CYBERSPACE AS A NATIONAL SECURITY ISSUE IN MALAYSIA

BY

AINAA NADZIRAH BINTI MALEK FAROK

A dissertation submitted in fulfilment of the requirement for the degree of Master of Human Sciences (Political Science)

Kulliyyah of Islamic Revealed Knowledge and Human Science
International Islamic University Malaysia

MARCH 2015

ABSTRACT

This study explains the linkages between cyberspace and national security of Malaysia. It also discusses the views of government personnel as well as those from private agencies about the relationship between cyberspace and national security of the country. The thesis examines the nature of threats to cyberspace in public and private sectors in Malaysia, and also analyses the policies adopted by the Malaysian government to deal with cyber threats in Malaysia. The research uses both primary and secondary sources. It uses data collected from online interviews conducted with a number of personnel working in public and private agencies in Malaysia. Data were also collected from such primary sources as official reports, publications and various documents on the subject published by CyberSecurity Malaysia, Bank Negara Malaysia, and the Malaysian Communications and Multimedia Commission.These primary sources were supplemented by various newspaper reports, books, magazines, and scholarly journals on the subject matter of this thesis. This study has found a clear relationship between Malaysia's cyberspace and the country's national security. The major threats to Malaysia's national security emanating from cyberspace are mostly centred on cyber-crimes. However, the thesis has also discovered that there is a lack of public awareness about cyber-crimes and other forms of threats to cyberspace in Malaysia. It is only through the adoption of strong policies and measures by the government that cyber threats and cyber-crimes can be dealt with. It is recommended that more measures should be undertaken by both the government and the private sectors to undertake technological and social research on the subject matter. In addition, government policies need to be looked at from time to time and if necessary, adopt new policies to keep them at pace with new technological innovations. The cooperation between various local and international agencies must be developed further in order to make sure that Malaysia's cyberspace is safe and remains well-protected, and thus making sure that Malaysia's cyber-security remains secured.

ملخص البحث

تسعى هذه الدراسة إلى توضيح الروابط المشتركة بين الفضاء السيبراني والأمن الوطني بماليزيا. كما أنها تناقش آراء الموظفين من الجهات الحكومية والخاصة حول هذه العلاقة. هذا البحث يدرس عن طبيعة التهديدات التي تعكس عنه في القطاعات العامة والخاصة للدولة، ويحلل الأنظمة التي اتخذها الحكومة الماليزية لمعالجة هذه التهديدات. كذلك يعمد إلى استخدام كلا المصدرين الأولية والثانوية، واعتمد في جمع البيانات عن طريق المقابلات على شبكة الانترنت أجريت مع فئة من العاملين في القطاعين. كما أن المصادر الأولية التي اعتمدت عليها هي: التقريرات الرسمية، والمنشورات، والوثائق المختلفة المنشورة من قبل: الأمن السيبراني بماليزيا، وبنك نيجارا ماليزيا، واللجنة الماليزية للاتصالات والوسائط المتعددة. هذه المصادر الأولية مزودة بتقريرات صحفية متنوعة، وكتب، ومجلات علمية وغير علمية منوطة بموضوع البحث. كذلك وجدت الدراسة أن هناك علاقة واضحة بين الفضاء السيبراني الماليزي والأمن الوطني للدولة، وأن التهديدات الرئيسة للأمن الوطني الماليزي نابعة من الفضاء السيبراني والتي ترتكز معظمها على الجرائم السبرانية. كما أن الدراسة كشفت الحاجة والضرورة بوجود الوعي العام لهذه الجرائم السيبرانية أو لأشكال أخرى تمثل هذه التهديدات. يمكن التعامل مع الجرائم السيبرانية وتهديدات الفضاء السيبراني من خلال الاعتماد على تدبيرات وسياسات قوية من قبل الحكومة. يوصي هذا البحث بالتضطلع إلى مزيد من التدبيرات التي ينبغي على كلا القطاعين العام والخاص النظر إليها تكنولوجيا واجتماعياً. إضافة إلى ضرورة إعادة النظر في السياسات الحكومية من وقت لآخر من أجل إنشاء سياسات جديدة تواكب الابتكارات التكنولوجية الجديدة. الجمعية التعاونية بين مختلف الوكالات المحلية والدولية يجب تحسينها لتوفر الأمن والحماية للفضاء السيبراني وتجعل الأمن السيبراني الماليزي يظل آمناً.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality as dissertation for the degree of Master of Human Sciences (Political Science).

……..……
Ishtiaq Hossain
Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality as a dissertation for the degree of Master of Human Sciences (Political Science).

……..……
Norhaslinda Bt Jamaiudin
Examiner

This dissertation was submitted to the Department of Political Science and is accepted as fulfilment of the requirement for the degree of Master of Human Sciences (Political Science).

……..……
Tunku Mohar Bin Tunku Mokhtar
Head, Department of Political Science

This dissertation was submitted to the Kuliyyah of Islamic Revealed Knowledge and Human Sciences and is accepted as fulfilment of the requirement for the degree of Master of Human Sciences (Political Science)

……..……..
Ibrahim Mohamed Zein
Dean, Kuliyyah of Islamic Revealed Knowledge and Human Sciences

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Ainaa Nadzirah Binti Malek Farok

Signature……. Date…….……

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

CYBERSPACE AS A NATIONAL SECURITY ISSUE IN MALAYSIA

Affirmed by Ainaa Nadzirah binti Malek Farok.

……..…… ……

Signature Date

This Study is Dedicated
To My Wonderful

~Ibu and Baba~

For Constant Doa', Love and Support

ACKNOWLEDGEMENTS

I am grateful to Allah S.W.T. the Most Compassionate, the Most Merciful, whose mercy and blessing have enabled me to complete this study.

A number of people have contributed to the successful completion of my thesis. First and foremost, I would like to thank my supervisor Assoc. Prof. Dr. Ishtiaq Hossain for supporting me with valuable advice and guidance. I appreciate his patience while guiding me in researching and drafting this thesis. My thanks also go to the members of the Department's Post-Graduate and Admission Committee. I am grateful to Assoc Prof Dr. Md. Moniruzzaman for his valuable advice. I am also grateful to Dr. Khairil Izamin, for his comments on my thesis proposal. His comments were very useful in improving the quality of this thesis. I express my sincere thanks to Dr. Tunku Mohar bin Tunku Mokhtar, Head, Department of Political Science, IIUM, for supporting me during the years of my study at the IIUM. Not to forget Sister Huda and Sister Asiah in the department as well as Brother Hashim and Brother Aslam from CPS for their help.

The success of this thesis owes much to the support and encouragement I received from my loving parents, Hj. Malek Farok B. Zainal Abidin and Hjh. Murni Bt Musli. They sacrificed everything to see their daughter complete her Master's programme in Political Science.

Last but not least, I am grateful to my friends Imana, Akmal, Tim, Rena, Aini, Hakimah and Mursyidee for sharing knowledge, and providing me with moral support, and lifetime friendship. Also, I express my gratitude to everyone who has directly and indirectly helped me in completing my thesis.

May Allah bless you all.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF DIAGRAMS

LIST OF ABBREVIATIONS

ABM	Association of Banks in Malaysia
AIBIM	Association of Islamic Banking Institutions Malaysia
APCERT	Asia Pacific Computer Emergency Response Team
ASEAN	Association of South East Asian Nation
BERNAMA	Pertubuhan Berita Nasional Malaysia (Malaysian National News Agency)
BNM	Bank Negara Malaysia (Central Bank of Malaysia)
DoS	Denial-of-service attack
DDoS	Distributed denial of service attacks
CA	Certification Authorities
CCU	Computer Crimes Unit
CNII	Critical National Information Infrastructure
CSIRT	Computer Security Incident Response Team
CERT	Computer Emergency Response Team
GLC	Government-Linked Companies
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information and Communications Technology
IMPACT	International Multilateral Partnership Against Cyber Threats
IPA	Information-technology Promotion Agency
IPR	Intellectual Property Rights
IR	International Relations
ISIS	Institute of Strategic and International Studies
ITU	International Telecommunication Union
ITU-D	Telecommunication Development Sector of the International Telecommunication Union
JARING	Joint Advanced Integrated Networking
MINDEF	Ministry of Defense
MOSTI	Ministry of Science, Technology and Innovation
MCMC	Malaysian Communications And Multimedia Commission
MSC	Multimedia Super Corridor
NATO	North Atlantic Treaty Organization
NCSP	National Cyber Security Policy
OIC	Organisation of the Islamic Conference
SMS	Short Message Service
RMP	Royal Malaysia Police
UKM	Universiti Kebangsaan Malaysia
UN	United Nation
UNDP	United Nations Development Programme

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND TO THE STUDY

Many countries, even developed ones such as the USA, have faced cyber-attacks. The USA, for example, has suffered from a number of cyber-attacks affecting several government-owned websites in 2000. These cyber-attacks were believed to have come from a group known as 'patriot hackers' from China (Klimburg, 2011). In 2007, at the height of Russia-Estonia tensions over the rights of Russians living in Estonia, its banking and financial services were shut down following massive cyber-attacks, allegedly by hackers based in Russia (Wilson, 2009).

It has now been revealed that during NATO's military operations in Libya, President Obama had considered but ultimately rejected the suggestions made by some of his security advisers to launch cyber-attacks on Gaddafi's air defence system. In November 2013, the government of the United Kingdom carried out a simulated "cyber-war" on all of its cyber-based resources including the country's defence, and banking and financial institutions. This was done to test the UK's cyber preparedness. These are just some of the startling new developments underlying the importance of cyberspace in national security affairs.

In November 2010, Wikileaks, a whistle-blower website run by an Australian, Julian Assange, published thousands of secret diplomatic cables between American embassies all over the world and the State Department in Washington. According to Heisbourg (2011), the publication of these sensitive cables had impaired US security interests. Washington and Beijing regularly trade accusations of cyber-attacks on each

other's government installations. In 2012, Iranian nuclear reactors became infected with the Stuxnet worm with Israel allegedly behind the attack. Although Iran seemed to be the main target, according to an American cyber expert, the Stuxnet worm attack also infected computers in other countries (Klimburg, 2011).

Anonymous, a loose international group of cyber-activists, has become infamous for launching cyber-attacks on governments and well-known multinational corporations like Sony, PayPal and Visa. Anonymous carried out 230 attacks between 2011 and 2012 on targets that included information technology/consulting firms, government agencies, and retail and commercial organizations in North America, Europe, Asia and Africa (Hammer and Khalid, 2013: 20-21).

Cyber-security and cyberspace are closely linked as they are both related to the use of the Internet. According to Betz and Stevens (2011: 9), "Cyberspace has come a long way since its birth as a concept in science fiction in the early 1980s. Within three decades it has been defined in military doctrine as a new domain of conflict, while in broader societal terms it has come to be seen as the informational substrate in which whole economic ecosystems and industries grow." Cyberspace is a virtual world, but it provides various useful and important functions for the global audience. Its functions have steadily made it essential as a means of connecting people all over the world within a short time and helping people to manage their daily lives.

In Malaysia, the use of cyberspace is increasing every day in line with technological development. According to CyberSecurity Scenario in Malaysia Mid-Year Review 2012, "at present, Malaysia has about 17.5 million Internet users... Malaysia has also about 30 million mobile phone users, larger than the total population of Malaysia (estimated at 28 million)" (www.cybersecurity.my).

The use of cyberspace makes its users vulnerable to criminal acts that may interfere with and interrupt the activity as reported in *Utusan Malaysia* (July 16, 2011), incidents involving cyber-security increased by 147 per cent within the first half of 2011, compared to the first half of 2010. Therefore, measures are needed to protect Malaysia's cyberspace. Cyber-security cannot be taken for granted as it may be considered one of the new dimensions of national security in the globalised era.

National security is traditionally viewed as protecting a country from external military attacks. Typically, it is achieved through the use of military capability in order to protect a country from perceived threats. In the post-modern age, the threat to national security includes attacks from hackers and terrorists. These threats do not necessarily require the use of military force in order to cause damage. Therefore, a new approach is required to protect the nation. Cyber threats differ from traditional (military) threats, thus it can be classified as non-military or non-traditional threats. The threats that emanate from the use of cyberspace are serious and can endanger the security of any nation.

Malaysia has suffered from a number of cyber-attacks. One such attack took place during its maritime territorial dispute with Indonesia over the Sulawesi Sea in March 2005 when a number of websites in Malaysia were attacked by Indonesian hackers (Shaharudin & Zahri, 2005). There have also been several cases of hacking of on-line personal bank accounts of people living in Malaysia. These cases underline the importance of providing cyberspace security in Malaysia.

1.2 STATEMENT OF THE PROBLEM

Globalisation has made virtually everything accessible through the Internet. The Internet may even be used to threaten and even launch attacks on the national security

of a country by launching cyber-attacks, among many others, on the military's command and control structure. Therefore, cyberspace should be considered as part of the national security concerns of a state. Ironically, developments in information technology, both at the hardware and software levels, have led to even greater chances of cyber-crimes.

This study will investigate the relationship between Malaysia's national security and cyberspace. The study will examine the nature of threats to cyberspace in the public (governmental) and private sectors (banking and financial institutions) in Malaysia. Furthermore, since the use of the Internet has been widened to the public and private sectors, and with the ease of access to social networking sites; it is necessary to analyse the natures of government policies on cyber-security. Therefore, this study will look at the responses taken by the Malaysian government in order to protect its cyberspace.

1.3 SIGNIFICANCE OF THE STUDY

There are three primary justifications for this research. Firstly, many studies have treated cyber-security as a national security concern. However, few studies have been able to link cyberspace to Malaysia's national security.

Secondly, government agencies and the banking and financial sectors face the greatest threat in the cyberspace. Previous studies, however, were limited to the different types of threats and did not focus specifically on the relationship between cyberspace and Malaysia's national security.

Finally, the study will analyse the Malaysian government's policies to deal with threats to cyberspace and the protection of Malaysian cyberspace users.

Additionally, this study would recommend some measures and global best practices to deal with cyber threats in the country.

1.4 RESEARCH OBJECTIVES

The objectives of this study are to:

1. Explain the views of government and private agencies in Malaysia about the relationship between cyberspace and national security of the country.
2. Examine the nature of threats to cyberspace in the public and private sectors in Malaysia, especially the banking and financial sectors, and government agencies.
3. Analyse the policies adopted by the Malaysian government to overcome the threats to cyberspace.

1.5 RESEARCH QUESTIONS

Based on the research objectives, this study attempts to answer the following questions:

1. How does Malaysian government and private agencies view the relationship between cyberspace and national security of Malaysia?
2. What is the nature of threats to cyberspace in the public and private sectors of Malaysia, especially in banking, financial and government agencies?
3. What are the policies adopted by the Malaysian government to deal with threats to cyberspace in the country?

1.6 LITERATURE REVIEW

For convenience, this literature review is divided into the following sections: cyberspace and cyber-security, and Malaysia's cyber-security and other related issues.

i. Cyberspace and Cyber-Security

Cyber-security is one of the prevention tools available when exploring cyberspace. Many authors like Hitchcock (2002) believe that the term cyberspace was introduced through a novel by William Gibson in which he refers to the existence of the Internet or World Wide Web. Deibert and Rohozinski (2010) assert that cyberspace emanated from the globalisation process, where its function was shaped by governments, civil society and individual actions.

Goodman (2010) agrees with Deibert and Rohozinski (2010), who believe that the Internet is a part of cyberspace. Goodman claims that the Internet was developed through telecommunication services at the national and international levels, which to a large extent, is widely dependent on the use of computer technology. However, Goodman's claims that "globalization has meant that the Internet is now less secure, with vulnerabilities resulting from new systems 'intimacies'" (2010: 26) is in direct contradiction to the points of views of Deibert and Rohozinski on Internet security as mentioned earlier.

Smith and Rupp (2002) also argue that "Internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts in a variety of ways, including gateways, routers, dial-up connections, and Internet services providers" (p.178). This means that the access to cyberspace and the use of the Internet is open worldwide. Therefore, any information shared can easily be accessed by anyone through cyberspace.

Cyberspace has been used and misused for various purposes from the very inception of the Internet. It should also be mentioned here that the user-friendly nature of the Internet has contributed to its misuse by criminals. The abuse of the technology has created other problems such as hacking, cyber-crime, money laundering, and threats to individuals and society.

The misuse of cyberspace has become one of the biggest threats to countries, since it can be considered to be an unseen enemy. In addition, it is also difficult to detect the real culprits behind these threats. As a result, cyberspace can be regarded as a new territory for war when its use threatens national security.

Cyber-security has been developed as a counter-measure against threats from cyberspace which may harm individuals, groups, organisations or governments. The development of cyber-security helps to protect confidential information from attacks. However, the threats to cyber-security continue to emerge and evolve daily.

As has been pointed out earlier, various threats to cyberspace threaten national sovereignty, and therefore, the national security of a state. However, as pointed out so aptly by Weaver; whether something is a threat or not, is ultimately decided by the elites of a state (Weaver, 2011: 95). In other words, anything can be considered national security threats so long as the elites of a state consider them as such. Therefore, in order to contain or prevent these threats, these must be considered as national security issues. Thus, cyber-security is considered to be part and parcel of national security.

Recognising the importance of this issue, countries like the US placed cyber-security under the control of institutions such as the Cyber Command headed by a three-star general. However, in Malaysia, unlike the US, the responsibility of providing cyber-security is in the hands of Ministry of Science and Technology and

Innovation (MOSTI). As a result, any threats to cyber-security are first reported to MOSTI. Only then MOSTI would report such threats to the concerned agencies, such as the police and other security agencies.

The practice of cyber-security is not just limited to the use of antivirus software, firewalls, and Internet security programmes; it covers a wide scope with regards to cyberspace, especially the protection of government's information and data. Lukasik, Goodman and Longhurst (2003) have suggested some strategic options as a preventive measure for cyber-attacks such as deterring an attacker, establishing standards of behaviour, and pre-empting an attacker. However, it depends on the ability of the government to implement such laws.

As cyber-security has existed in response to cyber threats, it is important to know why the threats still exist. Cavelty (2008) argues that, in the case of the US, "One of the main reasons why the issue of cyber threats has gained so much attention in recent years is the fact that in the process of threat politics, US officials have convincingly argued that they threatened the very fabric of modern societies" (p.138). It clearly demonstrates that even in an advanced country such as the US, cyber-security threats have become a major concern.

ii. Malaysia's Cyber-Security and Its Related Issues

Malaysia faced various traditional and non-traditional security challenges before independence. In the 1940s, the Japanese occupation during World War II was an example of traditional security threats faced by the government of the time. Later, the communist insurgency in the 1960s, which according to Ruhanas (2009) re-appeared in the 1970s, was another traditional security threat. In 1963, Malaysia faced another problem when Indonesia, under the Sukarno administration, launched the policy of

Konfrantasi (Confrontation) against Malaysia as a reaction to the formation of the federation of Malaysia (before that, Malaysia was known as *Malaya*) (Jastwan, 2009).

Ruhanas (2009) identifies the non-traditional security concerns in Malaysia after the Cold War as domestic security concerns. One such threat is the presence of immigrants, both legal and illegal. The presence of immigrants can be considered as part of the effects of globalisation faced by every developing country. However, the revolution in technology has accelerated globalisation and inadvertently contributed to the spiralling of cyber-security threats.

The Ernst & Young Globalisation Index ranked Malaysia 28th among the top 30 Asian countries in 2011 (Bhar, 2012). However, the *Globalization Index 2007,* published by *Foreign Policy* magazine (October, 2007) ranked Malaysia 20th among Internet users in the world and 41st based on the number of Internet hosts. Interestingly, the same index ranked Malaysia 35th out of 72 countries for secure servers behind Singapore (20th) but ahead of other Southeast Asian countries like Indonesia (50th), Philippines (42nd), Thailand (39th), and Vietnam (63rd). Though Malaysia has not attained the level of advanced countries like the US, the index shows that Malaysia is trying to improve its cyber-security in the globalised era.

There is a dearth of academic works specifically focusing on cyber-security and national security in Malaysia. Therefore, this study reviews the literature from a broader perspective focussing not only on Malaysia but also includes China and Singapore. Even then, most of the literature deals with the policy of regulations of the Internet. According to Xue (2005), the regulations of the Internet in China, Singapore and Malaysia are based on the "political regimes and existing regulatory practices" (p.239). She found the regulations in those three countries as "…fragmented and

controlled (China), somewhat integrated and more open (Malaysia), and integrated and controlled/open (Singapore)" (p. 239).

According to Xue (2005), even though the Internet in China has a significant role to play in the national economy; the government seems more concerned with spurious content of the Internet. She is also of the opinion that the Chinese government considers the freedom to access and publish political opinions and materials on the Internet as serious threats to China's political and social values (p. 241). In other words, the government in China considers the daily usage of the Internet by its people as possible challenges to its rule. As a result, while the state authorities in China are involved in improving the communications infrastructure, at the same time, they have also demonstrated an equal determination to control the content available on the Internet (Xue, 2005).

Most of the issues related to cyberspace in China are concerned with censorship. This is partly due to the State's concerns with opposition to its rule. But it is also partly due to Beijing's obsession with national security issues. It may be mentioned here that China is concerned with the situation in Xinjiang, an Autonomous Region, populated by Muslim Uighurs. Unhappy with the existing political, economic and religious conditions in Xinjiang, sections of the Uighurs are engaged in a violent movement to seek independence from Beijing.

Overseas Uighurs groups are well-organised and they extensively use the Internet to spread their grievances against Beijing. The Chinese government is bent on stopping the Uighurs from accessing the Internet, thus it makes sense to be concerned with the use of cyberspace. Just as the US and other Western countries complain about China-based cyber-attacks on their military and economic infrastructures, Beijing also