CYBER TERRORISM: THE RISING THREAT IN CYBER DIMENSION?

Commonwealth Cybersecurity Forum 2014
London
5 – 6 March 2014

Zahri Yunos
Chief Operating Officer
CyberSecurity Malaysia
CRITICAL NATIONAL INFORMATION INFRASTRUCTURE (CNII)
**Critical National Information Infrastructure (CNII) In Malaysia**

**VISION**

‘Malaysia’s Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well being and wealth creation’

### CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Assets (real & virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on

- National defense & security
- National economic strength
- National image
- Government capability to function
- Public health & safety

<table>
<thead>
<tr>
<th>Category</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFENCE &amp; SECURITY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TRANSPORTATION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BANKING &amp; FINANCE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HEALTH SERVICES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMERGENCY SERVICES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENERGY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFORMATION &amp; COMMUNICATIONS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GOVERNMENT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOOD &amp; AGRICULTURE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WATER</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Inter-Dependent
Interdependency of CNII

Threats to CNII: Interdependency

The high degree of interdependency between critical infrastructure sectors means failures in one sector can propagate into others.
Threats to CNII: SCADA Systems

The interconnection of SCADA systems to corporate networks & their reliance on common operating platforms and remote excess - exposing SCADA systems to vulnerabilities

Threats to CNII: The Use of ICT and Cyberspace by Terrorist

Psychological Warfare
Planning and Coordination
Publicity and Propaganda
Use of Internet By Terrorist
Data Mining
Sharing Information
Fundraising
Social Networking
Recruitment and Mobilization

Reference:


The perpetrator may utilize the cyberspace for conducting cyber attacks on critical national information infrastructure facilities.
Why would a perpetrator decide to use ICT instead of using the usual methods of assassination, hostage-taking, guerrilla warfare and bombing?

- Many nations all over the world constantly increase their dependency on cyberspace by maximising the use of ICT.

- Interdependencies that exist within critical infrastructures have raised concerns - successful cyber attacks on one computer system can have serious cascading effects on other, resulting in potentially catastrophic damage and disruption.

- Through ICT, perpetrators can disrupt critical services, hence affecting the nation’s operation and its ability to function.
CYBER TERRORISM
Cyber Attack to CNII - Estonia

Cyber Attack on Estonia
- Occurred in May 2007
- Estonia was under cyber attacks for 3 weeks
- Attack targeted government, banking, media, police websites
- Paralyzed internet communication.
- Attacks from 128 sources outside Estonia
- US and European countries aided Estonia in overcoming the cyber attacks

You don't see buildings reduced to piles of rubble or dead bodies strewn across the street ……
There's nothing to take photos ……
There's only economic damage, websites that cannot be accessed and transactions that cannot be made …..

By destabilizing the country, the people of the country are subject to riots, rallies and protests, and could result in violence and creating unrest in the country.

YB Datuk Seri Dr Ahmad Zahid Hamidi, DSA 2012

Is it cyber terrorism?
Is it cyber crime?
Is it cyber war?
Cyber Attack to CNII – Stuxnet

Stuxnet was targeted at Siemens industrial software and equipment running Microsoft Windows (June 2010). Symantec reported that nearly 60% of the approximately 100,000 infect hosts were located in Iran, which has lead to speculation that Stuxnet's target was Iran's nuclear power plant or uranium enrichment facility.
Cyber Attack to CNII – Shamoon

Is it cyber terrorism?

Is it cyber crime?

Is it cyber war?
OP Malaysia – Cyber Attacks by Anonymous Hackers (15-19 June 2011)

Is it cyber terrorism?

Is it cyber crime?

Is it cyber war?
“Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economics loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.”

Definition: Cyber Terrorism .. many more

• There are many definitions on cyber terrorism provided by researchers, policy makers and individuals

• Interestingly, most governments in the world do not agree on one single definition of cyber terrorism. There is no common definition of cyber terrorism

• The ambiguity in the definition brings indistinctness in action; as the old maxim goes “one man’s terrorist is another man’s freedom fighter” [1].

• According to Schmid, “there is no agreement among experts and there is not likely to be an agreement as long they cannot even agree on a common definition on terrorism (and cyber terrorism).“ [2]

Reference:
Cyber Terrorism Framework: Veerasamy

Provide context in which cyber terrorism is functioning

Methods of carrying cyber terrorism

Motivation

Cyber Terrorism Framework: Heickero

# Cyber Terrorism Framework: Gordon and Ford

<table>
<thead>
<tr>
<th>Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Perpetrator</strong></td>
<td>Group/Individual In cyber context, virtual interactions can lead to anonymity.</td>
</tr>
<tr>
<td><strong>Place</strong></td>
<td>Worldwide The event does not have to occur in a particular location. The Internet has introduced globalization of the environment.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Threats/Violence/Recruitment/Education/Strategies Terrorist scenarios typically are violent or involve threats of violence. Violence in virtual environment includes psychological effects, possible behavior modification and physical trauma.</td>
</tr>
<tr>
<td><strong>Tool</strong></td>
<td>Kidnapping/ Harassment/Propaganda/Education Terrorist use the computer as tool. Facilitating identity theft, computer viruses, hacking are examples fall under this category.</td>
</tr>
<tr>
<td><strong>Target</strong></td>
<td>Government Officials/Corporations Potential targets are corporations and government computer systems.</td>
</tr>
<tr>
<td><strong>Affiliation</strong></td>
<td>Actual/Claimed Affiliation refers to recruitment in carrying out given instructions. Affiliation can result in strengthening of the individual organizations as they can immediately acquire access to the information resources of their allies.</td>
</tr>
<tr>
<td><strong>Motivation</strong></td>
<td>Social/Political Change Political, social and economic are the motivations present in the real-world terrorism.</td>
</tr>
</tbody>
</table>

Cyber Terrorism Framework: Brickey

Cyber Terrorism Framework: Yunos & Ahmad

- Critical National Information Infrastructure computer system
- Critical Infrastructure
- Civilian population
- Political
- Ideological
- Social
- Economic
- Network warfare
- Psychological operation
- Cyberspace (includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers)
- Borderless

Target

Motivation

Impact

Method of Action

Tools of Attack

Domain

Factor ‘AND’

- Mass disruption or seriously interfere critical services operation
- Cause fear, death or bodily injury
- Severe economic loss
- Unlawful means
- Illegal acts

Extended CERT-taxonomy from Howard and Longstaff (1998)

Initiatives in Safeguarding Malaysia CNII Against Cyber Threats
Topping the list of possible perpetrator abuse of the ICT and cyberspace is the potential for actual attacks on the network itself, or “cyber terrorism”

Terrorist cyber-attack on critical information infrastructure is possible, where motivation and resources are fundamental

Therefore, there is a need to have a strategy at the national level for the protection of the CNII against cyber terrorism

The strategy for the CNII protection could be through industry cooperation and information sharing, awareness and education program, adequate laws related to infrastructure protection, R&D program and organizational structure
The National Cyber Security Policy
- Background and Objectives

Objectives:

- Address The Risks To The Critical National Information Infrastructure (CNII)
- To Ensure That Critical Infrastructure Are Protected To A Level That Is Commensurate With The Risks
- To Develop And Establish A Comprehensive Program And A Series Of Frameworks

The policy recognizes the critical and highly interdependent nature of the CNII and aims to develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of cyber security controls over vital assets.
The National Cyber Security Policy - Policy Thrust

1. EFFECTIVE GOVERNANCE
   National Security Council

2. LEGISLATION & REGULATORY FRAMEWORK
   Attorney General’s Chambers

3. CYBER SECURITY TECHNOLOGY FRAMEWORK
   Ministry of Science, Technology & Innovation

4. CULTURE OF SECURITY & CAPACITY BUILDING
   Ministry of Science, Technology & Innovation

5. R & D TOWARDS SELF RELIANCE
   Ministry of Science, Technology & Innovation

6. COMPLIANCE & ENFORCEMENT
   Ministry of Communication & Multimedia

7. CYBER SECURITY EMERGENCY READINESS
   National Security Council

8. INTERNATIONAL COOPERATION
   Ministry of Communication & Multimedia

‘Malaysia’s Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well being and wealth creation.
The National Cyber Security Policy - Current Progress

PT 1
EFFECTIVE GOVERNANCE

PT 2
LEGISLATION & REGULATORY FRAMEWORK

A STUDY ON THE LAWS OF MALAYSIA TO ACCOMMODATE THE LEGAL CHALLENGES IN THE CYBER ENVIRONMENT

PT 3
CYBER SECURITY TECHNOLOGY FRAMEWORK

NATIONAL STRATEGY FOR CYBER SECURITY ACCULTURATION AND CAPACITY BUILDING PROGRAM

PT 4
CULTURE OF SECURITY & CAPACITY BUILDING

PT 7
CYBER SECURITY EMERGENCY READINESS
Public-private partnership is essential in order to enhance the security of Malaysia’s cyber space – Government led and supported by the industries, academia and NGOs.
A **framework** that outlines the **strategy** for cyber attacks mitigation and response among Malaysia’s Critical National Information Infrastructure (CNII) through **public and private collaboration and coordination**.
ENGAGE

Participate in relevant cyber security meetings and events to promote Malaysia’s positions and interests in the said meetings and events.

PRIORITIZE

Evaluate Malaysia’s interests at international cyber security platforms and act on elements where Malaysia can get tangible benefits and voice third world interests.

LEADERSHIP

Explore opportunities at international cyber security platforms where Malaysia can vie for positions to play a leadership role to project Malaysia’s image and promote Malaysia’s interests.

OIC-CERT
Cyber security partnerships to strengthen self-reliant in the cyberspace.

ASEAN Regional Forum

APCERT
Asia Pacific Computer Emergency Response Team

APEC TEL WORKING GROUP
Asia-Pacific Economic Cooperation Telecommunications & Information Working Group
PT8: INTERNATIONAL COOPERATION
APCERT DRILL 2012, 2013 & 2014

Source: Secretariat, APCERT / JPCERT-CC
Conclusion

• Cyber world offers great opportunity, but the emergence of cyber threats brought together a number of repercussions that should not be taken for granted

• Hence it is important to address these threats in a comprehensive manner. These include:
  ✓ To have an integrated policy framework
  ✓ To enhance the use of technology and process to mitigate the threats
  ✓ To inculcate a cyber security acculturation through continuous training and awareness programs

• Public-Private Partnership is essential to enhance the security and safety of cyber space
Thank you

Corporate Office
CyberSecurity Malaysia,
Level 8, Block A,
Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.

T : +603 8946 0999
F : +603 8946 0888
H : +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my

www.facebook.com/CyberSecurityMalaysia
www.twitter.com/cybersecuritymy
www.youtube.com/cybersecuritymy

Best Brand
Mega Security
ISMS
STANDARDS
MSC
Status Company