UNIVERSITI TEKNOLOGI MARA
FACULTY OF ADMINISTRATIVE SCIENCE AND POLICY STUDIES

CYBER WARFARE IMPACT TO NATIONAL SECURITY - MALAYSIA EXPERIENCES

DAYANG NURFAUZIAH BINTI FAUZI
201262282
DINA HAZELBELLA BINTI DILLAH
2012600148

JUNE 2015

Table of Contents **Page**

ABSTRACT

This research study analyzes the cyber warfare impact to national security and focusing on Malaysia experiences. The issues regarding the cyber warfare is become a serious issues since it was a threat to national security in Malaysia. Cyber Security Malaysia department was involved in assist us in answering the questions regarding our research. The respondent who has helped us partly in completing our research was the Senior Manager, Research Management Centre, Strategic Research & Advisory Department. This research can contribute to improve security of the national security by requiring the government to foster a comprehensive acquisition risk management strategy. It also to facilitate the development of highly effective offensive and defensive strategies of an organization in meeting the future challenges of cyber warfare threat. A preliminary contacts research design was utilized for the purpose of this study in order to assess the validity and reliability of the data. A qualitative research design was used for the purpose of this study, in a way to acquire the desired outcomes of the research.

CHAPTER 1

INTRODUCTION

1.0 Introduction

As mentioned by Global Information Assurance Certification Paper (2004) cyber warfare can be defined as cyber-attacks offer terrorists the possibility of greater security and operational flexibility. This theoretically they can launch a computer assault from almost anywhere in the world, without directly exposing the attacker to physical harm. In other words, this cyber warfare can hacked the system of the computer without the owner of the computer knows that their computers been hacked by those cyber-attackers. They can attack the computer from one location to another location just by one click of the mouse.

According to Ahmad Hemmat (2011) in recent decades, the world has witnessed salient social transformation as our lives became inextricably linked and dependent upon technology and more particularly the internet. It has brought the influences in every aspect of people business and governmental transactions. There is crucial to understand and learn more about the cyber warfare due to the current environment now that all depending solely on the internet.

Furthermore, based on what U.S Army's Cyber Operations and Cyber Terrorism Handbook defines cyber warfare as simply the latest form of information warfare and can include computer network attack (CNA), which consists of operations to disrupt, deny, degrades or destroy information resident in computers or computer networks or the computers and network themselves (Swanson, 2010). Basically, a CNA involves in "hacking" of another nation's computer networks but uses data systems as opposed to physical weapons to execute the attack.

There are important elements that must be highlighted which are attack and defend. The information would be the one been attacked. Based on Ahmad Hemmat (2011) stealing information from storage devices and also attack on processes that collect, analyse, and disseminate information using any medium or form and attack on the networking.

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

This chapter will succinctly and clearly identify and define the cyber warfare issues and area of concern so as to provide a context in which the literature to be reviewed. This will indicate the area of investigation and theoretical perspective and include the importance, interesting and relevant of the cyber warfare. This chapter will also depict the parameters of cyber warfare and explain the approach used by Malaysian government in curbing the cyber warfare issues.

2.1 Literature Review

2.1.1 Definition

Cyber warfare can be defined as attacking and defending information and computer networks in cyberspace, as well as denying and adversary's ability to do the same (Global Information Assurance Certification Paper, 2004). According to Billo (2004) cyber warfare involves units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computer or network through electronic means. There are two important elements in the definition, those is attack and defend. The important element needs to be attacked are:

i. Information- For instance, stealing information from storage devices.
ii. Information based processes- attack on processes that collect, analyze and disseminate information using any medium or form.
iii. Information and communication systems- For example, attack on the infrastructure, organization, personnel and components that collect, process, store and act on information.

On top of that, important elements that also need to be defended are including: