 High-Tech	🟦 Low-Tech	🟥 No-Tech
Average score	0.7874	0.6190	0.4534

Figure 5.12: Rank LL 30%

Next, the criterion “HDA” is examined with respect to the alternative “No-Tech”. The least evaluation grade of this criterion is “*Poor*” while the highest evaluation grade is “*Good*”. By increasing 30% of the belief degree value of the grade “Poor” change from 0.1046 to 0.1339, “Reasonably Poor” change from 0.2505 to 0.2090, “Average” change from 0.2518 to 0.2879, “Reasonably Good” change from 0.2266 to 0.2253, and decreasing the value of the grade "*Good*" by 0.00425 from 0.1865 to 0.1440, it shows that the overall assessment score for this alternative decrease from 45.31% to 44.67%.

Table 5.26: HDA for the alternative "No-TECH"

Weight value of the sub-criteria			Evaluation Grades					
%	SUB-CRITERIA		Poor	Reasonably Poor	Average	Reasonably Good	Good	
0%	HDA	*β0*	10.46%	23.05%	25.18%	22.66%	18.65%	100.00%
30%	HDA	*β1*	13.39%	20.90%	28.79%	22.53%	14.40%	100.00%



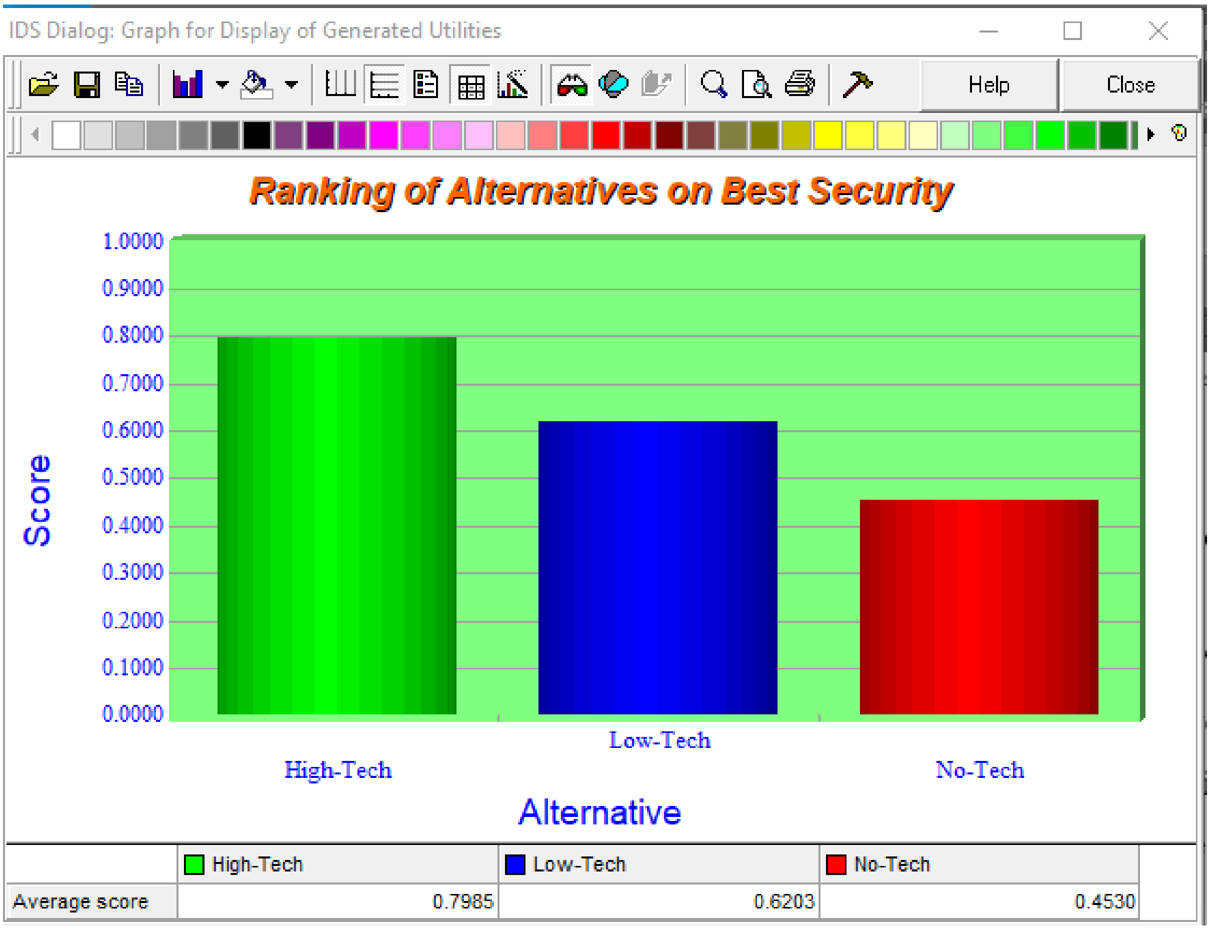
	🟩 High-Tech	🟦 Low-Tech	🟥 No-Tech
Average score	0.7917	0.6154	0.4467

Figure 5.13: HDA (30%) For the Ranking of Alternatives On Best Security

In a similar way, the criterion "Security" is examined with respect to the alternative "No-Tech". The highest evaluation grade of such a criterion is "*Poor*" while the least evaluation grade is "Good". By increasing 30% of the belief degree value of the grade "Poor" change from 0.1836 to 0.1701, "Reasonably Poor" change from 0.4536 to 0.4610, "Average" change from 0.3252 to 0.3494, "Reasonably Good" change from 0.00279 to 0.00145, and decreasing the value of the grade "*Good*" by 0.0047 from 0.0097 to 0.005, it shows that the overall assessment score for this alternative decrease from 45.31% to 45.30%.

Table 5.27: SECURITY for the alternative “No-TECH”

Weight value of the sub-criteria			Evaluation Grades					
%	SUB-CRITERIA		Poor	Reasonably Poor	Average	Reasonably Good	Good	
0%	SECURITY	$\beta 0$	18.36%	45.36%	32.52%	2.79%	0.97%	100.00%
30%	SECURITY	$\beta 1$	17.01%	46.10%	34.94%	1.45%	0.50%	100.00%



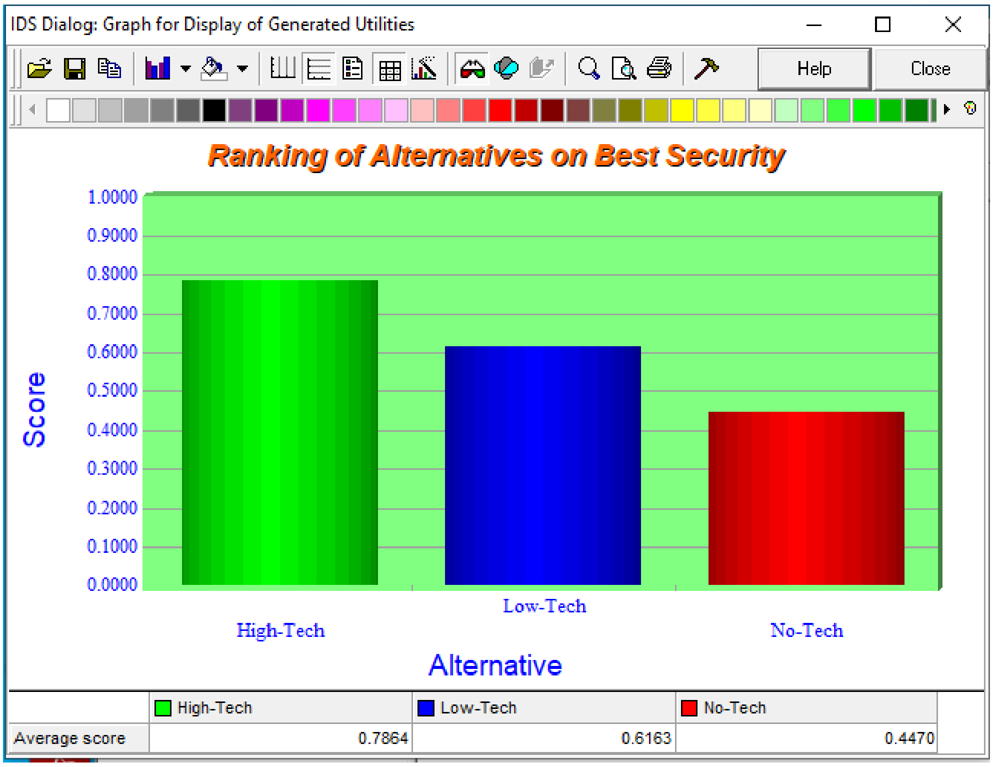
	🟩 High-Tech	🟦 Low-Tech	🟥 No-Tech
Average score	0.7985	0.6203	0.4530

Figure 5.14: Security (30%) for the Ranking of Alternatives on Best Security

Table 5.28 summarises the overall assessment score of the alternative “No-Tech” in three different scenarios after having the validation process described previously. The original overall assessment score has been obtained from Figure 5.10 (first scenario, *R1*). By reducing 30% of the belief degree values of the least evaluation grade and increasing the values of the highest evaluation grade by the same amount for the sub-criteria “LL” and “HDA” from Figure 5.15 (second scenario, *R2*), the overall assessment score of the alternative “No-Tech” is known to be 44.70%. In a similar way, the sub-criterion “Security” is added to the process together with the second scenario from Figure 5.16 (third scenario, *R3*), the overall assessment score for this alternative increase from 45.31% to 44.69%. According to the three overall assessment scores of this alternative, it can be ranked as follows: S*R1 > SR2 > SR*3. From the above, it can be seen that Axiom 2 is satisfied.

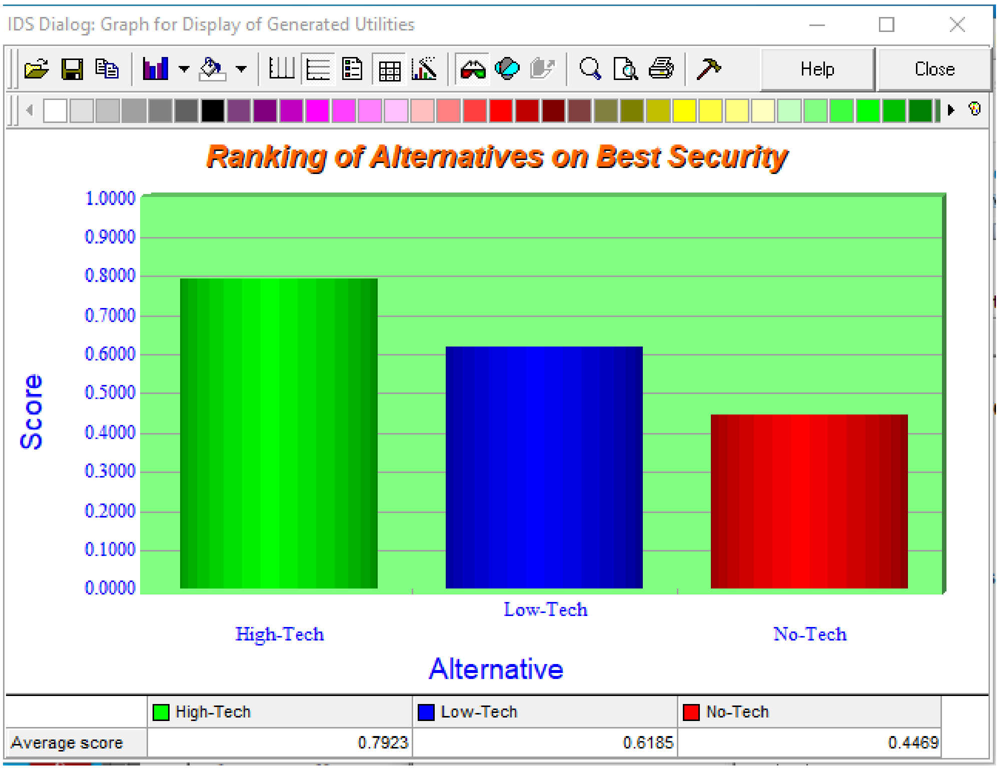
Table 5.28: The sensitivity analysis score of the alternative “No-Tech” in three scenarios

Scenario	Overall Assessment Score
The original overall assessment score, SR1	45.31%
The overall assessment score after applying the axiom 1 to the criteria "LL" and "HDA". SR2	44.70%
The overall assessment score after applying the axiom 1 to the criteria "LL", HDA and "Security".SR3	44.69%



	🟩 High-Tech	🟦 Low-Tech	🟥 No-Tech
Average score	0.7864	0.6163	0.4470

Figure 5.15: LL (30%) and HDA (30%) for the Ranking of Alternatives on Best Security



	🟩 High-Tech	🟦 Low-Tech	🟥 No-Tech
Average score	0.7923	0.6185	0.4469

Figure 5.16: LL (30%), HDA (30%) and Security (30%) for the Ranking of Alternatives on Best Security

5.4 Conclusions

A set of seven security countermeasure functions was conceptualised and articulated in this study for developing a comprehensive structural assessment framework. These criteria were hierarchically aggregated, through the use of an ER approach. Such an approach was used to aggregate the assessments criteria and rank the three alternatives, respectively. Besides, this study also demonstrated the application of the powerful decision analysis method, which was AHP. The necessary data of this study was fully obtained from six expert judgements. The results produced by the decision-making technique in this chapter are capable of assisting a port operator in making a rational decision in choosing the most effective terrorist security countermeasure.

After getting the results on the most effective terrorist security countermeasure, port operators are required to monitor the successful implementation of such a strategy. Further research can be conducted on another area of security which is cybersecurity instead of the physical terrorist attack aspect of security. Cyber security refers to the protection and the availability and integrity of the port information, port systems, confirmation of business made electronically and protecting the usefulness of cyber assets (Boyes *et al*., 2016). In January 2012, the World Economic Forum considered cyber-attacks as the fourth top global risk. Last year, on 27 June 2017, Port of Los Angeles was attacked by a ransomware called NotPetya, which forced the port operator to shut down the port operation for 3 days and suffered a loss of around USD300 million (CBS Los Angeles, 2018).

Chapter 6: Contributions and Findings

Summary

This chapter briefly summarises the risk assessment and decision-making approaches and techniques in all previous chapters which would be beneficial in Port Facility security fighting terrorism, design, operation and management. The areas, which require more effort to be devoted to the improvement of the developed approaches, are outlined.

6.1 Contribution of Research to Knowledge

6.1.1 Ports Functions and Their Categories

This research is a study on port security, where the chosen port is situated on the Peninsular Malaysia facing the narrow and busy Straits of Malacca. It was one of the main trading ports since the British colonial times and is now one of the busiest ports in Southeast Asia. A port has four main functions, which are: it ensures the legal and economic interests of the State are protected, promotes the State’s interests in the wider scope of the regional economy, handles imports and exports of goods, and acts as a trade hub for the State as well as the region. A port generally has four categories of facilities, which are the port gate(s), the wharf on site, the yard on site and the administrative facilities on site. As its name implies, the port gate(s) act as the entry and exit points and the rest of the facilities are within its controlled area. The gate controls access to the port’s other facilities. The wharf on site is usually the fixed platform where the goods are loaded onto and unloaded from the ships berthed there. The yard on site acts as storage, transit areas of loading and unloading of goods onto other and connecting mode of transportation. The administrative facilities on site comprise the resources management offices including the safety and security offices. By virtue of its roles, a port handles a State’s trades comprising a multitude of invaluable cargoes. This in itself may attract attacks from criminal or terrorist elements, depending on their respective motivations and objectives.

6.1.2 Containerisation and its advantages

Historically, since the middle of the twentieth century the introduction of “intermodalism” in handling of goods or cargo has contributed to the growth of trades and ports. Prior to that, cargoes were held in small boxes of various sizes. In ancient times goods were put in barrels, sacks or wooden crates and were individually loaded onto and unloaded from ships. Later on, there were efforts to bundle the goods in barrels, sacks and wooden pallets by using ropes. The loading and unloading processes were labour intensive. Intermodalism started in 1956 in the US when cargoes were put into containers and loaded onto ships. Intermodalism hinges on the use of containers to move cargoes. Initially containers varied in sizes. Later on, the container size was standardised. The popular sizes are the 20-foot and 40-foot long. They are measured and called TEUs (twenty-foot equivalent units) and FEUs (forty-foot equivalent units). Containerisation brings benefits in terms of efficient stacking and speedy loading and unloading. The use of containers as a method of transportation of goods promotes trade and eventually 90% of cargoes in recent years have been put in containers. With giant cranes, loading and unloading of goods uses much less labour and is seamless along the supply chain. In addition to efficient movement, there is less theft and loss of such cargoes.

6.1.3 Terrorist attacks on port

Being a place where the amount and values of the cargoes are high, it may attract "an attacks" either by criminals or terrorists. Attacks on ports are "attractive" to both criminal gangs and terrorist groups as the "yield" is high. Criminals are financially motivated and goods they grab from such attacks bring them money. Terrorists on the other hand are politically motivated and attacks on ports or against shipping can cause great publicity to their cause due to the great damage such attacks can inflict on the port facilities as well as trades. Port stakeholders need to be vigilant against attacks be it by criminal gangs or terrorist groups or both. In addition to the efficient running of ports in terms of management and operational processes, the port authority needs to adopt efficient and effective security systems to prevent such potential attacks. To enable the port authority to institute efficient and effective safety and security systems, it has to plan and make the necessary preparations against such attacks. It has to identify the types of attacks, assess its (the port's) overall risk and institute countermeasures.

6.1.4 Attack Scenarios

This study identifies four potential attack scenarios namely suicide attacks using tampered trucks targeting port entrances, hijacking of a vessel and attack on the wharf on site after overcoming security guards, smuggling in tampered containers including explosives and conduct the attack from inside, and more complex attack operations involving infiltration of terrorists into a port area and carrying out attacks from inside the port area. Suicide attack is easy to carry out but it carries a high risk of failure. The impact and damage are high especially at the entrances. Hijacking a vessel is harder to carry out but it can cause great damage, while the last two require inside help.

6.1.5 Maritime Security and Threats in the Region and the Port under Study

The port under this study is located on the Straits of Malacca where it is a 600-mile long narrow sea passage having three countries; Indonesia, Malaysia and Singapore bordering it. It is the busiest maritime sea-lane handling world trade. In terms of threats to the port security, the study concludes that the port under study faces pirate rather than terrorist attacks. Most of the “terror” groups in Southeast Asia are land-lubbers and attack land targets with the exception of the Sulu Sea where kidnap-for-ransom attacks are quite frequent. Piracy, by definition, is not classified as terrorism. Acts of piracy are carried out by criminals and they are financially motivated. Post 9/11, the United States has pressed for transnational efforts in combating terrorism. Despite some reservations by the littoral countries on the counterterrorism measures proposed by the U.S., some agree measures do suppress the incidences of piracy in the region especially the Straits of Malacca. The 2004 tsunami and the subsequent peace agreement between the Indonesian government and its autonomy-seeking Free Acheh Movement reduced the incidences of piracy further. So far there has been no direct attack by criminals or terrorists on the port under study itself but the threat of such attacks in the future cannot be totally ruled out.

6.2 Findings

6.2.1 The Most Likely Target of Attacks

Based on the analysis of the collected data, this study finds that the most likely target of an attack to the port under study is the wharf on site. Attacks on wharf would cause greater damage than other possible attacks and the consequences are worse to the operators, trades etc. The study also finds the possible and most likely type of attacks on the wharf are, 1) Vessel Hijacking, 2) Collision attack (may involve explosion and fire), and 3) an attack using heavy weapons.

6.2.2 The Countermeasures

The port under study has existing countermeasures against the four possible types of attacks. With regards to the first two ‘threats” namely an attack on wharf using vessels and an attack using weapons the response team are found to be adequately trained. They also have adequate knowledge and skills in detecting and deterring possible attacks and take the necessary actions during attacks such as evacuation procedures and so on. The response team also has adequate skills and knowledge to handle “threats” or attacks in the form of explosions or fires.

The study finds that, in terms of countermeasures the Port under study is not vulnerable to terrorist attacks. The study shows that there is 88.9% of the probability of the countermeasures being effective. However, there is a small chance of 11.1% of an attack, if it indeed happens for a terrorist attack to be successful. The port is not vulnerable to the threat of explosions. The analysis finds that there is 89.2% probability the countermeasures are effective.

The port is also not vulnerable to the threat of fire, with the countermeasures against fire having 81.7% probability of success.

6.2.3 Ranking of Security Effectiveness

Security countermeasures are categorised into high-technology, low-technology and no-technology types. Examples of high-technology security countermeasures are card technologies, access credentials, security command, photo ID detectors, sensors etc., low-technology security countermeasures are locks, revolving doors, barriers, mechanical or electronic turnstiles, vehicular patrol etc. while no-technology security countermeasures are security policies, awareness programmes, guards, security staffing etc. The study finds that high-technology countermeasures are ranked first in terms of security effectiveness (with score of 0.7926 out of the scale 0.00-1.00, 1.00 being the most effective), followed by low-technology countermeasures (with the score 0.6181) and no-technology last (with the score 0.4531). Some would argue with the characteristic of all the alternative shown, anybody can predict the result of the rank and there is no need to conduct a study. However, by using this method, besides able to see the ranking itself, the exact numerical extent of the high tech better than the low tech and better than the no tech would be shown. From those numbers, how much the differences between each of the alternative is shown and from there it is easier for researcher to quantify their differences.

Overall the conclusions of the research are as follows:

a. The types of possible attacks against the port under study are the attack on wharf on site using vessels, the attack on wharf on site using weapons, explosions and fires.
b. The most vulnerable facility of the port under study that may "attract" attacks is the wharf on site
c. The most vulnerable facility in terms of security is the wharf
d. The countermeasures are adequate and effective in thwarting possible attacks
e. The most effective countermeasures are the high-technology measures.

6.3 Novelty

6.3.1-Likelihood and the consequence of terrorist attack

This study is focusing on terrorist attack in container port facilities which started with using BN and RCA to calculate the likelihood of terrorist attack (in chapter three) and using a combination of ETA and BN to calculate the consequence of the attack (in chapter four). The use of BN and RCA enables us to know or identify which component of the port facilities has the highest probability to be attacked. The event tree diagram creates multiple path starting with initiating event (the attack) and completed with BN in analysing the security countermeasure's ability in countering the attack. Pereira (2015) have done the same approach by combining a bow tie model with Bayesian. Such integrated model combines three method (Fault Tree Analysis, Even Tree Analysis and BN) were then simplified by using only two method which is ETA and BN. For further illustration of the model, see Figure 4.3.

6.3.2-New Security Function

Chapter five detailed about Norman's (2015) list of 7 security countermeasure function (which is Access Control, Deterrence, Detect Attack, Assessment, Delay, Respond And Collecting The Evidence) being grouped into just three main criteria (which is Access Control, Delay and Deterrence (ACD), Detection and Assessment (DA), Response to the Threat (RTT)). In addition of these 3 main criteria, another main criterion was added (Personnel and Equipment Security Cost). This new criterion covers about its training cost, salary, new equipment installation fees and maintenance fees which is important element to decision maker to select which is the best security countermeasure.

6.4 Recommendations for Future Research

This study is limited in scope to the physical threats against a port. The focus is on the degree of risk faced by its (the port's) components and the efficiency and effectiveness of its security countermeasures. The Bayesian Network model and its associate probability components are excellent tools for assessing the risks and predicting the probability of attacks as well evaluating the effectiveness of countermeasures.

As for the future, the researcher suggests that another and more current threat be considered for further research. Cyberterrorism, despite being a late-comer to the security scene, should be properly studied in respect of port security. Cybersecurity, in this age of digitalisation, refers to the security of information and data. Modern port operations generate and deal with a lot data and information systems involving communication, navigation and loading information on board ships, navigation data in the cloud, systems at major ports and maritime computer systems at maritime companies. Perpetrators of cyber-crimes are nation states, rival companies, criminal organisations, free-lance hackers and insiders too such as corrupt employees. The motives can be financial, political or mere accidents caused by careless employees.

In 2017, a cyberterrorist attack happened in LA port resulting in billions of U.S. dollar loss. There was no bomb or a terrorist attack using armoury, but they were merely using the virus. Those attacks show how terrorists are able to economically damage a country's ports without risking the perpetrators' lives. There have been dozens of researches done on cyber-terrorism (Lewis, 2002), but none of them focuses on maritime let alone seaport except for two publications. First from J. Ahokas and T. Kisiski about "Cybersecurity in Ports" hazard report in 2017 (but it only gives a definition of cyberterrorism from a previous paper and never presents with new knowledge about cyberterrorism with maritime let alone port). Second, a publication from Yunos, Z., Ahmad R., and Abd. Aziz, N. A., about "Definition and Framework of Cyber Terrorism" paper in 2013 (it develops a framework of cyber terrorism and was published by Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) that focusing on maritime counter-terrorism but never present with new knowledge about cyberterrorism with maritime). Since cyber-attacks can cause 1) massive financial losses, 2) thefts of cargo or information malfunctions and 3) company disruptions, a Bayesian Network and its associated tools can be used in assessing threats of cybercrimes.

*There is a lot of paper related to maritime cybersecurity but none of them ever mention cyberterrorism.

6.5 Research summary

This study shows that there is a need to develop a simple and effective assessment tool that would allow port operators to operate a resilient security countermeasure to terrorist attacks. The problem faced by port operators has been characterised by subjective judgements and literature surveys. The proposed models produced valuable results for assisting port operators in the decision-making process concerning targets, evaluations and effectiveness concerning the security countermeasure. The outcome can be used by port operators to assess their security countermeasures accurately especially when they have added a new installation for security up-grade purposes. Finally, this research formulates a platform for port operators to improve their security system operations using decision making techniques.

Reference

Acciaro, M., & Patrizia, S. (2013), “Maritime Supply Chain Security: A Critical Review”, *International Forum on Shipping, Ports and Airports (IFSPA) 2013,* In *Trade, Supply Chain Activities and Transport: Contemporary Logistics and Maritime Issues,* Vol. 636.

Acharya, Arabinda. Whither Southeast Asia Terrorism? Vol. 6. World Scientific, 2014.

Ahokas, J., and Kisiski, T., (2017), Cybersecurity in Ports, Publications of the Hazard Project. Available from: https://www.utu.fi/en/sites/hazard/publications/Documents/HAZARD%20Publication%203%20CYBERSECURITY%20IN%20PORTS.pdf

Alberts, C.J., Behrens, S.G., Pethia, R.D. and Wilson, W.R., 1999. *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0* (No. CMU/SEI-99-TR-017). Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Alderton, P., (2008), Port Management and Operations. 3rd edition, Informa, London, pp. 224.

Alexander, M., 2012. Decision-Making using the Analytic Hierarchy Process (AHP) and SAS/IML®, Paper SD-04, SESUG 2012.

Andreassen, S., Jensen, F. V., Andersen, S. K., Falck, B., KJMl ff, U., Woldbye, M., SuensenA, ., Rosenfalck, A. and Jensen, F. (1989), "MUNIN - An Expert EMG Assistant", Computer-aided Electromyography and Expert Systems, Desmedt, J. E. (eds.), Elsevier Science Publishers, Amsterdam, pp. 255-277.

Balfour, A.J., 1917. The Balfour Declaration. London: British Foreign Office.

Barton, D. N., Saloranta, T., Moe, S. J., Eggestad, H. O., Kuikka, S., 2008. Bayesian Belief Networks As A Meta-Modelling Tool In Integrated River Basin Management — Pros and Cons in Evaluating Nutrient Abatement Decisions Under Uncertainty in a Norwegian River Basin. Ecological Economics 66: 91-104.

Bayes, T., Price, R., 1736. An Essay Towards Solving a Problem in The Doctrine of Changes. Philosophical Transactions (1683-1775) (53): 370-418.

Bhattacharya, A., Geraghty, J., Young, P., & Byrne, P. J. (2013), "Design of a Resilient Shock Absorber for Disrupted Supply Chain Networks: A Shock-Dampening Fortification

Framework for Mitigating Excursion Events", *Production Planning & Control*, Vol. 24, No. 8-9, pp, 721-742.

Bichou, K. and Gray, R., (2004), A Logistics and Supply Chain Management Approach to Port Performance Measurement. *Maritime Policy & Management*, *31*(1), pp.47-67.

Bjorgo, T. (ed.) et. al., Root Causes of Terrorism, Routledge, NY (2005)

Borsuk, M.E., Schweizer, S. and Reichert, P., 2012. A Bayesian Network Model For Integrative River Rehabilitation Planning and Management. *Integrated Environmental Assessment and Management*, *8*(3), pp.462-472.

Boyes, H., Isbell, R. and Luck, A., (2016), Code of Practice. Cyber Security for Ports and Port Systems. *Institution of Engineering and Technology*, *28*, p.2016.

Bradford, John F. "Japanese Anti-Piracy Initiatives in Southeast Asia: Policy Formulation and the Coastal State Responses." *Contemporary Southeast Asia* (2004): 480-505.

Brandt, P.T. and Sandler, T., 2009. Hostage Taking: Understanding Terrorism Event Dynamics. Journal of Policy Modelling, 31(5), pp.758-778.

Brewer, D. F. C. 2003, "EFT Evaluation: A Craftsman-Led Approach", Gamma Secure Systems Limited - Specialists in Information Security Management Systems (Iso/Iec 27001). Available from (Feb 10, 2003) http://www.gammassl.co.uk/research/archives/early/hot3.php

Bromley, J., Jackson, N. A., Clymer, O. J., Giacomelloa, A. M., Jensen, F. V., 2005. The Use of Hugin to Develop Bayesian Networks as an Aid to Integrated Water Resource Planning. Environmental Modelling and Software 20: 231-242.

Brooks, M.R., Pelot, R., 2008. Port Security: A Risk-Based Perspective. In: Talley, W.K. (Ed.), Maritime Safety. Security and Piracy, LLP, London, pp. 195–216.

Brown, K.E., 2011. Muriel's Wedding: News Media Representations of Europe's First Female Suicide Terrorist. *European Journal of Cultural Studies*, *14*(6), pp.705-726.

Brown, M.D. and Loewe, A.S., 2003. Reference Manual To Mitigate Potential Terrorist Attacks Against Buildings. *USA, FEMA*, pp.4-19.

Byrne, J. and Hoffman, S.M. eds., 1996. *Governing the Atom: The Politics of Risk* (Vol. 7). North Atlantic Books

Cagno, E., Caron, M., Mancini, M. and Ruggeri, F. (2000), "Using MP in Determining the Prior Distributions on Gas Pipeline Failures in a Robust Bayesian Approach", Reliability Engineering & System Safety, Vol. 67, No. 3, pp. 275-284.

Caldeirinha, V., Felício, J.A. and Dionísio, A., (2013), The Container Terminal Characteristics and Customer's Satisfaction (No. 2013_14). University of Evora, CEFAGE-UE (Portugal).

Carmona, G., Varela-Ortega, C., Bromley, J., 2011. The Use of Participatory Object-Oriented Bayesian Networks and Agro-Economic Models for Groundwater Management in Spain. Water Resources Management 25(5): 1509-1524.

Castelletti, A. and Soncini-Sessa, R., 2007. Bayesian Networks and Participatory Modelling in Water Resource Management. *Environmental Modelling & Software*, *22*(8), pp.1075-1088.

CBS Los Angeles ., 2018. "White House: Russia Behind Cyber-Attack Which Shut Down Port Of LA". Available from: https://losangeles.cbslocal.com/2018/02/16/russia-cyber-attack-port-of-la/

Chase, A., 2003. Harvard and the Unabomber: The Education of an American Terrorist. New York: WW Norton.

Chase, A., 2004. Book Review of Harvard and the Unabomber: The Education of an American Terrorist. Western Criminology Review, 5(1), pp.70-74.

Chitadze, N., 2014. International Terrorism-Main Threat to The World Community in the XXI Century. Journal of Social Sciences, 3(1), pp.19-26.

Clemens, P.L.; Rodney J. Simmons (March 1998). "System Safety and Risk Management". *NIOSH Instructional Module, A guide for Engineering Educators* (Cincinnati,OH: National Institute for Occupational Safety and Health): IX–3 – IX–7.

Code, I.S.P.S., (2003). International Ship and Port Facility Security Code and SOLAS Amendment 2002. *International Maritime Organization (IMO)*. 2003 Edition, http://www.ubak.gov.tr/BLSM_WIYS/DISGM/tr/HTML/20130304_142647_66968_1_67502.pdf

Crime Museum. 2016. "Types of Terrorism". Crime Museum. Retrieved 2016-07-13. https://www.crimemuseum.org/crime-library/terrorism/types-of-terrorism/

Defense Technical Information Center (DTIC) 2003 “A Military Guide to Terrorism in the Twenty-First Century” A U.S. Army Training and Doctrine Command Handbook. Available from August, 2003 http://www.dtic.mil/dtic/tr/fulltext/u2/a426964.pdf

Desker, B., 2007, “Re-thinking the Safety of Navigation in the Malacca Strait in Kwa Chong Quan and John K. Skogan (eds.)”, Maritime Security in Southeast Asia, Routledge, NY Barry Desker (2007)

Ericson, C.A., 2015. *Hazard Analysis Techniques for System Safety*. John Wiley & Sons.

Eski, Y., (2011), Port of Call: Towards a Criminology of Port Security. *Criminology & Criminal Justice*, *11*(5), pp.415-431.

Ezell, B.C., Bennett, S.P., Von Winterfeldt, D., Sokolowski, J. and Collins, A.J., 2010. Probabilistic Risk Analysis and Terrorism Risk. *Risk Analysis: An International Journal*, *30*(4), pp.575-589.

Feng, L., Jun-Qi, H., & Dao-Ming, X. (2010), "Managing Disruption Risks in Supply Chain", *2010 IEEE International Conference* in *Emergency Management and Management Sciences (ICEMMS)*, pp. 434-438.

Galić, S., Lušić, Z. and Skoko, I., 2014. “The Role and Importance of Safety in Maritime Transportation”. *Book of*, p.186. (Paper Presented to the 6th International Maritime Science Conference, 28-29 April 2014, Solin, Croatia).

Global Terrorism Database (2014a), "Line Chart Result of 48990 - Terrorist Event since 2004-2013." Available at (June 7, 2014), (http://www.start.umd.edu/gtd/search/results.aspx?start_yearonly=2004&end_yearonly=2013&start_year=&start_month=&start_day=&end_year=&end_month=&end_day=&asmselect0=&asmselect1=&dtp2=all&success=yes&casualties_type=b&casualties_max=).

Global Terrorism Database (2016), "Maritime Event - Terrorist Event since 2001-2015." Available at (Jan 27, 2016), (https://www.start.umd.edu/gtd/search/Results.aspx?page=2&search=maritime&count=100&expanded=no&charttype=line&chart=overtime&ob=GTDID&od=desc#results-table)

Gross, L., 1948. The Peace of Westphalia, 1648–1948. American Journal of International Law, 42(1), pp.20-41.

Grzelakowski, A.S., 2014. Container Shipping Operators as Integrators of Global Logistics Supply Chains. *Logistics and Transport*, *21*.

Guevara, C., 2002. Guerrilla Warfare. Rowman & Littlefield Publishers. https://www.marxists.org/history/erol/china/che.pdf

Gowsalya R S, & Asma V.K.M (2017) "A Study on Training Effectiveness", *International Journal for Research Trends and Innovation* (www.ijrti.org), Vol. 2, Issue. 5. Available from: http://www.ijrti.org/papers/IJRTI1705037.pdf

Haapasaari, P. and Karjalainen, T.P., 2010. Formalizing Expert Knowledge to Compare Alternative Management Plans: Sociological Perspective to the Future Management of Baltic Salmon Stocks. Marine Policy, 34: 477-486.

Haapasaari, P., Michielsens, C.G.J., Karjalainen, T. P., Reinikainen, K., and Kuikka, S., 2007. Management Measures and Fishers' commitment towards sustainable exploitation: A Case Study of Atlantic Salmon Fisheries in the Baltic Sea. ICES Journal of Marine Science, 64: 825-833.

Heckerman, D., Mamdani, E. H., and Wellman, M. (1995), "Real-World Applications of Bayesian Networks", Communicationso FACM, Vol. 38, No. 3, pp. 24-26.

Helle, I., Lecklin, T., Jolma, A., Kuikka S., 2011. Modelling The Effectiveness of Oil Combating from an Ecological Perspective - A Bayesian Network for the Gulf of Finland; the Baltic Sea. Journal of Hazardous Materials, 185(1): 182-192.

Here Begynneth, A. and Hood, R., 2018 "One Man's Terrorist is Another Man's Freedom Fighter": Deciding What is and What is not an Act of Terror. Available at https://gesteofrobinhood.com/2018/04/30/one-mans-terrorist-is-another-mans-freedom-fighter-deciding-what-is-and-what-is-not-an-act-of-terror-tyler-welch/

Hilbrenner, A. and Schenk, F.B., 2010. Introduction: Modern times? Terrorism in Late Tsarist Russia. Jahrbücher für Geschichte Osteuropas, (H. 2), pp.161-171. https://edoc.unibas.ch/17637/1/JGO%202010-2_Einleitung.pdf

Ho, J.H., 2006. The security of sea lanes in Southeast Asia. *Asian Survey*, *46*(4), pp.558-574.

Ho, M.W. and Ho, K.H.D., (2006), Risk Management in Large Physical Infrastructure Investments: The Context of Seaport Infrastructure Development and Investment. *Maritime economics & logistics*, *8*(2), pp.140-168.

Hong, Eun-Soo; In-Mo Lee, Hee-Soon Shin, Seok-Woo Nam, Jung-Sik Kong (2009). "Quantitative Risk Evaluation Based on Event Tree Analysis Technique: Application to the Design of Shield TBM". *Tunneling and Underground Space Technology* **24** (3): 269–277. doi:10.1016/j.tust.2008.09.004.

Hora, S.C., 2009. Expert Judgment in Risk Analysis.

Howard, R. A. (1968), "The Foundations of Decision Analysis". IEEE Transactions on Systems, Science and Cybernetic, No. 4, pp. 211-21 9.

Høyland, Arnljot, and Marvin Rausand. *System Reliability Theory: Models and Statistical Methods*. Vol. 420. John Wiley & Sons, 2009. Qualitative System Analysis Chapter 3 p. 109-118

Hu, Y. & Zhu, D. (2009), "Empirical Analysis of The Worldwide Maritime Transportation Network", *Physica A: Statistical Mechanics and Its Applications,* Vol. 388**,** pp. 2061-2071.

Janczewski, L. ed., 2007. *Cyber Warfare and Cyber Terrorism*. IGI Global.

Jenkins, B.M. and Johnson, J., 1975. International Terrorism: A Chronology, 1968-1974 (Vol. 1597, No. DOS/ARPA). RAND CORP SANTA MONICA CA. http://www.dtic.mil/dtic/tr/fulltext/u2/a008354.pdf

Jenkins, J. P., (2017), “Terrorism”, Available at (May 31, 2017), https://www.britannica.com/topic/terrorism

Jensen, F.V. and Nielsen, T.D (2007), *Bayesian Networks and Decision Graphs.* 2nd ed. Springer Science and Business Media, LCC. ISBN: 0387682813.

Jiaqi, Sun., (2017), “Risk Assessment Methodologies and Techniques by Category and Industry” of NOSA Group of Companies, Available at (July 27, 2017), (http://blog.nosa.co.za/blog/risk-assessment-methodologies-and-techniques-by-category-and-industry)

Jonathan, A.E. and Michael, N.T., 2014. An Electronically Controlled Automatic Security Access Gate. Leonardo Journal of Sciences, 25, pp.85-96.

Jordan, M.I. ed., 1998. *Learning in Graphical Models* (Vol. 89). Springer Science & Business Media.

Keeney, R.L. and Raiffa, H., (1976), *Decisions with Multiple Objectives: Preference and Value Tradeoffs*, Wiley: New York.

Kennett, M., Letvin, E., Chipley, M. and Ryan, T., 2005. Risk Assessment: A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings. *FEMA Risk Management Series*.

Kiras, J.D., 2006. *Special Operations and Strategy: From World War II to the War on Terrorism*. Routledge.

Kjaerulff, U.B. and Madsen, A.L. (2005), *Probabilistic Networks — An Introduction to Bayesian Networks and Influence Diagrams*. Aalborg University Press, Denmark.

Kleindorfer, P. R., & Saad, G. H. (2005),"Managing Disruption Risks in Supply Chains", *Production and Operations Management*, Vol.14, No. 1, pp. 53-68.

Kuikka, S., Hildén, M., Gislason, H., Hansson, S., Sparholt, H., Varis, O., 1999. Modelling Environmentally Driven Uncertainties in Baltic Cod (Gadus morhua) management by Bayesian Influence Diagrams. Canadian Journal of Fisheries and Aquatic Sciences 56: 629-641.

Kurapati, S., Lukosch, H., Verbraeck, A. and Brazier, F.M., 2015. Improving Resilience in Intermodal Transport Operations in Seaports: A Gaming Approach. *EURO Journal on Decision Processes*, *3*(3-4), pp.375-396.

Landoll, D.J., 2005. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. CRC Press.

Laqeur, W., 1977 Terrorism, Weidenfeld and Nicholson, London (1977), William Laqeur,

Lecklin, T., Ryömä, R. and Kuikka, S., 2011. A Bayesian Network for analysing Biological Acute and Long-term Impacts of an Oil Spill in the Gulf of Finland. Marine Pollution Bulletin 62: 2822-2835.

Lemkowitz, S.M. and Pasman, H.J., 2014. A Review of the Fire And Explosion Hazards of Particulates. KONA Powder and Particle Journal, 31, pp.53-81.

Lewis, James A. (2002) Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats. *Centre for Strategic & International Studies (CSIS).*

Linton, M., 2011. The Terror in the French Revolution. Kingston University, Retrieved, p.72. http://www2.port.ac.uk/special/france1815to2003/chapter1/interviews/filetodownload,20545,en.pdf

Liu, C., Tan, C.K., Fang, Y.S. and Lok, T.S., 2012. The security risk assessment Methodology. Procedia Engineering, 43, pp.600-609.

Loh, H.S. and Thai, V.V., (2015), Management of Disruptions by Seaports: Preliminary Findings. *Asia Pacific Journal of Marketing and Logistics, 27*(1), pp.146-162.

Mahadevan, S. and Rebba, R. (2005), "Validation of Reliability Computational Models Using Bayes Networks", Reliability Engineering & System Safety, Vol. 87, pp. 223-232.

Mansell, J.N., (2009), Flag State Responsibility: Historical Development and Contemporary Issues. Springer Science & Business Media.

Mantyniemi, S., Haapasaari, P., Kuikka, S. Parmanne, R., Lehtiniemi, M. and Kaitaranta, J., 2013. Incorporating stakeholders knowledge to stock assessment: Central Baltic herring. Canadian Journal of Fisheries and Aquatic Scienses, 70: 591-599.

Marsh & McLennan Companies., (2014), “Ports and Terminals Risk Challenges and Solutions” Global Infrastructure and Marine Practices. Published 7/2014. https://www.oliverwyman.com/content/dam/marsh/Documents/PDF/US-en/Ports%20and%20Terminals%20Risk%20Challenges%20and%20Solutions-06-2014.pdf

Martin, G., 2017 “Types of Terrorism in Developing Next Generation Countermeasures for Homeland Security Threat Prevention”, IGI Global, Hershly, Penn., US (2017) [Gus Martin]

Marxist-Leninist Journal 1990, “Theoretical Journal of The Revolutionary Communist Party of Britain” Vol.3 No.2. Available from: https://www.marxists.org/history/erol/uk.hightide/mlj-3-2.pdf

Marxist-Leninist, (1990) “Marxist- Leninist Journal - Theoretical Journal of The Revolutionary Communist Party of Britain” Vol.3, No.2 – July, 1990. Publish by Workers’ Publishing House. Available from: https://www.marxists.org/history/erol/uk.hightide/mlj-3-2.pdf

McCabe, B., AbouRizk, M. S., Member ASCE and Randy, G. (1998), "Belief Networks for Construction Performance Diagnostics", Journal of Computing in Civil Engineering, Vol. 12, No. 2, pp. 93-100.

Merkin, B.G. 1979, *Group choice*. John Wiley & Sons, NY.

Ministry of Defence of Finland (2011) *Security Strategy for Society*. Government Resolution 16.12.2010. Ministry of Defence, Helsinki.

Massachusetts Institute of Technology., (2015) “D-separation: How to Determine which Variables are Independent in a Bayes Net” Available at http://web.mit.edu/jmn/www/6.034/d-separation.pdf

Molina, J. L., Bromley, J., García-Aróstegui, J.L., Sullivan, C., Benavente, J., 2010. Integrated Water Resources Management of Overexploited Hydrogeological Systems using Object-Oriented Bayesian Networks. Environmental Modelling and Software 25: 383–397.

Mullai, A., 2006. *Risk Management System-Risk Assessment Frameworks and Techniques* (Vol. 5, No. 2006). DaGoB (Safe and Reliable Transport Chains of Dangerous Goods in the Baltic Sea Region) Project Office, Turku School of Economics, Turku, Finland. http://rop.lv/ru/smi/zagruzki/doc_download/42-risk-management-system-risk-assessment-frameworks-and-techniques.html

National Cyber Security Centre., (2017), “The Launch of The National Cyber Security Centre”. Available from: https://www.cipfa.org/~/media/files/services/ccfc/hm%20government%20national%20cyber%20security%20strategy%202016%202021.pdf

Navcen (2018) Navigation Center (U.S. Department of Homeland Security) United States Cast Guard. Available from: https://www.navcen.uscg.gov/?pageName=AISRequirementsRev

NCJRS, (1976) "Disorders and Terrorism" *(PDF). National Advisory Committee on Criminal Justice Standards and Goals. 1976. pp. 3–6.*

Neapolitan, R. E. (1990), Probabilistic Reasoning in Expert System: Theory and Algorithms, John Willey Sons, Inc., NY, USA.

Ng, A.K.Y. (2007): 'Port Security and the Competitiveness of Short Sea Shipping in Europe: Implications and Challenges. In: Bichou, K., Bell, M. and Evans, A. (Eds.): Risk Management in Port Operations, Logistics and Supply Chain Security, LLP, London, ISBN: 978-1-8431-1655-4, Chapter 20, pp. 347-366

Ng, Say, Wee., (2003), "An Overview of Practical Risk Assessment Methodologies", Available at (June 29, 2003), (https://www.giac.org/paper/gsec/3287/overview-practical-risk-assessment-methodologies/105426)

Norman, T.L., 2010. Risk Analysis and Security Countermeasure Selection. CRC press.

North, D. W. (1968), "A Tutorial Introduction to Decision Theory", IEEE Transactions on System Science and Cybernetic Vol. 4, pp. 201-210.

OSHA, 2019. Fire Service Features of Building and Fire Protection Systems", Occupational Safety and Health Administration. Available from https://www.osha.gov/Publications/OSHA3256.pdf

Pearl, J. (1982), "Reverend Bayes on Inference Engines: A Distributed Hierarchical Approach", National Conference on Artificial Intelligence, pp. 133-136.

Pereira, J.C. and Lima, G.B.A., 2015. Probabilistic Risk Analysis in Manufacturing Situational Operation: Application of Modelling Techniques and Causal Structure to Improve Safety Performance. *International Journal of Production Management and Engineering*, *3*(1), pp.33-42.

Pinto, C.A. and Talley, W.K., (2006), The Security Incident Cycle of Ports. *Maritime Economics & Logistics*, *8*(3), pp.267-286.

Port and Habours (2017) (Unit 14) Faculty of Maritime Studies Rijeka. Avaiable from: http://www.pfri.uniri.hr/~bopri/documents/14-ME-tal_001.pdf

Rahikainen, M., Helle, I., Haapasaari, P., Oinonen, S., Kuikka, S., Vanhatalo, J., Mäntyniemi, S., Hoviniemi, K.-M., 2014. Towards Integrative Management Advice of Water Quality, Oil Spills, and Fishery in the Gulf of Finland: A Bayesian Approach. Ambio 43: 115-123.

Rahman, N.A., 2012. Selection of the Most Beneficial Shipping Business Strategy for Containerships. *European Journal of Business and Management*, *4*(17), pp.153-167.

Raiffa, H. (1968), Decision Analysis, Addison-Wesley, Reading, MA, USA.

Raman B. and Hyderabad C. 2010, "Why LTTE Attacked Galle Naval Base and Harbour? - International Terrorism Monitor--Paper No. 141", Available from (Jun 20, 2010) (https://web.archive.org/web/20100620201219/http://southasiaanalysis.org/papers20/paper1997.html)

Reed-Schrader, E., Hayoun, M.A. and Goldstein, S., 2019. "EMS, Weapons of Mass Destruction and Related Injury," Available from (https://europepmc.org/books/NBK441954;jsessionid=C6CFF4CD45E7B140AC218A92C8141570)

Riahi, R. (2010), Enabling Security and Risk-Based Operation of Container Line Supply Chains Under High Uncertainties. PhD Thesis, *Liverpool John Moores University*, UK.

Robinson, R., 2002. Ports As Elements in Value-Driven Chain Systems: The New Paradigm. Maritime Policy & Management 29 (3), 241–255.

Rushton, A., Oxley, J. and Croucher, P. (2000), The Handbook of Logistics and Distribution Management, Institute of Logistics and Transport, Kogan Page Limited, London, UK, pp. 6.

Russell, S.J. and Norvig, P., 2016. *Artificial Intelligence: A Modern Approach*. Malaysia; Pearson Education Limited.

Saaty, T.L. 1980, *The Analytic Hierarchy Process*, McGraw-Hill Book Co., NY.

Saaty, T.L. 1990, How to Make a Decision: The Analytic Hierarchy Process, *European Journal of Operational Research*, vol.48, pp.9-26.

Saaty, T.L. 1994, *Fundamental of Decision Making*, RWS Publications, Pittsburgh, PA.

Safety of Life at Sea (SOLAS), 2014, Available at (Refer on June, 2014) https://www.loc.gov/law/help/us-treaties/bevans/m-ust000002-0782.pdf

Schneier, B., 1999 "Academic: Attack Trees - Schneier on Security", Dr Dobb's Journal, December (https://www.schneier.com/academic/archives/1999/12/attack_trees.html)

Scott, W.R., 1973. A Bayesian Approach to Asset Valuation and Audit Size. *Journal of Accounting Research*, pp.304-330.

Shachter, R.D. (1998), Bayes-ball: The Rational Pastime (For Determining Irrelevance and Requisite Information in Belief Networks and Influence Diagrams). *Proceedings of The 14th Conference on Uncertainty in Artificial Intelligence.* pp.480-487.

Shafer, G. (1990), "Decision Making", Readings in Uncertain Reasoning, Shafer, G. and Pearl,J . (eds)., Morgan-Kaufmann,S an Mateo, CA, USA, pp. 61-67.

Sjaastad, A.C., 2007. Southeast Asian SLOCs and Security Options. In *Maritime Security in Southeast Asia* (pp. 17-27). Routledge.

Snyder, L.V. and Tomlin, B., 2008. Inventory Management with Advanced Warning of Disruptions. *Bethlehem, PA: PC Rossin College of Engineering and Applied Sciences, Lehigh University*.

Soares, C. Guedes, and A. P. Teixeira. 2001 "Risk Assessment in Maritime Transportation." *Reliability Engineering & System Safety* 74.3 (2001): 299-309.]

Song, D.W. and Panayides, P.M., (2008), Global Supply Chain and Port/Terminal: Integration and Competitiveness. *Maritime Policy & Management*, *35*(1), pp.73-87.

Spiegelhalter, D. J. and Knill-Jones, R. P. (1984), "Statistical and Knowledge-based Approaches to Clinical Decision-support Systems", Journal of the Royal Statistical Society: Series A, Vol. 147, pp. 35-37.

Stoneburner, G., Goguen, A.Y. and Feringa, A., 2002. Sp 800-30. Risk Management Guide for Information Technology Systems.

Storms, A., 2004. Using Vulnerability Assessment Tools to Develop an OCTAVE Risk Profile. *SANS Information Security Reading Room*.

Stanton, N.A., Chambers, P.R. and Piggott, J., 2001. Situational Awareness and Safety. *Safety Science*, *39*(3), pp.189-204.

Straitstimes 2016- Look into on Feb 2017 : http://www.straitstimes.com/singapore/drop-in-piracy-in-regional-waters

Strong, S., 1992. *Shining Path: The World's Deadliest Revolutionary Force* (Vol. 260). London: HarperCollins.

Sultan, M. H., 2001 “Indian Parliament Attack” Daily Pakistan Observer. Available from Dec 14, 2018. https://pakobserver.net/2001-indian-parliament-attack/

Swanson, M., 2001. *Security Self-Assessment Guide for Information Technology Systems* (No. NIST-SP-800-26). Booz-Allen And Hamilton Inc Mclean Va.

Szolovits, P. and Pauker, S. G. (1993), "Categorical and Probabilistic Reasoning in Medicine Revisited", Artificial Intelligence, Vol. 59, pp. 167-180.

Tang, C. S. (2006), "Perspectives in Supply Chain Risk Management", *International Journal of Production Economics*, Vol. 103, No. 2, pp. 451-488.

Thai, V.V. and Grewal, D., (2007), The Maritime Security Management System: Perceptions of The International Shipping Community. *Maritime Economics & Logistics*, *9*(2), pp.119-137.

The Star, 2018. “Displaced Rohingya Refugees May End Up Being Radicalised by Terrorist Groups - Chief Defence Minister of Malaysia” Nation Section, The Star Online. Available from (27 August 2018): https://www.thestar.com.my/news/nation/2018/08/27/mat-sabu-displaced-rohingya-refugees-may-end-up-being-radicalised-by-terrorist-groups/

Thomas III, S.W., Amara, J.P., Bjork, R.E. and Swager, T.M., 2005. Amplifying Fluorescent Polymer Sensors for The Explosives Taggant 2, 3-dimethyl-2, 3-dinitrobutane (DMNB). *Chemical Communications*, (36), pp.4572-4574.

Varis, O., Kuikka, S., 1997. Joint Use of Multiple Environmental Assessment Models by a Bayesian Metamodel: The Baltic Salmon Case. Ecological Modelling 102(2-3): 341-351.

Vilde Skorpen Wikan, N., 2018 Is “One Man’s Terrorist Another Man’s Freedom Fighter”? Available at http://dspace.uni.lodz.pl/xmlui/bitstream/handle/11089/26142/593-616-machnikowski.pdf?sequence=1&isAllowed=y

Wald, A. (1950), Statistical Decision Functions, Wiley, NY, USA.

Wang, J. and Trbojevic, V. (2007), Design For Safety of Large Marine and Offshore Engineering Products. *Institute of Marine Engineering, Science and Technology*. ISBN: 1902536584.

Wang, J., Yang, J.B. and Sen, P. (1995), Safety Analysis and Synthesis Using Fuzzy Sets and Evidential Reasoning, *Reliability Engineering & System Safety*, vol.47 (2), pp.103-118.

Wang, J., Yang, J.B. and Sen, P. (1996), Multi-person and Multi-Attribute Design Evaluations Using Evidential Reasoning Approach Based on Subjective Safety and Cost Analysis, *Reliability Engineering and System Safety*, vol.52, pp.113-127.

Wang, John *et al.* (2000). What Every Engineer Should Know About Risk Engineering and Management, p. 69, at Google Books

White, D.M., 2010. The Federal Information Security Management Act of 2002: a Potemkin Village. *Fordham L. Rev.*, *79*, p.369.

Yang, J.B. and Sen, P. (1997), Multiple Attribute Design Evaluation of Large Engineering Products Using the Evidential Reasoning Approach, *Journal of Engineering Design*, vol.8 (3), pp.211-230.

Yang, J.B. and Xu, D.L. (2002), On The Evidential Reasoning Algorithm for Multiple Attribute Decision Analysis Under Uncertainty, *IEEE Transaction on System, Man and Cybernetics*, vol.32 (3), pp.289-304.

Yang, Z. (2006), "Risk Assessment and Decision Making of Container Supply Chains", *Phd Thesis*, Liverpool Logistics Offshore and Marine Research Institute (LOOM), Liverpool John Moores University.

Yang, Z., Ng, A.K. and Wang, J., 2014. A New Risk Quantification Approach in Port Facility Security Assessment. *Transportation Research part A: Policy and Practice, 59*, pp.72-90.

Yunos, Z., Ahmad R., and Abd. Aziz, N. A., 2013, "Definition and Framework of Cyber Terrorism" pg 67-77. Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT). Available from: http://www.searcct.gov.my/images/PDF_My/publication/SEARCCT_Selection_of_Articles_Vol._1-2013.pdf

Appendices

Appendix 1

Data Collection and Analysis of Each Node

GTD ID	DATE	COUNTRY	CITY	PERPETRATOR GROUP	FATALITIES	INJURED	TARGET TYPE
201511040046	2015-11-04	Mali	Tenenkou	Muslim Fundamentalists	0	1	Maritime
201506270009	2015-06-27	Yemen	Buraiqeh	Huthi Extremists	1	0	Business,Maritime
201505140032	2015-05-13	Somalia	Ceel Dheere district	Al-Shabaab	Unknown	Unknown	Maritime
201505060078	2015-05-06	Yemen	Aden	Huthi Extremists	86	67	Maritime
201504060041	2015-04-06	Pakistan	Pasni	Baloch Liberation Front (BLF)	0	7	Maritime
201503040003	2015-03-04	Libya	Benghazi	Ansar al-Sharia (Libya)	3	4	Military,Maritime
201502030092	2015-02-03	France	Nice	Unaffiliated Individual(s)	0	2	Military,Private Citizens & Property
201501300088	2015-01-30	Bangladesh	Gournadi	Pro Hartal Activists	0	2	Maritime
201501300071	2015-01-30	Egypt	Alexandria	Unknown	0	2	Maritime
201411100021	2014-11-10	Somalia	Kismayo	Unknown	0	0	Maritime
201410140050	2014-10-14	Malaysia	Kudat district	Abu Sayyaf Group (ASG) (suspected)	0	2	Maritime,Maritime
201410080023	2014-10-08	Libya	Benghazi	Unknown	1	1	Maritime,Maritime
201408110009	2014-08-11	Libya	Derna	Haftar Militia	0	3	Maritime
201407100007	2014-07-10	Somalia	Raage Ceele	Al-Shabaab	0	0	Maritime
201407060006	2014-07-05	Somalia	Mogadishu	Al-Shabaab (suspected)	0	0	Maritime
201406250055	2014-06-25	Pakistan	Karachi	Unknown	0	1	Maritime
201404100101	2014-04-10	Somalia	Mogadishu	Unknown	0	0	Maritime
201403120075	2014-03-12	Nigeria	Nembe district	Unknown	Unknown	Unknown	Maritime
201403120074	2014-03-12	Nigeria	Nembe district	Unknown	Unknown	Unknown	Maritime
201403110095	2014-03-08	Libya	As Sidr	Cyrenaica Self-Defense Force	0	0	Maritime
201402240115	2014-05-24	Thailand	Bana	Separatists (suspected)	0	5	Maritime
201401230018	2014-01-23	Kenya	Unknown	Merille Militia	1	Unknown	Maritime
201312100002	2013-12-10	Libya	Derna	Unknown	1	0	Maritime
201310230025	2013-10-23	Nigeria	Unknown	Movement for the Emancipation of the Niger Delta (MEND)	0	0	Maritime
201310070026	2013-10-07	Egypt	Port Said	Unknown	1	1	Police,Maritime
201309200009	2013-09-20	Yemen	Ain Ba Maabad	Al-Qaida in the Arabian Peninsula (AQAP)	1	0	Maritime
201308310027	2013-08-31	Egypt	Unknown	Al-Furqan Brigades	0	0	Maritime
201308170014	2013-08-17	Iraq	Basra	Unknown	0	4	Maritime
201305210020	2013-05-21	Philippines	Unknown	Abu Sayyaf Group (ASG)	0	0	Maritime
201305210010	2013-05-21	Pakistan	Karachi	Unknown	0	0	Maritime
201304110041	2013-04-10	Thailand	Arnohru	Unknown	0	0	Maritime
201304100066	2013-04-10	Thailand	Taluban	Unknown	0	0	Maritime
201302250018	2013-02-25	Philippines	Tabuk	Unknown	0	0	Maritime
201302050010	2013-02-05	Nigeria	Sagbama	Unknown	3	5	Military,Maritime
201208280004	2012-08-28	Bangladesh	Sadarghat	Unknown	0	2	Maritime
201201140016	2012-01-14	Laos	Unknown	Unknown	0	0	Maritime
201107200006	2011-07-20	Yemen	Aden	Al-Qaida in the Arabian Peninsula (AQAP) (suspected)	1	1	Business
201105220006	2011-05-22	Colombia	Medio Atrato	Revolutionary Armed Forces of Colombia (FARC) (suspected)	3	2	Maritime
201105170012	2011-05-17	Yemen	Aden	Unknown	0	0	Maritime
201009110003	2010-09-11	Somalia	Mogadishu	Unknown	0	2	Maritime
201007280009	2010-07-28	United Arab Emirates	Fujairah	Abdullah Azzam Brigades	Unknown	1	Maritime
201005200029	2010-05-20	Somalia	Mogadishu	Al-Shabaab (suspected)	2	4	Maritime
201003280020	2010-03-28	Cameroon	Bakassi district	Africa Marine Commando (suspected)	0	0	Maritime

GTD ID	DATE	COUNTRY	CITY	PERPETRATOR GROUP	FATALITIES	INJURED	TARGET TYPE
201003120016	2010-03-12	Cameroon	Bakassi district	Africa Marine Commando	0	2	Maritime,Maritime
201001270003	2010-01-27	Pakistan	Quetta	Unknown	0	0	Maritime
200912150011	2009-12-15	Afghanistan	Surobi district	Hizb-I-Islami	0	0	Maritime
200912150001	2009-12-15	Afghanistan	Surobi	Unknown	0	0	Maritime
200910090005	2009-10-09	Afghanistan	Khwaja	Taliban (suspected)	0	0	Maritime
200909090010	2009-09-09	Somalia	Mogadishu	Unknown	2	3	Maritime
200909080001	2009-09-08	Pakistan	Quetta	Unknown	0	0	Maritime
200907270012	2009-07-27	Colombia	Medio San Juan	Revolutionary Armed Forces of Colombia (FARC) (suspected)	6	0	Maritime
200907210024	2009-07-21	Pakistan	Hangu	Tehrik-i-Taliban Pakistan (TTP)	0	0	Maritime
200907170004	2009-07-17	Pakistan	Landi Kotal	Tehrik-i-Taliban Pakistan (TTP) (suspected)	0	1	Maritime
200907120018	2009-07-12	Nigeria	Lagos	Movement for the Emancipation of the Niger Delta (MEND) (suspected)	5	0	Maritime
200907050012	2009-07-05	Nigeria	Escravos district	Movement for the Emancipation of the Niger Delta (MEND)	0	0	Maritime
200905240011	2009-05-24	Philippines	Nasipit	Unknown	0	0	Business,Maritime
200905130013	2009-05-13	Nigeria	Chanomi Creek	Movement for the Emancipation of the Niger Delta (MEND) (suspected)	0	6	Maritime
200903090022	2009-03-09	Sri Lanka	Mullaitivu	Liberation Tigers of Tamil Eelam (LTTE) (suspected)	0	0	Maritime
200902120031	2009-02-12	Somalia	Mogadishu	Unknown	2	6	Maritime
200901210006	2009-01-21	Nigeria	Bonny	Movement for the Emancipation of the Niger Delta (MEND)	0	0	Military,Maritime
200901130007	2009-01-13	Pakistan	Matta	Tehrik-i-Taliban Pakistan (TTP) (suspected)	1	1	Maritime
200812190007	2008-12-19	Pakistan	Landi Kotal	Tehrik-i-Taliban Pakistan (TTP) (suspected)	3	0	Maritime
200812160018	2008-12-16	Pakistan	Landi Kotal	Unknown	0	0	Maritime
200811130010	2008-11-00	India	Porbandar	Lashkar-e-Taiba (LeT),Deccan Mujahideen	1	0	Maritime
200810220004	2008-10-22	Sri Lanka	Kankasanthurai	Liberation Tigers of Tamil Eelam (LTTE) (suspected)	0	0	Maritime
200808240002	2008-08-24	Nigeria	Bonny	Unknown	0	0	Maritime
200808120001	2008-08-12	Somalia	Unknown	Pirates	0	0	Maritime
200807260023	2008-07-26	Nigeria	Unknown	Unknown	0	0	Maritime-Other
200806190014	2008-06-19	Nigeria	Unknown	Movement for the Emancipation of the Niger Delta (MEND)	0	0	Maritime
200806190009	2008-06-19	Nigeria	Unknown	Movement for the Emancipation of the Niger Delta (MEND)	0	0	Maritime
200806100007	2008-06-10	Nigeria	Unknown	Unknown	9	4	Maritime
200806090016	2008-06-09	Nigeria	Unknown	Unknown	1	4	Maritime
200806080010	2008-06-08	Pakistan	Torkham	Unknown	0	0	Maritime
200806020011	2008-06-02	Indonesia	Jakarta	Unknown	0	0	Maritime
200805130009	2008-05-13	Pakistan	Mohmand district	Tehrik-i-Taliban Pakistan (TTP) (suspected)	0	0	Maritime
200805130007	2008-05-13	Nigeria	Unknown	Unknown	0	0	Maritime
200802150098	2008-02-15	Somalia	Mogadishu	Unknown	0	2	Maritime
200801160013	2008-01-16	Nigeria	Port Harcourt	Unknown	0	Unknown	Maritime
200712040003	2007-12-04	Nigeria	Unknown	Unknown	1	1	Maritime
200705250006	2007-05-25	Somalia	Mogadishu	Unknown	Unknown	Unknown	Maritime
200705250001	2007-05-25	Nigeria	Sengana	Movement for the Emancipation of the Niger Delta (MEND)	0	0	Maritime
200704210008	2007-04-21	France	Bastia	Corsican National Liberation Front (FLNC) (suspected)	0	0	Government (General)
200701210005	2007-01-21	Sri Lanka	Point Pedro	Liberation Tigers of Tamil Eelam (LTTE) (suspected)	2	1	Maritime

GTD ID	DATE	COUNTRY	CITY	PERPETRATOR GROUP	FATALITIES	INJURED	TARGET TYPE
200701130007	2007-01-13	Nigeria	Ekulama	Unknown	12	0	Maritime,Private Citizens & Property
200612230003	2006-12-23	Sri Lanka	Mullaitivu	Liberation Tigers of Tamil Eelam (LTTE)	0	1	Maritime
200612030020	2006-12-03	Nigeria	Okono	Niger Delta Vigilante (NDV)	1	Unknown	Maritime
200610180005	2006-10-18	Sri Lanka	Tangalle	Liberation Tigers of Tamil Eelam (LTTE)	16	14	Military,Maritime,Private Citizens & Property
200604040016	2006-04-04	Somalia	Unknown	Other (suspected)	0	0	Business,Maritime
200508290003	2005-08-28	Philippines	Lamitan	Abu Sayyaf Group (ASG)	0	30	Maritime,Private Citizens & Property
200508100011	2005-08-10	Trinidad and Tobago	Port-of-Spain	Unknown	0	0	Maritime
200507240006	2005-07-24	Pakistan	Unknown	Unknown	1	3	Maritime
200506070001	2005-06-07	Afghanistan	Spin Boldak	Taliban	2	0	Military,Maritime
200504280007	2005-04-28	Togo	Lome	Unknown	0	0	Educational Institution
200407310007	2004-07-31	Pakistan	Gwadar	Unknown	0	0	Maritime
200404240001	2004-04-24	Iraq	Basra	Tawhid and Jihad	6	4	Military,Maritime
200403140001	2004-03-14	Israel	Ashdod	Hamas (Islamic Resistance Movement),Al-Aqsa Martyrs Brigade	12	20	Maritime
200402270002	2004-02-27	Philippines	Manila	Abu Sayyaf Group (ASG)	116	Unknown	Maritime
200401090004	2004-01-09	Nigeria	Warri	Unknown	18	0	Maritime
200304020001	2003-04-02	Philippines	Davao City	Jemaah Islamiya (JI) (suspected),Moro Islamic Liberation Front (MILF) (suspected)	16	55	Maritime
200303200001	2003-03-20	Sri Lanka	Chundikulam	Liberation Tigers of Tamil Eelam (LTTE) (suspected)	14	1	Maritime
200210060001	2002-10-06	International	Gulf of Aden	Adan Abyan Islamic Army (AAIA),Al-Qaida	1	12	Maritime
200207090001	2002-07-09	Greece	Piraeus	New Revolutionary Popular Struggle (NELA) (suspected)	0	0	Maritime
200204220002	2002-04-22	Philippines	General Santos	Unknown	0	0	Maritime
200112120005	2001-12-12	Colombia	Magangue district	People's Revolutionary Army (ERP)	0	0	Maritime
200111130001	2001-11-13	Indonesia	Ambon	Unknown	3	5	Maritime
200110300001	2001-10-30	Sri Lanka	Point Pedro	Liberation Tigers of Tamil Eelam (LTTE)	10	Unknown	Maritime
200109040002	2001-09-04	Burundi	Nyanza-Lac	Unknown	4	0	Maritime
200108150018	2001-08-15	Sudan	Wangkei	Sudan People's Liberation Army (SPLA)	0	0	Maritime
200108140005	2001-08-14	Colombia	Bocas de Sogamoso	National Liberation Army of Colombia (ELN)	0	0	Business,Maritime,Private Citizens & Property
200108050006	2001-08-05	Burundi	Kazimia	Mayi Mayi,National Council for Defense of Democracy (NCDD)	0	0	Maritime

Page 1
https://www.start.umd.edu/gtd/search/Results.aspx?page=2&search=maritime&count=100&expanded=no&charttype=line&chart=overtime&ob=GTDID&od=desc#results-table
Page 2

https://www.start.umd.edu/gtd/search/Results.aspx?page=2&search=maritime&count=100&expanded=no&charttype=line&chart=overtime&ob=GTDID&od=desc#results-table

110 cases in maritime of terrorist attack

Appendix 2

Questionnaire

Questions Part 1

A set of questionnaire for obtaining the probability values relating to terrorist attacks to ports.

Instructions: Fill out your brief Personal Information

Brief of Personal Information

Age: (__) 20 to 30 years old

(__) 31 to 40 years old

(__) 41 to 50 years old,

(__) 51 to 60 years old,

(__) 61 and above.

Job Area: (__) Port Authority,

(__) Port Employee,

(__) Ministry of Transportation,

(__) Education,

(__) Others.

Job Experience: (____) years.

Questions Part 2

Instructions: Based on your opinions and past experience, please give a percentage between successful attacks in each of the item.

Likelihood of having a successful attack.

Highly likely	If you think that the likelihood of the attack is highly likely to be successful, then its value should be in the range 80% to 100%.

Likely	If you think that the likelihood of the attack is likely to be successful, then its value should be in the range 60% to 80%.
Average	If you think that the likelihood of the attack is successful on average, then its value should be in the range 40% to 60%.
Unlikely	If you think that the likelihood of the attack is unlikely to be successful, then its value should be in the range 20% to 40%.
Highly Unlikely	If you think that the likelihood of the attack is highly unlikely to be successful, then its value should be in the range 0% to 20%.

If you can provide percentage, it is the best. However if you have any difficulty to do that, you may use the linguistics grades whether high or low to define the answers to the questions.

Linguistics Grades	
YES	The likelihood of an attack **succeeded**
NO	The likelihood of an attack **failed**

Example. Using Tampered Truck(s)

In your opinion, what is the chance for the suicide attacker(s) planning to **use tampered truck(s)** (strap with bomb) as means of attacks? (85%)
Explanation - If you think that the likelihood is highly likely, then a value in the range from 80% to 100% can be chosen (i.e. 85%) in the table.

1. Using Tampered Truck(s)

In your opinion, what is the chance for the suicide attacker(s) planning to **use tampered truck(s)** (strap with bomb) as means of attacks? (____)

2. Terrorist(s) Overcome Prevention Unauthorized Entry

In your opinion, what is the chance for the terrorist(s) **to overcome** the port security barriers? (____)

3. Using Tempered Container

In your opinion, what is the chance for the terrorist planning to **use tampered container** (installed with bomb) as means of attacks? (____)

4. Overcome Identification for Visitor

In your opinion, what is the chance for the terrorist(s) pose as external person(s) (such as truck driver or shipping agent) **to overcome** the port security background-check? (____)

5. Overcome Identification for Employee

In your opinion, what is the chance for the terrorist pose as internal worker(s) **to overcome** the port security background-check? (____)

6. Hijacking the Vessel

In your opinion, what is the chance for the suicide attacker(s) succeeded to **hijack the vessel**, if the terrorist(s) **have overcome** the port security barriers? (____)

In your opinion, what is the chance for the suicide attacker(s) succeeded to **hijack the vessel**, if the terrorist(s) **have not overcome** the port security barriers? (____)

7. Overcome Routine Security Inspection

In your opinion, what is the chance for the container to **remain undetected** by the security routine inspection, if the terrorist(s) **successfully install** the bomb inside the container? (____)

In your opinion, what is the chance for the container to **remain undetected** by the security routine inspection, if the terrorist(s) **unsuccessfully install** the bomb inside the container **(Poor Installation/ not fully conceal)?** (____)

8. Overcome Prevention of Unauthorized Document Access

In your opinion, what is the chance for the internal worker terrorist(s) **install false container information in port's database,** if he/she/they able to enter the port **without raising any suspicion?** (____)

In your opinion, what is the chance for the internal worker terrorist(s) **install false container information in port's database,** if he/she/they **raise suspicion** when enter the port**?** (____)

9. Smuggling Unauthorized Containers (bomb)

In your opinion, what is the chance for the **terrorist**(s) **able to smuggle** a tempered container, if the container **remain undetected** and the internal worker terrorist(s) **able to change the container information**? (____)

In your opinion, what is the chance for the **terrorist**(s) **able to smuggle** a tempered container, if the container **remain undetected** and the internal worker terrorist(s) **unable to change the container information**? (____)

In your opinion, what is the chance for the **terrorist**(s) **able to smuggle** a tempered container, if the container **detected** and the internal worker terrorist(s) **able to change the container information**? (____)

In your opinion, what is the chance for the **terrorist**(s) **able to smuggle** a tempered container, if the container **detected** and the internal worker terrorist(s) un**able to change the container information**? (____)

10. Overcome Prevention of Unauthorized Item Introduced in the Port Facilities

In your opinion, what is the chance for the **terrorist**(s) **succeeded in** smuggling weapons into the port, if both internal worker(s) and external person(s) who work for terrorist able to enter the port **without raising any suspicion?** (____)

In your opinion, what is the chance for the **terrorist**(s) **succeeded in** smuggling weapons into the port, if internal worker(s) who work for terrorist able to enter the port **without raising any suspicion** but external person(s) were not**?** (____)

In your opinion, what is the chance for the **terrorist**(s) **succeeded in** smuggling weapons into the port, if external person(s) who work for terrorist able to enter the port **without raising any suspicion** but internal worker(s) were not**?** (25____)

In your opinion, what is the chance for the **terrorist**(s) **succeeded in** smuggling weapons into the port, if both internal worker(s) and external person(s) who work for terrorist **raise suspicion** when enter the port**?** (_5___)

11. Armed Attackers Overcome Prevention Unauthorized Entry

In your opinion, what is the chance for the armed attackers/terrorists **to overcome** the port security barriers, if they **have help from internal worker?** (_95__)

In your opinion, what is the chance for the armed attackers' terrorist **to overcome** the port security barriers, if **internal worker cannot help them?** (_20__)

12. Suicide Collision by Truck

In your opinion, what is the chance for the suicide attacker(s) **successfully** attack the port gate, if the terrorist(s) **use** the tampered truck(s) as means of weapons? (____)

13. Suicide Collision by Vessel(s)

In your opinion, what is the chance for the terrorist(s) **succeeded** to attack the port wharf using the vessel, if the terrorist(s) use the **tampered vessel** as means of weapons? (____)

14. Container Bomb

In your opinion, what is the chance for **successful** attack using the container bomb, if the **terrorist**(s) **able to smuggle** the tempered container into the port? (____)

15. Weaponry Attacks

In your opinion, what is the chance for **successful** attack using the conceal weapon, if the **terrorist**(s) **succeeded in** smuggling weapons into the port and the armed attackers' terrorist able **to overcome** the port security barriers. (____)

In your opinion, what is the chance for **successful** attack using the conceal weapon if the **terrorist**(s) **succeeded in** smuggling weapons into the port and the armed attackers' terrorist **unable to overcome** the port security barriers. (____)

In your opinion, what is the chance for **successful** attack using the conceal weapon, if the **terrorist**(s) **failed in** smuggling weapons into the port and the armed attackers' terrorist **able to overcome** the port security barriers. (____)

Questions Part 3

Instructions: Based on your opinions and past experience, please give a percentage of risky in each of the item.

Likelihood of having a successful attack.

Catastrophic	If you think that the severity of the attack is catastrophic, then it should be a value in the range 80% to 100%.
Major	If you think that the severity of the attack is major, then it should be a value in the range 60% to 80%.
Moderate	If you think that the severity of the attack is moderate, then it should be a value in the range 40% to 60%.
Minor	If you think that the severity of the attack is minor, then it should be a value in the range 20% to 40%.
Insignificant	If you think that the severity of the attack is insignificant, then it should be a value in the range 0% to 20%.

If you can provide percentage, it is the best. However if you have any difficulty to do that, you may use the linguistics grades whether risky or safe to define the answers to the questions.

Linguistics Grades	
RISKY	The severity of an attack is **high**
SAFE	The severity of an attack is **low**

16. Port Gate

In your opinion, what is the chance of Port Gate completely damaged, if the suicide attack **succeeded**? (____)

17. Wharf Operation Site

In your opinion, what is the chance of Wharf Operation Site completely damaged, if suicide attack, container bomb attack and weaponry attack **succeeded?** (____)

In your opinion, what is the chance of Wharf Operation Site completely damaged, if suicide attack and container bomb attack **succeeded but** weaponry attack **failed?** (____)

In your opinion, what is the chance of Wharf Operation Site completely damaged, if suicide attack and weaponry attack **succeeded** but container bomb attack **failed?** (____)

In your opinion, what is the chance of Wharf Operation Site completely damaged, if suicide attack **succeeded** but container bomb attack and weaponry attack **failed?** (____)

In your opinion, what is the chance of Wharf Operation Site completely damaged, if container bomb attack and weaponry attack **succeeded** but suicide attack **failed?** (____)

In your opinion, what is the chance of Wharf Operation Site completely damaged, if container bomb attack **succeeded** but suicide attack and weaponry attack **failed?** (____)

In your opinion, what is the chance of Wharf Operation Site completely damaged, if weaponry attack **succeeded** but suicide attack and container bomb attack **failed?** (____)

18. Yard Operation Site

In your opinion, what is the chance of Yard Operation Site **completely damaged**, if container bomb attack and weaponry attack **succeeded?** (____)

In your opinion, what is the chance of Yard Operation Site **completely damaged**, if container bomb attack **succeeded** and weaponry attack **failed?** (____)

In your opinion, what is the chance of Yard Operation Site **completely damaged**, if weaponry attack **succeeded** and container bomb attack **failed?** (____)

19. Administration Site

In your opinion, what is the chance of Administration Site **completely damaged**, if weaponry attack **succeeded?** (____)

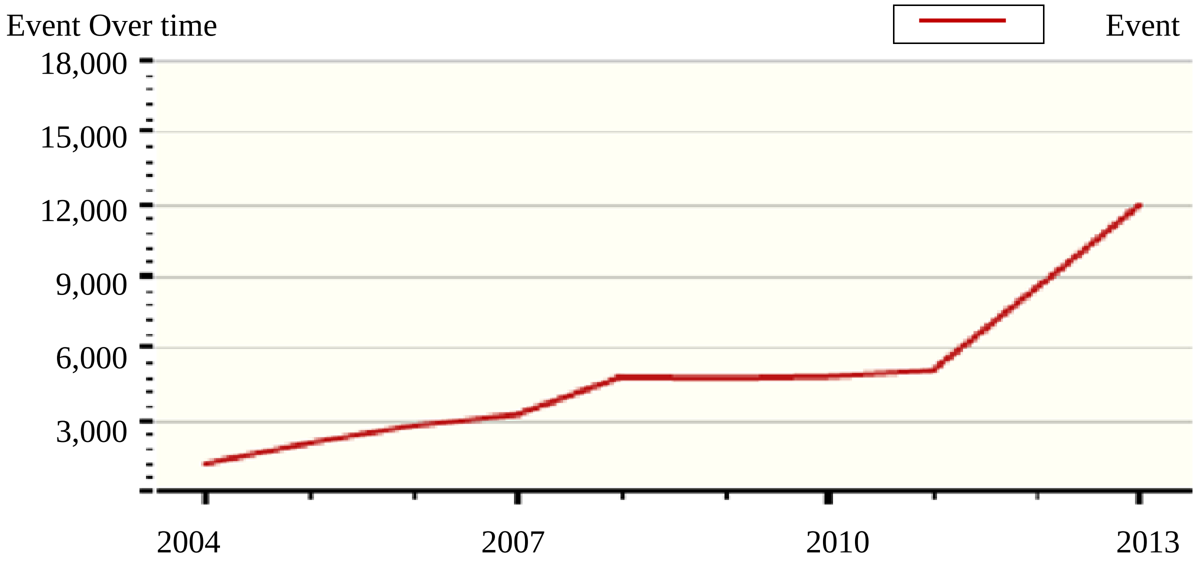
Thank you very much for spending your precious time in filling this questionnaire. If you wish to receive a summary of our survey findings, please provide us at W.M.AbdulHalim@2013.ljmu.ac.uk with your name and email address with the answered questionnaire and then we will send you the questionnaire result when it is ready for publication.

Example

Name: Angela R (Operations Manager)
Email: Angie.R@liverpool.gov.uk

Appendix 3

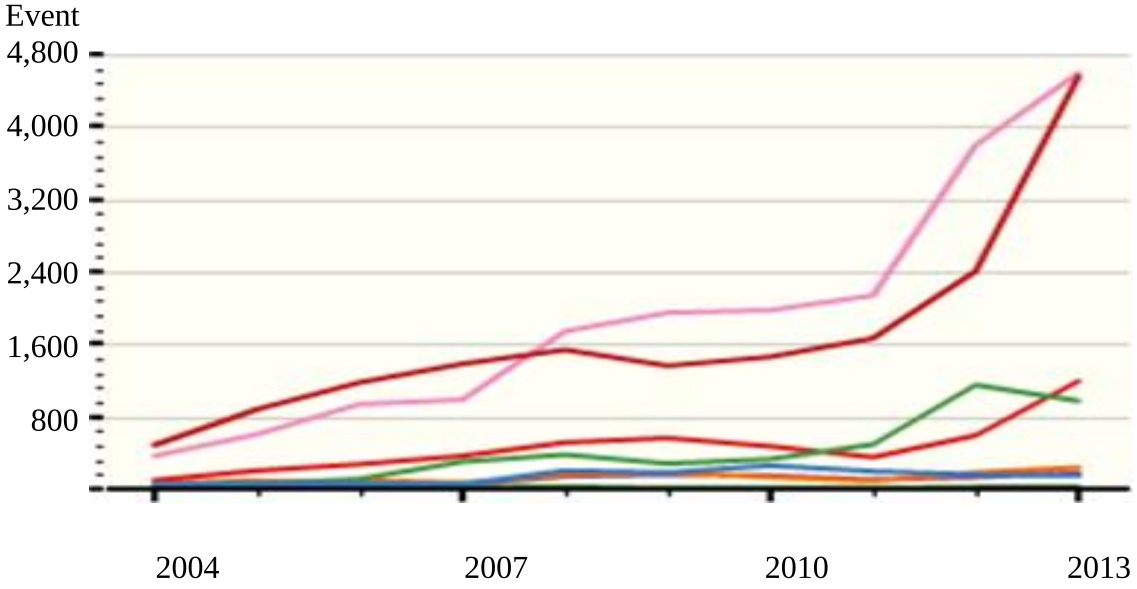
Line Chart Result: 48990 Events



Terrorist event since 2004-2013 (Source from Global terrorism database 2014)

Appendix 4

Line Chart Result on the Regions: 48990 Events

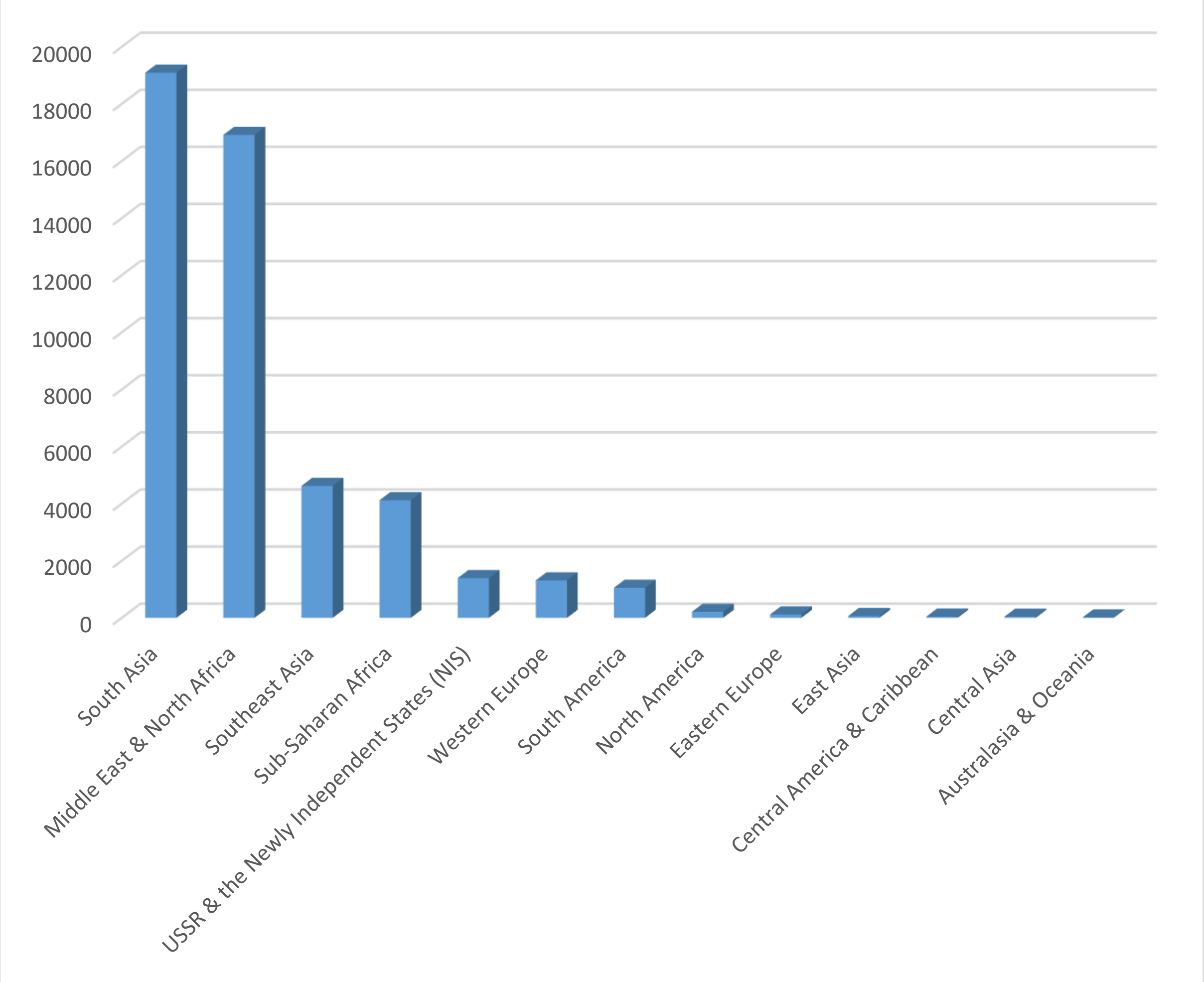


Line Chart: Categories of regions attacked by terrorist since 2004 until 2013

Regions		Event
—	South Asia	19091
—	Middle East & North Africa	16913
—	Southeast Asia	4620
—	Sub-Saharan Africa	4118
—	Western Europe	1392
—	South America	1312
—	USSR & the Newly Independent States (NIS)	1053
—	North America	211
—	Eastern Europe	119
—	East Asia	64
—	Central America & Caribbean	43
—	Central Asia	40
—	Australasia & Oceania	14

Appendix 5

The Bar Chart Result: 48990 Events



The Bar Chart: Categories of regions attacked by terrorist since 2004 until 2013

Appendix 6

Questionnaire

Researcher started with interviewing the expert from industry about the factors inside the countermeasures if any attack from terorrist would happen to the wharf.

Questions Part 1

A set of questionnaire for obtaining the probability values relating to terrorist attacks to ports.

Instructions: Fill out your brief Personal Information

Brief of Personal Information

Age: (__) 20 to 30 years old

(__) 31 to 40 years old

(__) 41 to 50 years old,

(__) 51 to 60 years old,

(__) 61 and above.

Job Area: (__) Port Authority,

(__) Port Employee,

(__) Ministry of Transportation,

(__) Education,

(__) Others.

Job Experience: (____) years.

Questions Part 2

The Scales for Countermeasure Effectiveness of Port Forces

List of Questions – English Version

Instructions: Based on your opinions and past experience, please give an answer in percentage between 0% to 100% at the scale line provided for each question (tick on the line)

List of Port forces	
1	Port Police
2	Port Fire Fighter

Example 1 – Countermeasure Effectiveness to counter terrorist attack on Wharf

In your opinion, how high the level of training does Port Forces received in order to counter terrorist attacks? (85%)

Low Level (0%)

High Level (100%)

CE-1 Tested

1.0.Training

1.1.In your opinion, how high the level of training does Port Forces received in order to counter terrorist attacks?

2.0.Experience

2.1.In your opinion, how high level of does Port Forces received in order to counter terrorist attacks?

3.0.Skills

3.1.In your opinion, how high level of skills does Port Forces received in order to counter terrorist attacks if they have high level of training and experience? (%)

3.2.In your opinion, how high level of skills does Port Forces have to counter terrorist attacks if they have high level of training and low level of experience? (%)

3.3.In your opinion, how high level of skills does Port Forces have to counter terrorist attacks if they have low level of training and high level of experience? (%)

3.4.In your opinion, how high level of skills does Port Forces have to counter terrorist attacks if they have low level of training and experience? (%)

4.0. Visual or Hearing Awareness

4.1.In your opinion, is it easy for Port Forces to see or hear from their places if any attack(s) happen on Wharf on Sites? (%)

5.0. Emergency Call

5.1.In your opinion, does Port Forces have easy Access for Emergency Call from the workers at the wharf if any attack(s) happen on Wharf on Sites? (%)

6.0. Situation Awareness

6.1.In your opinion, how high level of Situation Awareness does Port Forces have if it is easy for them to see or hear any attacks from their places and easy Access for Emergency Call? (%)

6.2.In your opinion, how high level of Situation Awareness does Port Forces have if it is easy for them to see or hear any attacks from their places and bad Access for Emergency Call? (%)

6.3.In your opinion, how high level of Situation Awareness does Port Forces have if it is difficult for them to see or hear any attacks from their places and easy Access for Emergency Call? (%)

6.4.In your opinion, how high level of Situation Awareness does Port Forces have if it is difficult for them to see or hear any attacks from their places and bad Access for Emergency Call? (%)

7.0. Armoury Defense Supply

7.1.In your opinion, does Port Forces have high numbers of weapon for security and defense purposes? (%)

8.0. Countermeasure Effectiveness – 1

8.1.In your opinion, how high does Port Forces Countermeasure Effectiveness 1 if they have high level of Skills and Situation Awareness, and High Supply of Armoury for Defence? (%)

8.2.In your opinion, how high does Port Forces Countermeasure Effectiveness 1 if they have high level of Skills and Situation Awareness, but low Supply of Armoury for Defence? (%)

8.3.In your opinion, how high does Port Forces Countermeasure Effectiveness 1 if they have high level of Skills but low level of Situation Awareness, and low Supply of Armoury for Defence? (%)

8.4.In your opinion, how high does Port Forces Countermeasure Effectiveness 1 if they have high level of Situation Awareness and high Supply of Armoury for Defence but low level of Skills? (%)

8.5.In your opinion, how high does Port Forces Countermeasure Effectiveness 1 if they have high level of Situation Awareness but low level of Skills, and low Supply of Armoury for Defence? (%)

8.6.In your opinion, how high does Port Forces Countermeasure Effectiveness 1 if they have high level of Skills and high Supply of Armoury for Defence but low level of Situation Awareness? (%)

8.7.In your opinion, how high does Port Forces Countermeasure Effectiveness 1 if they have low level of Skills and Situation Awareness, but high Supply of Armoury for Defence? (%)

8.8.In your opinion, how high does Port Forces Countermeasure Effectiveness 1 if they have low level of Skills and Situation Awareness, and low Supply of Armoury for Defence? (%)

CE-2 Tested

B.Explosion
9.1. In your opinion, what is the probability that the explosion occurred when the terrorist attack Port Wharf?

B. Countermeasure Effectiveness of Port Forces acting on Explosion occurs in wharf.

RE2 –if explosion happen in wharf.

10.0.Training

10.1. In your opinion, how high level of training does Port Forces received to counter terrorist attacks?

11.0. Experience

11.1. In your opinion, how high level of experience does Port Forces have to counter terrorist attacks?

12.0. Skills

12.1. In your opinion, how high level of skills does Port Forces have to counter terrorist attacks if they have high level of training and experience?

12.2.In your opinion, how high level of skills does Port Forces have to counter terrorist attacks if they have high level of training and low level of experience?

12.3.In your opinion, how high level of skills does Port Forces have to counter terrorist attacks if they have low level of training and high level of experience?

12.4.In your opinion, how high level of skills does Port Forces have to counter terrorist attacks if they have low level of training and experience?

13.0. Visual/ Hearing Awareness

13.1 In your opinion, is it easy for Port Forces to see or hear from their places if any attack(s) happen on Wharf on Sites?

14.0. Emergency Call

14.1.In your opinion, does Port Forces have easy Access for Emergency Call from the workers at the wharf if any attack(s) happen on Wharf on Sites?

15.0. Situation Awareness

15.1. In your opinion, how high level of Situation Awareness does Port Forces have if it is easy for them to see or hear any attacks from their places and easy Access for Emergency Call?

15.2.In your opinion, how high level of Situation Awareness does Port Forces have if it is easy for them to see or hear any attacks from their places and bad Access for Emergency Call?

15.3.In your opinion, how high level of Situation Awareness does Port Forces have if it is difficult for them to see or hear any attacks from their places and easy Access for Emergency Call?

15.4In your opinion, how high level of Situation Awareness does Port Forces have if it is difficult for them to see or hear any attacks from their places and bad Access for Emergency Call?

16.0. Armoury Defence Supply

16.1. In your opinion, does Port Forces have high numbers of weapon for security and defense purposes?

17.0. Countermeasure Effectiveness- 2

17.1. In your opinion, how high does Port Forces Countermeasure Effectiveness 2 if they have high level of Skills and Situation Awareness, and High Supply of Armoury for Defence?

17.2.In your opinion, how high does Port Forces Countermeasure Effectiveness 2 if they have high level of Skills and Situation Awareness, but low Supply of Armoury for Defence?

17.3.In your opinion, how high does Port Forces Countermeasure Effectiveness 2 if they have high level of Skills but low level of Situation Awareness, and low Supply of Armoury for Defence?

17.4.In your opinion, how high does Port Forces Countermeasure Effectiveness 2 if they have high level of Situation Awareness and high Supply of Armoury for Defence but low level of Skills?

17.5.In your opinion, how high does Port Forces Countermeasure Effectiveness 2 if they have high level of Situation Awareness but low level of Skills, and low Supply of Armoury for Defence?

17.6.In your opinion, how high does Port Forces Countermeasure Effectiveness 2 if they have high level of Skills and high Supply of Armoury for Defence but low level of Situation Awareness?

17.7.In your opinion, how high does Port Forces Countermeasure Effectiveness 2 if they have low level of Skills and Situation Awareness, but high Supply of Armoury for Defence?

17.8.In your opinion, how high does Port Forces Countermeasure Effectiveness 2 if they have low level of Skills and Situation Awareness, and low Supply of Armoury for Defence?

CE-3 Tested

C.Fire

18.1. In your opinion, what is the probability of fire occur if terrorist attack Wharf?

C.Countermeasure Effectiveness of Port Forces acting on Fire occurs in wharf.

19.0. Training

19.1. In your opinion, how high level of training does Port Forces received to counter terrorist attacks?

20.0. Experience

20.1 In your opinion, how high level of experience does Port Forces have to counter terrorist attacks?

21.0. Skills

21.1 In your opinion, how high level of skills does Port Forces have to counter terrorist attacks if they have high level of training and experience?

21.2.In your opinion, how high level of skills does Port Forces have to counter terrorist attacks if they have high level of training and low level of experience?

21.3.In your opinion, how high level of skills does Port Forces have to counter terrorist attacks if they have low level of training and high level of experience?

21.4.In your opinion, how high level of skills does Port Forces have to counter terrorist attacks if they have low level of training and experience?

22.0. Visual/ Hearing Awareness

22.1In your opinion, is it easy for Port Forces to see or hear from their places if any attack(s) happen on Wharf on Sites?

23.0. Emergency Call

23.1 In your opinion, does Port Forces have easy Access for Emergency Call from the workers at the wharf if any attack(s) happen on Wharf on Sites?

24.0. Emergency Fire Alarm

24.1 In your opinion, will the emergency fire alarm works if any attack(s) happen on Wharf on Sites?

25.0. Situation Awareness

25.1.In your opinion, how high level of Situation Awareness does Port Forces have if it is easy for them to see or hear any attacks from their places, easy Access for Emergency Call and the emergency fire alarm works?

25.2.In your opinion, how high level of Situation Awareness does Port Forces have if it is easy for them to see or hear any attacks from their places, easy Access for Emergency Call but the emergency fire alarm broke?

25.3.In your opinion, how high level of Situation Awareness does Port Forces have if it is easy for them to see or hear any attacks from their places, but bad Access for Emergency Call and the emergency fire alarm broke?

25.4.In your opinion, how high level of Situation Awareness does Port Forces have if it is difficult for them to see or hear any attacks from their places, but easy Access for Emergency Call and the emergency fire alarm works?

25.5.In your opinion, how high level of Situation Awareness does Port Forces have if it is difficult for them to see or hear any attacks from their places, and the emergency fire alarm broke but easy Access for Emergency Call?

25.6.In your opinion, how high level of Situation Awareness does Port Forces have if it is easy for them to see or hear any attacks from their places and the emergency fire alarm works, but bad Access for Emergency Call?

25.7.In your opinion, how high level of Situation Awareness does Port Forces have if it is difficult for them to see or hear any attacks from their places, bad Access for Emergency Call but the emergency fire alarm work?

25.8.In your opinion, how high level of Situation Awareness does Port Forces have if it is difficult for them to see or hear any attacks from their places, bad Access for Emergency Call and the emergency fire alarm broke?

26.0. Armoury Defence Supply

26.1. In your opinion, does Port Forces have high numbers of weapon for security and defense purposes?

27.0. Countermeasure Effectiveness

27.1. In your opinion, how high does Port Forces Countermeasure Effectiveness 3 if they have high level of Skills and Situation Awareness, and High Supply of Armoury for Defence?

27.2.In your opinion, how high does Port Forces Countermeasure Effectiveness 3 if they have high level of Skills and Situation Awareness, but low Supply of Armoury for Defence?

27.3.In your opinion, how high does Port Forces Countermeasure Effectiveness 3 if they have high level of Skills but low level of Situation Awareness, and low Supply of Armoury for Defence?

27.4.In your opinion, how high does Port Forces Countermeasure Effectiveness 3 if they have high level of Situation Awareness and high Supply of Armoury for Defence but low level of Skills?

27.5.In your opinion, how high does Port Forces Countermeasure Effectiveness 3 if they have high level of Situation Awareness but low level of Skills, and low Supply of Armoury for Defence?

27.6.In your opinion, how high does Port Forces Countermeasure Effectiveness 3 if they have high level of Skills and high Supply of Armoury for Defence but low level of Situation Awareness?

27.7.In your opinion, how high does Port Forces Countermeasure Effectiveness 3 if they have low level of Skills and Situation Awareness, but high Supply of Armoury for Defence?

27.8.In your opinion, how high does Port Forces Countermeasure Effectiveness 3 if they have low level of Skills and Situation Awareness, and low Supply of Armoury for Defence?

D. Injury and Loss of life

28.1. In your opinion, what is the probability that workers suffer injuries if terrorist attack the Wharf?

28.2. In your opinion, what is the probability that workers loss their life if terrorist attack the Wharf?

Thank you very much for spending your precious time in filling this questionnaire. If you wish to receive a summary of our survey findings, please provide us at W.M.AbdulHalim@2013.ljmu.ac.uk with your name and email address with the answered questionnaire and then we will send you the questionnaire result when it is ready for publication.

Example
Name: Angela R (Operations Manager)
Email: Angie.R@liverpool.gov.uk

Appendix 7

Questionnaire Part 2: The Measurement Scales for Countermeasure Effectiveness of Port Police

1.Port Police received training

Item	Condition(s)/ Situation(s)	No/Low					Neutral	Yes/High				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port Police received training	**When:** Average Condition											

2.Port police level of experience

Item	Condition(s)/ Situation(s)	No/Low					Neutral	Yes/High				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police level of experience	**When:** Average Condition											

3.Port police level of skills

Item	Condition(s)/ Situation(s)	No/Low					Neutral	Yes/High				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police level of skills	**When:** Port Police have high training											
	When: Port police have high level of experience											

4.Port police have the visual and hearing awareness if any attack(s) happen

Item		No/Low	Neutral	Yes/High

	Condition(s)/ Situation(s)	(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police have the visual and hearing awareness if any attack(s) happen	**When:** Average Condition											

5. Port police accessibility for emergency call

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police accessibility for emergency call	**When:** Average Condition											

6.Port police level of situation awareness if any attack(s) happen

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police level of situation awareness if any attack(s) happen	**When:** Port police have high visual and hearing awareness if any attack(s) happen											
	When: Port police high accessibility for emergency call											

7.Port police’s weapon for security and defense supply

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police’s weapon for security and defense supply	**When:** Average Condition											

8.Port police countermeasure effectiveness 1

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police countermeasure effectiveness 1	**When:** Port police high level of skills											

	When: Port police high level of situation awareness if any attack(s) happen											
	When: Port police's weapon for security and defense supply are high											

CE-2

1.Port Police received training

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port Police received training	**When:** Average Condition											

2.Port police level of experience

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police level of experience	**When:** Average Condition											

3.Port police level of skills

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police level of skills	**When:** Port Police have high training											
	When: Port police have high level of experience											

4.Port police have the visual and hearing awareness if any attack(s) happen

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5

Port police have the visual and hearing awareness if any attack(s) happen	**When:** Average Condition											

5. Port police accessibility for emergency call

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police accessibility for emergency call	**When:** Average Condition											

6.Port police level of situation awareness if any attack(s) happen

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police level of situation awareness if any attack(s) happen	**When:** Port police have high visual and hearing awareness if any attack(s) happen											
	When: Port police high accessibility for emergency call											

7.Port police’s weapon for security and defense supply

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police’s weapon for security and defense supply	**When:** Average Condition											

8.Port police countermeasure effectiveness 2

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police countermeasure effectiveness 2	**When:** Port police high level of skills											
	When: Port police high level of											

	situation awareness if any attack(s) happen											
	When: Port police's weapon for security and defense supply are high											

RE3

1.Port Police received training

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port Police received training	**When:** Average Condition											

2.Port police level of experience

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police level of experience	**When:** Average Condition											

3.Port police level of skills

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police level of skills	**When:** Port Police have high training											
	When: Port police have high level of experience											

4.Port police have the visual and hearing awareness if any attack(s) happen

Item	**Condition(s)/ Situation(s)**	**No/Low**					**Neutral**	**Yes/High**				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police have the visual and	**When:** Average Condition											

hearing awareness if any attack(s) happen												

5. Port police accessibility for emergency call

Item	Condition(s)/ Situation(s)	No/Low					Neutral	Yes/High				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police accessibility for emergency call	**When:** Average Condition											

6. Port police accessibility for emergency fire alarm

Item	Condition(s)/ Situation(s)	No/Low					Neutral	Yes/High				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police accessibility for emergency fire alarm	**When:** Average Condition											

7.Port police level of situation awareness if any attack(s) happen

Item	Condition(s)/ Situation(s)	No/Low					Neutral	Yes/High				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police level of situation awareness if any attack(s) happen	**When:** Port police have high visual and hearing awareness if any attack(s) happen											
	When: Port police high accessibility for emergency call											
	When: Port police high accessibility for emergency fire alarm											

8.Port police’s weapon for security and defense supply

Item	Condition(s)/ Situation(s)	No/Low					Neutral	Yes/High				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police's weapon for security and defense supply	**When:** Average Condition											

9.Port police countermeasure effectiveness 3

Item	Condition(s)/ Situation(s)	No/Low					Neutral	Yes/High				
		(5)	(4)	(3)	(2)	(1)	0	1	2	3	4	5
Port police countermeasure effectiveness 3	**When:** Port police high level of skills											
	When: Port police high level of situation awareness if any attack(s) happen											
	When: Port police's weapon for security and defense supply are high											

Appendix 8

Data collection was conducted by getting expert judgement on the subject of the study. A set of questionnaires was given to each of the selected experts and they were expected to respond based on their expert opinions. Discussions were held with the experts through scheduled interview sessions.

In this case study, all the necessary qualitative data were obtained from expert judgments by using the said questionnaires (Appendix 8). Five experts were selected based on their knowledge, expertise and experience in maritime industry of more than 10 years. All the experts contributed their opinion and judgements in developing a novel model, determining parameters and answering questionnaires. Below are their responses on the main criteria effectiveness on countermeasures.

Part A: Personal Information

Fill out your brief personal information

Brief of personal information. Please tick (/) for question Q02 and Q03.

Q01.Name	
Q02.Age	(__) 20 to 30 years old (__) 31 to 40 years old (__) 41 to 50 years old, (__) 51 to 60 years old, (__) 61 and above.
Q03.Job Area	(__) Port Authority, (__) Port Employee, (__) Ministry of Transportation, (__) Academician, (__) Others.
Q04.Job Experience	(__) years.

Part B until F:

Pair-Wise Comparison

Instructions: The goal of this study is to select which of the countermeasure alternatives is the most important in security effectiveness. The main criteria and the sub-criteria need to be evaluated by using a Pair-Wise Comparison" Technique.

Main Criteria	Sub-Criteria
Access Control and Deterrence	Landscaping and Layout
	Gate and Barrier
	Screening and Check-up
	Flexibility
Detection and Assessment	Hearing Detection and Assessment
	Visual Detection and Assessment
	Others Detection and Assessment
Response to The Threat	Security Staff Training
	Hiring Experience Staff
	Non-security Staff Training
Personnel and Security Equipment Cost	Drill Training Cost
	Experience Staff Salary
	Procurement Equipment Cost
	Security Equipment Maintenance Cost

Table 1: List of Main criteria and sub-criteria

Criteria	Meaning
Access Control and Deterrence	Is about limiting access to vulnerable assets only to those who have a legitimate need to access them and creating a psychological impression that the risk of acting as a threat actor could be greater than the reward, either through creating the possibility that the threat action may not succeed, or that the threat actor may be caught and penalized.

Detection and Assessment	Is about utilising detection technologies that can alert a security staff of any unwanted or inappropriate activity within their compound (seaport compound) and assess what has been detected to determine if it is a real threat or just a false alarm.
Response to The Threat	Is about people actions. When the attack event occurs, they need to know what they should do (such as giving a warning to the threat actors, deploy a barrier to delay the threat and aggressive responses like automated weapons when needed). The people that will be included will be the security staff, security expert and non-security staff.
Personnel and Security Equipment Cost	The cost of security consist Fixed Cost (High-Tech: annual payment for system licence, Low-Tech: Electricity payment the tech, or guard monthly for No-Tech), and Installation Cost (payment for one off installation of the system for example the Hi-Tech item, installation of the Electronic Turnstiles, or policy enforcement for No-Tech).
Landscaping and Layout	Reshaping the layout of the port compound into a secure environment without effecting the operation. (No-Tech - the physical shape of the port facilities such as CPTED element, Low-Tech – the lighting in the layout and High-Tech – installing security sensor along port layout)
CPTED (crime prevention through environmental design) is a scientifically proven architectural discipline that helps reduce criminal behaviour by creating spaces that encourage appropriate behaviour and reducing the likelihood of criminal activity.	
Gate and Barrier	Control the access from outside to prevent unwanted visitor from entering the compound. (No-Tech – Policies and Procedures, Low-Tech - Deployable Barriers/ Vehicle Gates/ Revolving Doors, and High-Tech - Card Technologies System/ Access Credential Reader Technologies).
Screening and Check-up	Conduct a check-up and screening to prevent any illegal item from entering the facilities (weapons and bomb). (No-Tech guard search/trained dog's inspection, Low-Tech - Mechanical and Electronic Turnstiles, High Tech - Photo Id Detectors).
Flexibility	A flexibility sub-criteria has one purpose, which is to take into consideration about customer satisfaction. While, having a good access control and deterrence security would be good to prevent threat and ensure the customer that their merchandise/container were well protected but it come with a huge cost which is tighter security would cause a delay, bottle neck and discomfort for the customer since port operations deals with a lot of outsiders from the land and the sea.
Hearing Detection and Assessment	Creating detection method using hearing that can alert a security staff of any unwanted or inappropriate activity within their compound then assess what has been detected to determine if it is a real threat or just a false alarm. (No-Tech – Security Post/ Routine Patrol, Low-Tech – Emergency Alarm/Fire Alarm/ Communication Device – Walkie Talkie, and High-Tech - Seismic Detection Systems/ Ultrasonic Sensors/ Duress Alarm).
Visual Detection and Assessment	Creating detection method using visual that can alert a security staff of any unwanted or inappropriate activity within their compound then assess what has been detected to determine if it is a real threat or just a false alarm. (No-Tech – Security Post/ Routine Patrol, Low-Tech – Visual Device – binocular scope/ Pan and Tilt CCTV, and High-Tech Capacitance Detection Systems/ Infrared and Laser Detection Systems / Ground-Based Radar).
Others Detection and Assessment	Creating detection method using others that can alert a security staff of any unwanted or inappropriate activity within their compound then assess what has been detected to determine if it is a real threat or just a false alarm. (No-Tech – Security Post/ Routine Patrol, Low-Tech – Vehicles Patrols – Surveillance Boat, Cars And Motorcycle, and High-Tech - Fiber-Optic Detection Systems/ Thermal Imaging Sensors such as x-ray and Chemical residue detection systems).
Security Staff Training	After security team confirm the threat from the assessment, they are responsible to protect the lives and the assets. This is done by delaying the threat actor from start taking action or mitigate the threat while waiting for help from outside back-up. No-Tech – consist of security guard (armed/Unarmed) training program. Low-Tech – training security guard with a Non-Lethal Weapon such as Water Canon, Net- Boat Trap, Fire Engine, Bomb Diffused program, and High-Tech– training security guard with an Advance Non-Lethal (such as -Long Range Acoustic Device (LRAD), Advanced Bomb Suit) and training to familiarise the with advance High-Tech security system for detection and assessment.
Hiring Experience Staff	Definition of experience staff in this aspect does not reflect only for experience in security. It also included a person who involve with military background, an expert in bomb defused, previously worked as a fireman and a person who previously worked as medical soldier. In here, their role is to train the security staff in using No-Tech, Low-Tech and High-Tech item.
Non-security Staff Training	All non-security staff were responsible to have some knowledge about the security countermeasure. This included with familiar with the security system High-Tech and Low-Tech installed in the facilities compound and prevent from any behaviour that may exploit those security items. On No-Tech areas, non-security should involve in emergency preparedness programs, and disaster recovery programs.
Drill Training Cost	Drill and Training Cost covers for both security staff and non-security staff. High-Tech would require more expenses since it required costly equipment, and hiring expert to train security staff and explain to non-security staff. Low-Tech and No Tech Would be lower cost than High-Tech.
Experience Staff Salary	Experience staff would be a little bit tricky since a lot of things need to be consider such as how many years has the expert work on such field, their accomplishment before being hired in to the company, their current condition right now does they still performs the same as before or even better, and were they just hired to became as instructor to trained new blood or they need to be involve in the security operation. The experts extra payment as a security staff will be consider due to their expertise in handling the items of security countermeasure (High-Tech, Low-Tech, No-Tech). [Justification – to measure the effectiveness of countermeasure]
Procurement Equipment Cost	Purchase of equipment for safety depends on the technology levels, while High-Tech has good technology (it can protect the building area with bigger range) but it costs a lot of money. On the other hand, No-Tech does not use technology (such as security staffs and dogs - they cannot protect the compound as a whole and if it wants to cover the whole area of the building, it will increase the cost of hiring the employee and the possibility of security control being compromise due to the risk of unethical and treacherous workers).
Security Equipment Maintenance Cost	Equipment maintenance for security also depends on technology level. For High-Tech, it may be cheaper since it requires a small number of employees to protect the entire port area. Unlike No-Tech, maintenance costs may be higher as it requires a large number of security personnel to monitor the entire port area. They also need to be protected with life and health insurance and provide training from time to time.

Table 2: Criteria's and definition

The pair-wise comparison technique is the technique of collecting data from expert opinion. Before proceeding with this technique, an expert has to understand the ratio scale measurement used in this study (Table 3). This table contain two parts which describe the numerical assessment together with the linguistic meaning of each number. The first part is on the left side which explains "Important", while the right side is the second part of the table which describe "Unimportant".

Numerical Assessment	Linguistic Meaning	Numerical Assessment	Linguistic Meaning
1	Equally Important	1	Equally Important
2	Intermediate Values of Importance	1/2	Intermediate Values of Unimportance
3	A Little Important	1/3	A Little Unimportant
4	Intermediate Values of Importance	1/4	Intermediate Values of Unimportance
5	Important	1/5	Unimportant
6	Intermediate Values of Importance	1/6	Intermediate Values of Unimportance
7	Very Important	1/7	Very Unimportant
8	Intermediate Values of Importance	1/8	Intermediate Values of Unimportance
9	Extremely Important	1/9	Extremely Unimportant

Table 3: Ratio Scale for Pair-Wise Comparisons

An expert is required to give a possible judgement to all question based on his/her expertise and experience in the shipping industry. The judgement process has to be focussed on how to achieve the Goals (Part C and Part D). Please tick (/) accordingly the rate of importance of each criteria, sub-criteria and sub-sub-criteria in the given column. For instance:

Goal: To select the most important component of a computer.

1) Monitor

	Unimportant								Equally Important	Important							
	1/9	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is the monitor compared to the keyboard?															/		
To achieve the above goal, how important is the monitor compared to the mouse?											/						
To achieve the above goal, how important is the monitor compared to the central unit processing (CPU)?		/															

The explanation of the above example,

i) The monitor screen is 7 times more "IMPORTANT" than the mouse. It is because we can still use our computer even without the mouse. If the mouse is broken, then we can use the short cut system to access any file or document in the computer by using a keyboard, for instance: to print (Ctrl+P), to save document (Ctrl+S), *etc*..

ii) The monitor screen is 3 times more “IMPORTANT” than the keyboard. It is because we can still explore a computer even without the keyboard, for example, to search file in My Document by using a mouse. Additionally, we can read any journal or article papers on the monitor screen even without the keyboard. The only thing we cannot do without the keyboard is typing.

iii) The monitor screen is 1/8 times less “UNIMPORTANT” than the CPU. The monitor is useless without the CPU.

Part B: Main Criteria

Goal: The goal of this question is to choose which one is the most important.

Q05. Access Control and Deterrence.

	Unimportant								Equally Important	Important							
	1/9	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Access Control and Deterrence compared to Detection and Assessment?																	
To achieve the above goal, how important is Access Control and Deterrence compared to Response to The Threat?																	
To achieve the above goal, how important is Access Control and Deterrence compared to Personnel and Security Equipment Cost?																	

Q06. Detection and Assessment.

	Unimportant								Equally Important	Important							
	1/9	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Detection and Assessment compared to Response to The Threat?																	
To achieve the above goal, how important is Detection and Assessment compared to Personnel and Security Equipment Cost?																	

Q07. Response to the Threat.

	Unimportant								Equally Important	Important							
	1/9	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Response to The Threat compared to Personnel and Security Equipment Cost?																	

Part C: Sub-Criteria for Access Control and Deterrence

Goal: To select the most important sub-criteria that influencing Access Control and Deterrence.

Q08. Landscaping and Layout.

	Unimportant								Equally Important	Important							
	$^1/_9$	$^1/_8$	$^1/_7$	$^1/_6$	$^1/_5$	$^1/_4$	$^1/_3$	$^1/_2$	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Landscaping and Layout compared to Gate and Barrier?																	
To achieve the above goal, how important is Landscaping and Layout compared to Screening and Check-up?																	
To achieve the above goal, how important is Landscaping and Layout compared to Flexibility?																	

Q09. Gate and Barrier.

	Unimportant								Equally Important	Important							
	$^1/_9$	$^1/_8$	$^1/_7$	$^1/_6$	$^1/_5$	$^1/_4$	$^1/_3$	$^1/_2$	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Gate and Barrier compared to Screening and Check-up?																	
To achieve the above goal, how important is Gate and Barrier compared to Flexibility?																	

Q10. Screening and Check-up.

	Unimportant								Equally Important	Important							
	$^1/_9$	$^1/_8$	$^1/_7$	$^1/_6$	$^1/_5$	$^1/_4$	$^1/_3$	$^1/_2$	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Screening and Check-up to Flexibility?																	

Part D: Sub-Criteria of Detection and Assessment

Goal: To select the most important sub-criteria that influencing Detection and Assessment.

Q11. Hearing Detection and Assessment

	Unimportant								Equally Important	Important							
	$^1/_9$	$^1/_8$	$^1/_7$	$^1/_6$	$^1/_5$	$^1/_4$	$^1/_3$	$^1/_2$	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Hearing Detection and Assessment to Visual Detection and Assessment?																	
To achieve the above goal, how important is Hearing Detection and Assessment to Others Detection and Assessment?																	

Q12. Visual Detection and Assessment

	Unimportant								Equally Important	Important							
	1/9	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Visual Detection and Assessment to Others Detection and Assessment?																	

Part E: Sub-Criteria of Response to the Threat

Goal: To select the most important sub-criteria that influencing Response to The Threat.

Q13. Security Staff Training.

	Unimportant								Equally Important	Important							
	1/9	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Security Staff Training to Hiring Experience Staff?																	
To achieve the above goal, how important is Security Staff Training to Non-security Staff Training?																	

Q14. Hiring Experience Staff.

	Unimportant								Equally Important	Important							
	1/9	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Hiring Experience Staff to Non-security Staff Training?																	

Part F: Sub-Criteria of Personnel and Security Equipment Cost

Goal: To select the most important sub-criteria that influencing Personnel and Security Equipment Cost.

Q15. Drill Training Cost

	Unimportant								Equally Important	Important							
	1/9	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Drill Training Cost to Experience Staff Salary?																	
To achieve the above goal, how important is Drill Training Cost to Procurement Equipment Cost?																	
To achieve the above goal, how important is Drill Training Cost to Security Equipment Maintenance Cost?																	

Q16. Experience Staff Salary

	Unimportant								Equally Important	Important							
	$^1/_9$	$^1/_8$	$^1/_7$	$^1/_6$	$^1/_5$	$^1/_4$	$^1/_3$	$^1/_2$	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Experience Staff Salary to Procurement Equipment Cost?																	
To achieve the above goal, how important is Experience Staff Salary to Security Equipment Maintenance Cost?																	

Q17. Procurement Equipment Cost.

	Unimportant								Equally Important	Important							
	$^1/_9$	$^1/_8$	$^1/_7$	$^1/_6$	$^1/_5$	$^1/_4$	$^1/_3$	$^1/_2$	1	2	3	4	5	6	7	8	9
To achieve the above goal, how important is Procurement Equipment Cost to Security Equipment Maintenance Cost?																	

Appendix 9

A set of questionnaires (Appendix 9) was sent to each of the selected experts for their evaluation and their feedbacks were investigated accordingly based on their judgments on the criteria under discussion. Referring to the four main criteria as mentioned earlier and together with Equation 5.19, a 4×4 pair-wise comparison matrix was developed to obtain the weightage of these criteria. *A(AcdDaRttPesc)* is a pair-wise comparison matrix expressing the qualified judgment with regard to the relative priority of ACD, DA, RTT, and PESC (Table 5.10).

Part G: A set of questionnaire for obtaining the belief degree values

Instructions: Please select a possible number listed in Table 4 for determining belief degree values of each selected criterion with respect to all alternatives.

Number	Meaning
0.1 between 0.2	*Low*
0.3 between 0.4	*Reasonably Low*
0.5 between 0.6	*Average/Moderate*
0.7 between 0.8	*Reasonably High*
0.9 between 1.0	*High*

Table 4: The linguistic belief degree

The questionnaire for the value of "belief degree" is one of the techniques to collect data from expert opinion. You need to fill your confidence rate values for a topic between 0.1 and 1.0. You can fill in two or three squares of the available tables (Colour Table).

Please make sure your belief degree total are equal to 1

For example:

Which are the possible number listed in Table 4 for determining belief degree values of the criterion "Phone Price" with respect to all the alternatives?

Alternative	Phone Price						Total
	Expensive	Reasonably Expensive	Average	Reasonably Cheap	Cheapest		
Iphone	0.9	0.1				0.9+0.1=	1
Samsung	0.8	0.2				0.8+0.2=	1
Sony	0.2	0.6	0.2			0.2+0.6+0.2=	1
Oppo		0.15	0.7	0.15		0.15+0.7+0.15=	1
Vivo				0.55	0.45	0.55+0.45=	1

Explanation:

1. The phone price of the Iphone is {(0.9, Expensive), (0.1, Reasonably Expensive)} which is higher than the Sony Phone's {(0.2, Expensive), (0.6, Reasonably Expensive), (0.2, Average)}.

2. The phone price of the Oppo Phone is {(0.15, Reasonably Expensive), (0.7, Average), (0.15, Reasonably Cheap)} which is higher than the Vivo Phone’s {(0.55, Reasonably Cheap), (0.45, Cheapest)}.

Alternatives	Meaning
High-Tech Security Countermeasure	Hi-tech (electronic) countermeasures employ electronic systems to deter, detect, assess, and assist in the response and to collect evidence.
Low-Tech Security Countermeasure	Lo-tech solutions include locks, barriers, lighting, and architectural solutions.
No-Tech Security Countermeasure	No-tech solutions include policies and procedures, security staffing, training, awareness programs, investigations, and security dogs

Q18. Which are the possible number listed in Table 4 for determining belief degree values of the criterion “Landscaping and Layout” with respect to all the alternatives?

Alternative	Landscaping and Layout				
	Poor	Reasonably Poor	Average	Reasonably Good	Good
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q19. Which are the possible number listed in Table 4 for determining belief degree values of the criterion “Gate and Barrier” with respect to all the alternatives?

Alternative	Gate and Barrier				
	Poor	Reasonably Poor	Average	Reasonably Good	Good
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q20. Which are the possible number listed in Table 4 for determining belief degree values of the criterion “Screening and Check-up” with respect to all the alternatives?

Alternative	Screening and Check-up				
	Poor	Reasonably Poor	Average	Reasonably Good	Good

High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q21. Which are the possible number listed in Table 4 for determining belief degree values of the criterion “Flexibility” with respect to all the alternatives?

Alternative	Flexibility				
	Poor	Reasonably Poor	Average	Reasonably Good	Good
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q22. Which are the possible number listed in Table 4 for determining belief degree values of the criterion “Hearing Detection and Assessment” with respect to all the alternatives?

Alternative	Hearing Detection and Assessment				
	Poor	Reasonably Poor	Average	Reasonably Good	Good
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q23. Which are the possible number listed in Table 4 for determining belief degree values of the criterion “Visual Detection and Assessment” with respect to all the alternatives?

Alternative	Visual Detection and Assessment				
	Poor	Reasonably Poor	Average	Reasonably Good	Good
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q24. Which are the possible number listed in Table 4 for determining belief degree values of the criterion “Others Detection and Assessment” with respect to all the alternatives?

Alternative	Others Detection and Assessment				
	Poor	Reasonably Poor	Average	Reasonably Good	Good
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q25. Which are the possible number listed in Table 4 for determining belief degree values of the criterion “Security Staff Training” with respect to all the alternatives?

Alternative	Security Staff Training				
	Poor	Reasonably Poor	Average	Reasonably Good	Good
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q26. Which are the possible number listed in Table 4 for determining belief degree values of the criterion “Hiring Experience Staff with respect to all the alternatives?

Alternative	Hiring Experience Staff				
	Poor	Reasonably Poor	Average	Reasonably Good	Good
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q27. Which are the possible number listed in Table 4 for determining belief degree values of the criterion “Non-security Staff Training” with respect to all the alternatives?

Alternative	Non-security Staff Training				
	Poor	Reasonably Poor	Average	Reasonably Good	Good
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q28. Which are the possible number listed in Table 4 for determining belief degree values of the criterion “Drill Training Cost” with respect to all the alternatives?

Alternative	Drill Training Cost				
	High Cost	Reasonably High Cost	Average Cost	Reasonably Low Cost	Low Cost
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q29. Which are the possible number listed in Table 4 for determining belief degree values of the criterion "Experience Staff Salary" with respect to all the alternatives?

Alternative	Experience Staff Salary				
	High Salary	Reasonably High Salary	Average Salary	Reasonably Low Salary	Low Salary
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q30. Which are the possible number listed in Table 4 for determining belief degree values of the criterion "Procurement Equipment Cost" with respect to all the alternatives?

Alternative	Procurement Equipment Cost				
	High Cost	Reasonably High Cost	Average Cost	Reasonably Low Cost	Low Cost
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

Q31. Which are the possible number listed in Table 4 for determining belief degree values of the criterion "Security Equipment Maintenance Cost" with respect to all the alternatives?

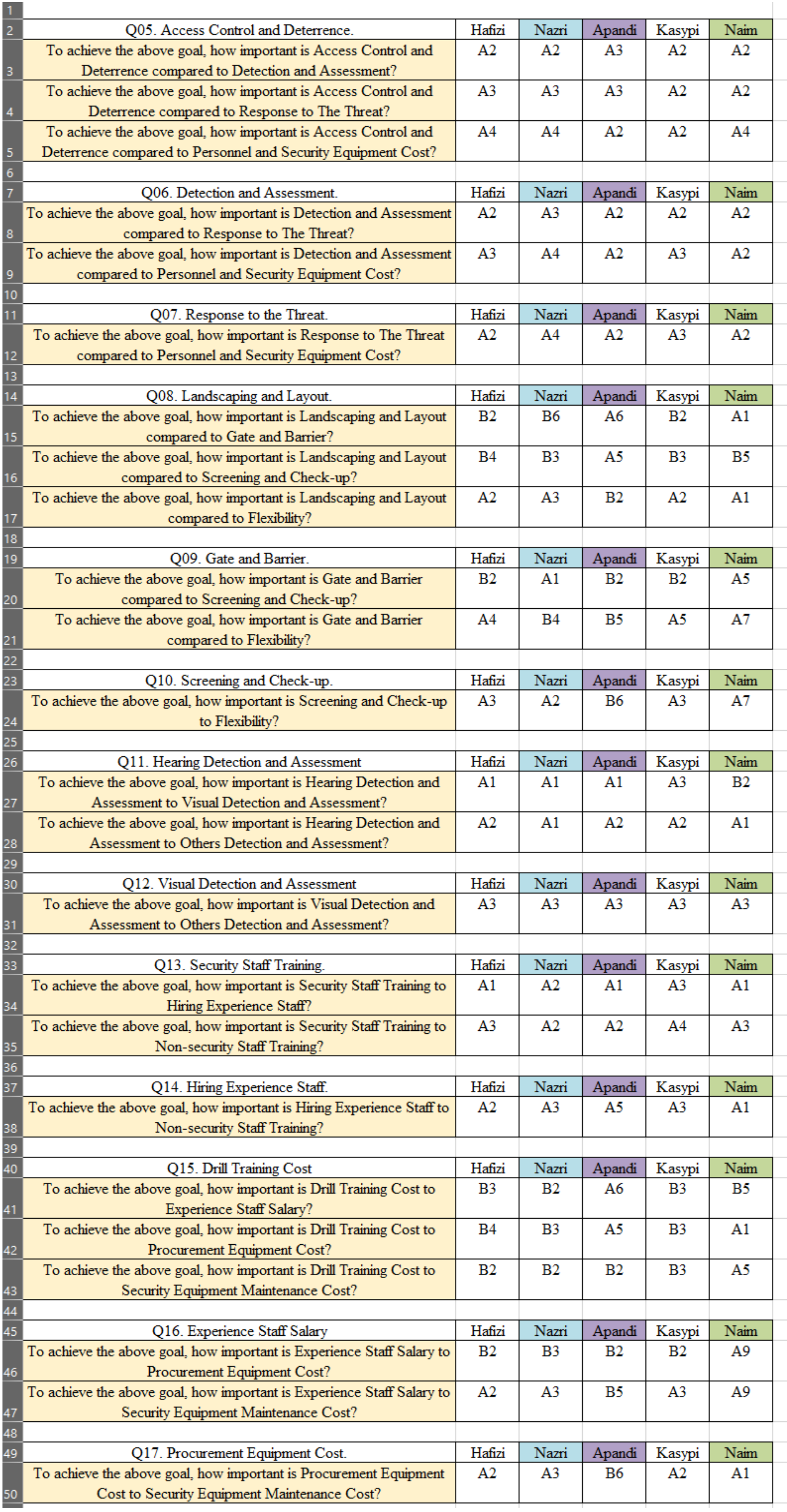
Alternative	Security Equipment Maintenance Cost				
	High Cost	Reasonably High Cost	Average Cost	Reasonably Low Cost	Low Cost
High-Tech Security Countermeasure					
Low-Tech Security Countermeasure					
No-Tech Security Countermeasure					

This is the end of the questionnaire. Thank you very much for your help.

Thank you very much for spending your precious time in filling this questionnaire. If you wish to receive a summary of our survey findings, please provide us at onezu3@gmail.com with your name and email address with the answered questionnaire and then we will send you the questionnaire result when it is ready for publication.

Example
Name: Angela R (Operations Manager)
Email: Angie.R@liverpool.gov.uk

Appendix 10 – A Result from Survey in Obtaining the Weight Values -Q05 till Q17



Q05. Access Control and Deterrence.	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Access Control and Deterrence compared to Detection and Assessment?	A2	A2	A3	A2	A2
To achieve the above goal, how important is Access Control and Deterrence compared to Response to The Threat?	A3	A3	A3	A2	A2
To achieve the above goal, how important is Access Control and Deterrence compared to Personnel and Security Equipment Cost?	A4	A4	A2	A2	A4

Q06. Detection and Assessment.	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Detection and Assessment compared to Response to The Threat?	A2	A3	A2	A2	A2
To achieve the above goal, how important is Detection and Assessment compared to Personnel and Security Equipment Cost?	A3	A4	A2	A3	A2

Q07. Response to the Threat.	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Response to The Threat compared to Personnel and Security Equipment Cost?	A2	A4	A2	A3	A2

Q08. Landscaping and Layout.	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Landscaping and Layout compared to Gate and Barrier?	B2	B6	A6	B2	A1
To achieve the above goal, how important is Landscaping and Layout compared to Screening and Check-up?	B4	B3	A5	B3	B5
To achieve the above goal, how important is Landscaping and Layout compared to Flexibility?	A2	A3	B2	A2	A1

Q09. Gate and Barrier.	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Gate and Barrier compared to Screening and Check-up?	B2	A1	B2	B2	A5
To achieve the above goal, how important is Gate and Barrier compared to Flexibility?	A4	B4	B5	A5	A7

Q10. Screening and Check-up.	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Screening and Check-up to Flexibility?	A3	A2	B6	A3	A7

Q11. Hearing Detection and Assessment	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Hearing Detection and Assessment to Visual Detection and Assessment?	A1	A1	A1	A3	B2
To achieve the above goal, how important is Hearing Detection and Assessment to Others Detection and Assessment?	A2	A1	A2	A2	A1

Q12. Visual Detection and Assessment	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Visual Detection and Assessment to Others Detection and Assessment?	A3	A3	A3	A3	A3

Q13. Security Staff Training.	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Security Staff Training to Hiring Experience Staff?	A1	A2	A1	A3	A1
To achieve the above goal, how important is Security Staff Training to Non-security Staff Training?	A3	A2	A2	A4	A3

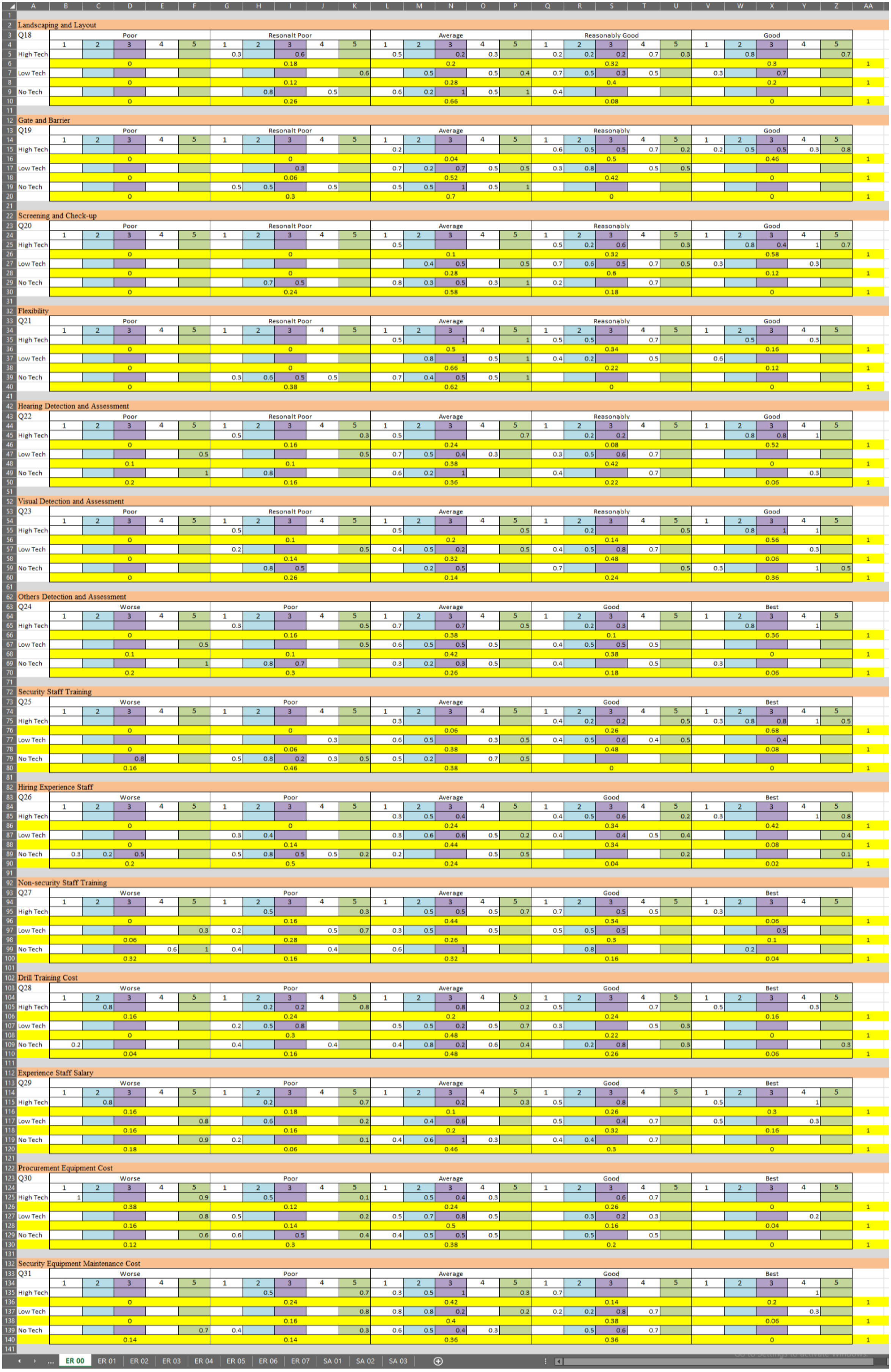
Q14. Hiring Experience Staff.	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Hiring Experience Staff to Non-security Staff Training?	A2	A3	A5	A3	A1

Q15. Drill Training Cost	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Drill Training Cost to Experience Staff Salary?	B3	B2	A6	B3	B5
To achieve the above goal, how important is Drill Training Cost to Procurement Equipment Cost?	B4	B3	A5	B3	A1
To achieve the above goal, how important is Drill Training Cost to Security Equipment Maintenance Cost?	B2	B2	B2	B3	A5

Q16. Experience Staff Salary	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Experience Staff Salary to Procurement Equipment Cost?	B2	B3	B2	B2	A9
To achieve the above goal, how important is Experience Staff Salary to Security Equipment Maintenance Cost?	A2	A3	B5	A3	A9

Q17. Procurement Equipment Cost.	Hafizi	Nazri	Apandi	Kaspyi	Naim
To achieve the above goal, how important is Procurement Equipment Cost to Security Equipment Maintenance Cost?	A2	A3	B6	A2	A1

Appendix 11 – A Result from Survey in Obtaining the Belief Degree Values -Q18 till Q31



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA
1																											
2	Landscaping and Layout																										
3	Q18	Poor					Resonalt Poor					Average					Reasonably Good					Good					
4		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
5	High Tech						0.3		0.6			0.5		0.2	0.3		0.2	0.2	0.2	0.7	0.3		0.8			0.7	
6		0					0.18					0.2					0.32					0.3					1
7	Low Tech										0.6		0.5		0.5	0.4	0.7	0.5	0.3	0.5		0.3		0.7			
8		0					0.12					0.28					0.4					0.2					1
9	No Tech							0.8		0.5		0.6	0.2	1	0.5	1	0.4										
10		0					0.26					0.66					0.08					0					1
11																											
12	Gate and Barrier																										
13	Q19	Poor					Resonalt Poor					Average					Reasonably					Good					
14		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
15	High Tech											0.2					0.6	0.5	0.5	0.7	0.2	0.2	0.5	0.5	0.3	0.8	
16		0					0					0.04					0.5					0.46					1
17	Low Tech								0.3			0.7	0.2	0.7	0.5	0.5	0.3	0.8		0.5	0.5						
18		0					0.06					0.52					0.42					0					1
19	No Tech						0.5	0.5		0.5		0.5	0.5	1	0.5	1											
20		0					0.3					0.7					0					0					1
21																											
22	Screening and Check-up																										
23	Q20	Poor					Resonalt Poor					Average					Reasonably					Good					
24		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
25	High Tech											0.5					0.5	0.2	0.6		0.3		0.8	0.4	1	0.7	
26		0					0					0.1					0.32					0.58					1
27	Low Tech												0.4	0.5		0.5	0.7	0.6	0.5	0.7	0.5	0.3			0.3		
28		0					0					0.28					0.6					0.12					1
29	No Tech							0.7	0.5			0.8	0.3	0.5	0.3	1	0.2			0.7							
30		0					0.24					0.58					0.18					0					1
31																											
32	Flexibility																										
33	Q21	Poor					Resonalt Poor					Average					Reasonably					Good					
34		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
35	High Tech											0.5		1		1	0.5	0.5		0.7			0.5		0.3		
36		0					0					0.5					0.34					0.16					1
37	Low Tech												0.8	1	0.5	1	0.4	0.2		0.5		0.6					
38		0					0					0.66					0.22					0.12					1
39	No Tech						0.3	0.6	0.5	0.5		0.7	0.4	0.5	0.5	1											
40		0					0.38					0.62					0					0					1
41																											
42	Hearing Detection and Assessment																										
43	Q22	Poor					Resonalt Poor					Average					Reasonably					Good					
44		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
45	High Tech						0.5				0.3	0.5				0.7		0.2	0.2				0.8	0.8	1		
46		0					0.16					0.24					0.08					0.52					1
47	Low Tech					0.5					0.5	0.7	0.5	0.4	0.3		0.3	0.5	0.6	0.7							
48		0.1					0.1					0.38					0.42					0					1
49	No Tech					1		0.8				0.6	0.2	1			0.4			0.7					0.3		
50		0.2					0.16					0.36					0.22					0.06					1
51																											
52	Visual Detection and Assessment																										
53	Q23	Poor					Resonalt Poor					Average					Reasonably					Good					
54		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
55	High Tech						0.5					0.5				0.5		0.2			0.5		0.8	1	1		
56		0					0.1					0.2					0.14					0.56					1
57	Low Tech						0.2				0.5	0.4	0.5	0.2		0.5	0.4	0.5	0.8	0.7					0.3		
58		0					0.14					0.32					0.48					0.06					1
59	No Tech							0.8	0.5				0.2	0.5			0.7				0.5	0.3			1	0.5	
60		0					0.26					0.14					0.24					0.36					1
61																											
62	Others Detection and Assessment																										
63	Q24	Worse					Poor					Average					Good					Best					
64		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
65	High Tech						0.3				0.5	0.7		0.7		0.5		0.2	0.3				0.8		1		
66		0					0.16					0.38					0.1					0.36					1
67	Low Tech					0.5					0.5	0.6	0.5	0.5	0.5		0.4	0.5	0.5	0.5							
68		0.1					0.1					0.42					0.38					0					1
69	No Tech					1		0.8	0.7			0.3	0.2	0.3	0.5		0.4			0.5		0.3					
70		0.2					0.3					0.26					0.18					0.06					1
71																											
72	Security Staff Training																										
73	Q25	Worse					Poor					Average					Good					Best					
74		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
75	High Tech											0.3					0.4	0.2	0.2		0.5	0.3	0.8	0.8	1	0.5	
76		0					0					0.06					0.26					0.68					1
77	Low Tech									0.3		0.6	0.5		0.3	0.5	0.4	0.5	0.6	0.4	0.5			0.4			
78		0					0.06					0.38					0.48					0.08					1
79	No Tech			0.8			0.5	0.8	0.2	0.3	0.5	0.5	0.2		0.7	0.5											
80		0.16					0.46					0.38					0					0					1
81																											
82	Hiring Experience Staff																										
83	Q26	Worse					Poor					Average					Good					Best					
84		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
85	High Tech											0.3	0.5	0.4			0.4	0.5	0.6		0.2	0.3			1	0.8	
86		0					0					0.24					0.34					0.42					1
87	Low Tech						0.3	0.4				0.3	0.6	0.6	0.5	0.2	0.4		0.4	0.5	0.4					0.4	
88		0					0.14					0.44					0.34					0.08					1
89	No Tech	0.3	0.2	0.5			0.5	0.8	0.5	0.5	0.2	0.2			0.5	0.5					0.2					0.1	
90		0.2					0.5					0.24					0.04					0.02					1
91																											
92	Non-security Staff Training																										
93	Q27	Worse					Poor					Average					Good					Best					
94		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
95	High Tech							0.5			0.3		0.5	0.5	0.5	0.7	0.7		0.5	0.5		0.3					
96		0					0.16					0.44					0.34					0.06					1
97	Low Tech					0.3	0.2			0.5	0.7	0.3	0.5		0.5		0.5	0.5	0.5					0.5			
98		0.06					0.28					0.26					0.3					0.1					1
99	No Tech				0.6	1	0.4			0.4		0.6		1				0.8					0.2				
100		0.32					0.16					0.32					0.16					0.04					1
101																											
102	Drill Training Cost																										
103	Q28	Worse					Poor					Average					Good					Best					
104		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
105	High Tech		0.8					0.2	0.2		0.8			0.8		0.2	0.5			0.7		0.5			0.3		
106		0.16					0.24					0.2					0.24					0.16					1
107	Low Tech						0.2	0.5	0.8			0.5	0.5	0.2	0.5	0.7	0.3			0.5	0.3						
108		0					0.3					0.48					0.22					0					1
109	No Tech	0.2					0.4			0.4		0.4	0.8	0.2	0.6	0.4		0.2	0.8		0.3					0.3	
110		0.04					0.16					0.48					0.26					0.06					1
111																											
112	Experience Staff Salary																										
113	Q29	Worse					Poor					Average					Good					Best					
114		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
115	High Tech		0.8					0.2			0.7			0.2		0.3	0.5		0.8			0.5			1		
116		0.16					0.18					0.1					0.26					0.3					1
117	Low Tech					0.8		0.6			0.2		0.4	0.6			0.5		0.4	0.7		0.5			0.3		
118		0.16					0.16					0.2					0.32					0.16					1
119	No Tech					0.9	0.2				0.1	0.4	0.6	1	0.3		0.4	0.4		0.7							
120		0.18					0.06					0.46					0.3					0					1
121																											
122	Procurement Equipment Cost																										
123	Q30	Worse					Poor					Average					Good					Best					
124		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
125	High Tech	1				0.9		0.5			0.1		0.5	0.4	0.3				0.6	0.7							
126		0.38					0.12					0.24					0.26					0					1
127	Low Tech					0.8	0.5				0.2	0.5	0.7	0.8	0.5			0.3	0.2	0.3					0.2		
128		0.16					0.14					0.5					0.16					0.04					1
129	No Tech					0.6	0.6		0.5		0.4	0.4	0.5	0.5	0.5			0.5		0.5							
130		0.12					0.3					0.38					0.2					0					1
131																											
132	Security Equipment Maintenance Cost																										
133	Q31	Worse					Poor					Average					Good					Best					
134		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
135	High Tech							0.5			0.7	0.3	0.5	1		0.3	0.7								1		
136		0					0.24					0.42					0.14					0.2					1
137	Low Tech										0.8	0.8	0.8	0.2		0.2	0.2	0.2	0.8	0.7					0.3		
138		0					0.16					0.4					0.38					0.06					1
139	No Tech					0.7	0.4				0.3	0.6	0.5	0.4	0.3			0.5	0.6	0.7							
140		0.14					0.14					0.36					0.36					0					1
141																											