SECURING OUR DIGITAL CITY: 
THE WAY FORWARD

PROFESSOR ABU BAKAR MUNIR 
FACULTY OF LAW 
UNIVERSITY OF MALAYA 
&
ASSOCIATE PROFESSOR SITI HAJAR MOHD YASIN 
FACULTY OF LAW 
UNIVERSITI TEKNOLOGI MARA

CSM-ACE 2010 
KUALA LUMPUR CONVENTION CENTRE
26-27 OCTOBER 2010
Cybercrime

- Cybercrime Convention
- Council of Europe Framework Decision 2005/222/JHA
- Computer Crimes Legislation
Cyber terrorism

- International Criminal Laws
- UN Conventions on Terrorism
- UN International Convention for the Suppression of Terrorist Bombings
- International Convention for the Suppression of Acts of Nuclear Terrorism
- International Convention for the Suppression of Unlawful Acts Against Safety of Civil Aviation
cont...

- European Convention on the Suppression of Terrorism
- E.U Framework Decision on Combating Terrorism (2002/475/JHA)
- E.U Data Retention Directive
- Countries’ Anti-Terrorism Legislation
- Countries’ Criminal Law
How about Cyberwar?
Is there any Legal and Policy Instrument?
Is Cyber War Real?

“The next world war could happen in cyberspace and that would be a catastrophe... there is no such thing as a superpower.”

ITU (2009)

“Not only will cyber war be a force in future warfare, it may also turn out to be the great equalizer for nations.”

United Nations Institute of Research and Training (UNITAR)
“The overall international security landscape has become more complex and unpredictable... over the longer term we cannot rule out a possible re-emergence of a major state-led threat to the United Kingdom. That could come about through... or other forms of threat, which render distance irrelevant, for example state-sponsored cyber-attack.”

2008 UK Cabinet Office Report

“In summary, our warfare methods must adapt to the needs of information warfare”

Former Chinese General
When would a cyber attack amount to a cyber war?

Can a cyber war be regarded as a war?

Can the laws of war be applied to cyber war?
Questions arise out of attacks on Estonia

- Does the attack warrant a reaction from NATO? (North Atlantic Treaty Organization)
- Can Article 5 of NATO be invoked?
- Article 5 – An assault on one allied country obligates alliance to attack the aggressor.
- How about the United Nations?
Challenges to the International Law

- The types of damage are different from the kind of physical damage caused by the traditional warfare.

- Sovereignty of states is disrupted by the ability of technology to cross borders without hindrances.

- Harder to define the targets of cyber war as either military or civilian.
US Current Thinking

- Preemptive cyber strike?
Pentagon is contemplating an aggressive approach to defending its computer systems that includes preemptive actions/preemptive strikes.

“We have to have offensive capabilities, to, in real time, shoot down somebody trying to attack us.”

General Keith Alexander
Pentagon Cyber Command
(July 2010)
Would this be done without violating international law or other countries’ sovereignty?
Lessons from Cyber-Storm II

- Cyber Storm I: February 2006
- Cyber Storm II: March 2008, US + 4 countries (Australia, Canada, N.Z & UK)
- Cyber Storm III: September 2010, US +12 countries

Cybersecurity exercises involving several departments of the US Govt and foreign countries like Australia, Canada, France, Germany, Hungary, Japan, Italy, the Netherlands, New Zealand, Sweden, Switzerland and the UK.

The report is not out yet
Findings of Cyber Storm II

• Effective response is enhanced by routinely reviewing and testing the Standard Operation Procedures (SOPs), Incidents Response Plans and/or crisis management arrangements.

• Non-crisis interaction among key stakeholders enhances effective crisis response during an incident.

• Crisis communication procedures, predicated on accurate and appropriate points of contact, must be formalized within contingency planning.
Cyber crisis require a tailored response that takes into account multiple interdependencies.

Developing internal reporting and external notification thresholds assists in effective incident response by creating better situated awareness.
The United Nations systems should have the leading role in inter-governmental activities for the functioning and protection of cyberspace.

Cybercrime, cyberterrorism and cyber war activities should be dealt with by the competent organ by the UN systems under the international law.

Nationally and internationally, an educational framework for promoting awareness should be developed for the public.
International law enforcement organization, such as the Interpol and Europol, should assume a stronger role in the international promotion of cyber crime issue.

International cooperation in the areas of legal aspects, technical measures, organizational structures and capacity building is very crucial.