Cyber Security and International Relations

Some Definitions

According to the U.S. Dept of Commerce:

n. **cybersecurity**: “information security”

n. **information security**: The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

Some Definitions

“Cyber Security Information Act” According to H.R. 4246 (US Cyber Security)

> **cybersecurity**: “The vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the United States, or that threatens public health or safety.”

One way to think about it !

cybersecurity = security of cyberspace

information systems and networks

availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

Cyber Security

- Cyber adalah awalan yang mengacu pada teknologi berbasis elektronik dan komputer. Cyber-Security didefinisikan oleh (*International Tellecomunication Union*) yaitu sekumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan maya, organisasi dan aset pengguna (*user*).

- Joseph Nye dalam tulisannya yang berjudul *Cyber Power*, *Cyber security* dihadapkan kepada empat ancaman utama yaitu, spionase, kejahatan, perang cyber dan terorisme cyber. Kemungkinan ancaman ini di tentukan oleh tiga faktor yaitu kelemahan dalam desain internet, kelemahan dalam perangkat keras dan lunak serta langkah dalam penempatan sistem yang disebutnya "*more critical*" dalam dunia maya/virtual.

Why are we talking about cybersecurity?

Cyber Security : Case Phenomenon

- **February 7 - 9, 2000**
  Yahoo!, Amazon, Buy.com, CNN.com, eBay, E*Trade, ZDNet websites hit with massive DOS
- Attacks received the attention of president Clinton and Attorney General Janet Reno.
- **“A 15-year-old kid could launch these attacks, it doesn’t take a great deal of sophistication to do”**
  – Ron Dick, Director NIPC, February 9
- U.S. Federal Bureau of Investigation (FBI) officials have estimated the attacks caused $1.7 billion in damage

Slammer Worm

- **January 2003**
  Infects 90% of vulnerable computers within 10 minutes
- **Effect of the Worm**
  - Interference with elections
  - Cancelled airline flights
  - 911 emergency systems affected in Seattle
  - 13,000 Bank of America ATMs failed
- **Estimated ~$1 Billion in productivity loss**

- In August 2012, hackers attacked the networks of Saudi Aramco, destroying data on some 30,000 of the company’s computers.
- Then in November, Chevron revealed that it had been infected by Stuxnet, the malware the United States and Israel had allegedly designed to slow Iran’s nuclear program. Some U.S. policymakers and analysts have suggested that the attacks originated in Iran as retribution for the sabotage campaign. Those who claimed responsibility said that they are a hacking collective, with no ties to Iran, angry about an anti-Islam film posted on YouTube

Increasing Dependence

We are increasingly dependent on the Internet:

Directly

- **Communication (Email, IM, VoIP)**
- **Commerce (business, banking, e-commerce, etc)**
- **Control systems (public utilities, etc)**
- **Information and entertainment**
- **Sensitive data stored on the Internet**

Indirectly

- **Biz, Edu, Gov have *permanently* replaced physical/manual processes with Internet-based processes**

Cybersecurity Roadblocks

- **No metrics to measure (in)security**
- **Internet is inherently international**
- **Private sector owns most of the infrastructure**
- **“Cybersecurity Gap”: a cost/incentive disconnect?**
  - Businesses will pay to meet business imperatives
  - Who’s going to pay to meet national security imperatives?

This level of dependence makes the Internet a target for **asymmetric attack** and a weak spot for **accidents and failures**

A solution to this problem will require both the right **technology** and the right **public policy**.

This is the cybersecurity challenge.

Cybersecurity Questions

- How vulnerable is state to a cyberattack? Are we heading for an “electronic pearl harbor”?
- What areas of vulnerability require the greatest attention in order to improve our national cybersecurity?
- With what parties must the government work in order to make significant cybersecurity improvements?
- Are market forces sufficient to provide national cybersecurity? Should the government get involved to change these forces, and if so, how?