



Cyber Security in Asia



“There is a pressing need to contain cyber-crime through international cooperation. Without effective...control it is impossible to develop a networked society that is secure, convenient and comfortable.” [*Japan Times*, 2004]

“The internet is fast, whereas criminal law systems are slow and formal. The internet offers anonymity, whereas criminal law systems require identification of perpetrators...The internet is global, whereas criminal law systems are generally limited to a specific territory. Effective prosecution with national remedies is all but impossible in a global space.” [Sieber, 2004]

National Strategy to Secure Cyberspace

‘Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation’s critical infrastructures, economy, or national security...Because of the increasing sophistication of computer attack tools, an increasing number of actors are capable of launching nationally significant assaults against our infrastructures and cyberspace.’

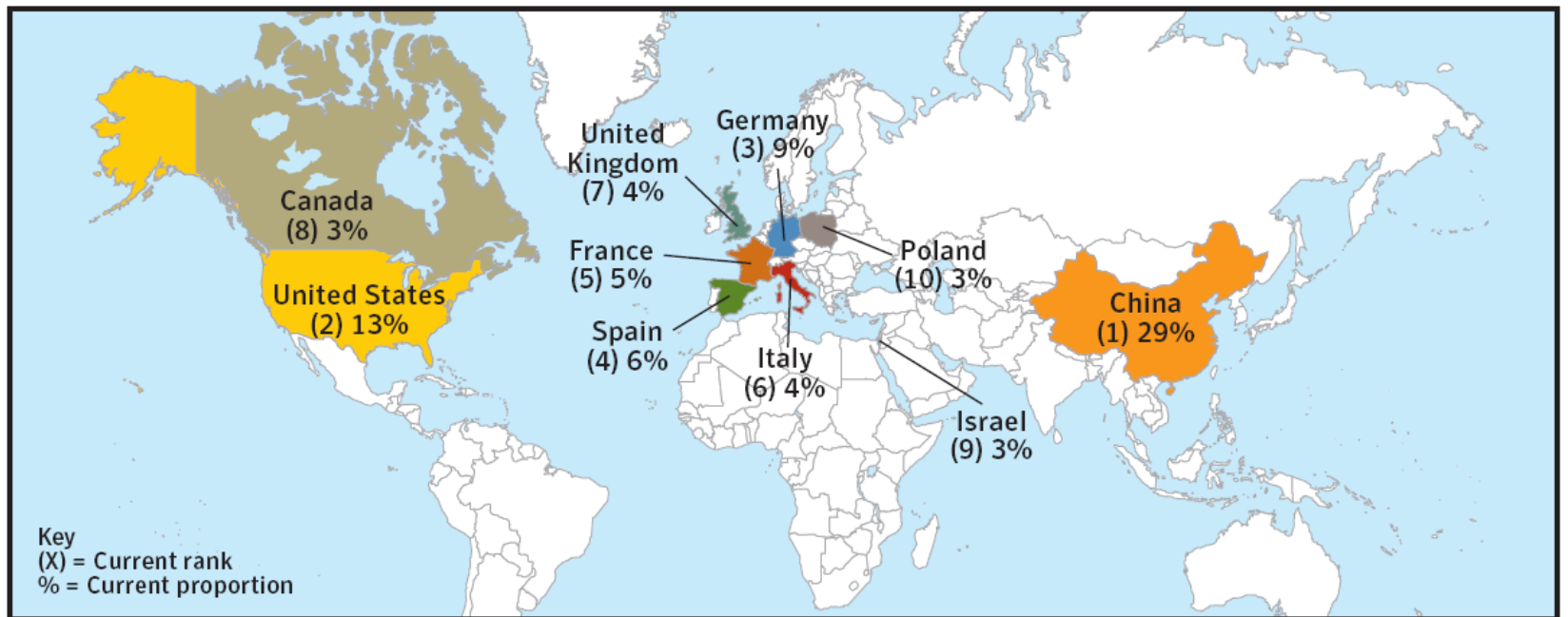
Threat Potential

- Japanese cybercrimes: 2081 in 2003, 2200 in 2004, 3061 in 2005
- ROK – 121 in 1997, 60000 in 2002, 70545 in 2006
- Typologies: phishing scams, which use phone web sites to steal credit card numbers and perpetrate identity theft; fraudulent spam that launches viruses or spyware; and “malware” such as Trojans.
- For the first half of 2007, China accounted for 29 percent of all global bot attacks



Examples of Typologies (II)

- 'Phishing' scams
- Worms
- Identity theft
- Viruses or spyware delivered by spam
- 'Malware'



Real World Divides

Table 1: Socio-economic Indicators in East Asian States

Country	GDP per capita (US)	Adult Illiteracy rates, 15 yrs and over (% of population)	Children underweight for age (% ages 0-5) 2004	Human Development Index ranking	Political Freedoms/ Civil Liberties	Life expectancy at birth (F/M)
Brunei	\$28,161	7.3%	----	30	6/5	79/75
Cambodia	\$2,727	26.4%	45%	131	6/5	61/64
China	\$6,757	9.1%	8%	81	7/6	74/70
Indonesia	\$3,843	9.6%	28%	107	2/3	70/66
Japan	\$31,267	1%	----	8	1/2	85/78
ROK	\$22,029	1%	----	26	1/2	81/74
Laos	\$2,039	31.3%	40%	130	7/6	57/54
Malaysia	\$10,882	11.3%	11%	63	4/4	76/71
Myanmar	\$1,027	10.1%	32%	132	7/7	64/58
Philippines	\$5,137	7.4%	28%	90	4/3	73/69
Singapore	\$29,663	7.5%	3%	25	5/4	82/78
Thailand	\$8,677	7.4%	18%	78	6/4	74/68
Vietnam	\$3,071	9.7%	27%	105	7/5	73/68

Digital Divides

- Japan, South Korea and Singapore
- China, Indonesia, Malaysia, the Philippines and Thailand
- Brunei, Cambodia, Laos, Myanmar or Vietnam
- Globally even more divides when considering the capacities in North America and Europe



Domestic responses and issues

- Different countries face different challenges in securing cyberspace
- In Japan or South Korea, connections to the web are commonplace vs Laos or Vietnam where the presence of the Internet is very restricted.
- The differences in Internet connectivity have a direct correlation with a state's economic modernisation as well as with its integration with global processes of development.

Table 2: Internet Penetration and Usage in Asia

Country	Population (2007 Est.)	Internet Users (Year 2000)	Internet Users, Latest Data	Penetration % Population	% Users in Asia	Use Growth 2000-2007
Brunei	374,577	30,000	176,029	47.0 %	0.0 %	486.8 %
Cambodia	13,995,904	6,000	44,000	0.3 %	0.0 %	633.3 %
China	1,321,851,888	22,500,000	210,000,000	15.9 %	41.1 %	833.3 %
Indonesia	234,693,997	2,000,000	20,000,000	8.5 %	4.3 %	900.0 %
Japan	127,433,494	47,080,000	87,540,000	68.7 %	19.0 %	85.9 %
ROK	49,044,790	19,040,000	34,910,000	71.2 %	6.8 %	83.4 %
Laos	6,521,998	6,000	25,000	0.4 %	0.0 %	316.7 %
Malaysia	24,821,286	3,700,000	14,904,000	60.0 %	3.2 %	302.8 %
Myanmar	47,373,470	1,000	300,000	0.6 %	0.1 %	29,900.0 %
Philippines	91,077,287	2,000,000	14,000,000	15.4 %	3.0 %	600.0 %
Singapore	4,553,009	1,200,000	2,421,800	53.2 %	0.5 %	101.8 %
Thailand	65,068,149	2,300,000	8,465,800	13.0 %	1.8 %	268.1 %
Vietnam	85,262,356	200,000	18,226,701	21.4 %	3.6 %	9,013.4 %

Domestic (II)

- Political systems shape threat typologies, eg. the threat deemed to be posed by certain types of online materials.
- Some governments restrict information (ie a threat) while others adopt a more open-ended response (ie not a threat).
- Role of local culture is very important, eg. web-based pornography in Japan or online speech in Singapore

Regional Responses

- “Regional initiatives have two main advantages because they are pursued within an environment where there are ‘fewer’ cultural differences and ‘fewer’ problems of compatibility in judicial systems and can focus on specific problems that often complement other political and economic joint efforts. In addition to historical and geographical homogeneity and contiguity, the differences in political and economic development in a particular region may not be too dramatic as to create mutual suspicion, and even where this exists, they can be counterbalanced by other cohesive factors.” [Shehu, 2001]

Regional

- Regional responses shaped by existing security architecture
- Economic development of the countries seen as a critical issue in addressing cyber insecurities
- Post 9/11 more focus on cyber threats

“As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all.” UN GA 57/239

Regional Organisations' Responses

- ASEAN: First, there has been a generalized attempt to improve regional capacity and resources through the e-ASEAN process. Second, there has been a set of more explicit attempts to secure cyberspace from transnational subversion of national security; especially those stemming from the activities of criminal and terrorist organizations.
- APEC has taken a different approach, with cyber issues being mainly dealt with under the telecommunications area.

ASEAN

- e-ASEAN Initiative began in 1999 to collectively explore methods by which the lesser-developed Southeast Asian states could overcome the digital divide.
- ASEAN has sought to deepen regional cyber linkages and capacity it has also engaged China, Japan and South Korea (under ASEAN+1 and +3) in the formation of new ICT networks.
- Cyber security issues have also been pursued with e-development programs, such as the formation of CERTs.

APEC

- APEC's responses to cyber issues and threats have focused on issues such as e-commerce, identity theft, and related developments, before shifting in the late 1990s to focus on the criminal aspects of cyberspace (particularly information security), and then post 9/11 to focus on cyber terrorism.
- Begun to study ways to develop a cyber crime investigation agency between its member economies.
- Since January 2003 working with the OECD in developing guidelines to enhance cyber security.
- More proactive than ASEAN in engaging with the business sector and, more recently, civil society organizations

International- EU (I)

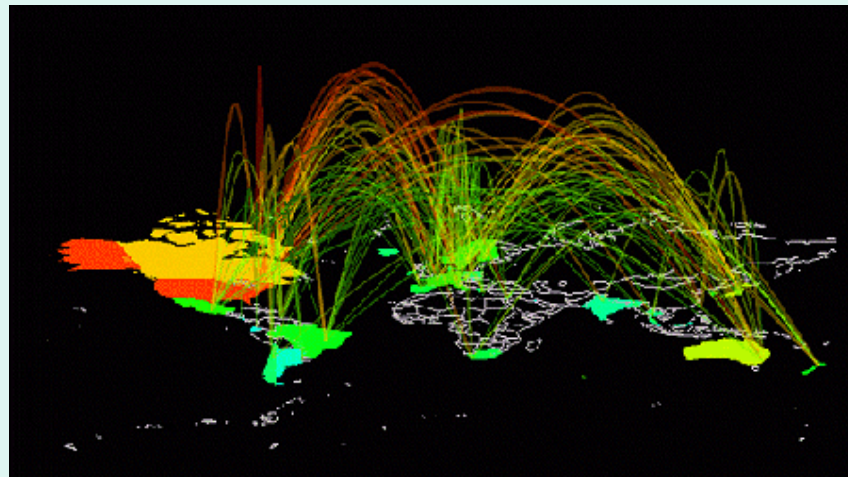
- 1989 - the European Committee on Crime Problems issued a report recommending member states develop criminal legislation in respect to certain actions undertaken via a computer network
- 1995 - the CoE issued a report that further reviewed the progress by member states in developing criminal law connected with information technology.
- 1997 an expert committee on crime in cyberspace was established by the Council of Ministers “to prepare a “legally binding instrument”, which in CoE terms, means an international treaty.

International- EU (II)

- The 2001 European Convention on Cyber-Crime (also referred to as the Budapest Convention), is considered a landmark treaty addressing cyber security matters at the domestic and regional level.
- The Convention also goes further than the CERT idea, with ratifying states committed to providing national contact points for cyber offences “24/7”; in other words, 24 hours a day, 7 days a week. The 24/7 network personnel – based on pre-existing (but more limited) G8 network – not only provides technical assistance but may also directly participate in the investigation.
- In April 2007, for example, the CoE presented the Convention to a joint APEC/ASEAN meeting on cybercrime, which led to cooperation between the CoE and the Philippines as well as a later request for accession from that state.
- In November 2007, the CoE made a similar presentation in the Gulf, which led to the *Cairo Declaration Against Cybercrime* being promulgated, information-sharing between the Gulf States and the CoE as well as new legislated initiatives against cybercrime.

Conclusion (I)

- Cyberspace is the critical medium through which most of the world operates.
- Increased connectivity has meant increased openness to a new generation of threats hitherto unexperienced by states, markets or societies.



Conclusion (II)

- Three key conclusions:
 - (1) the notion that the speech act by a securitizing actor to a target audience represents an act of securitisation is too limited.
 - (2) when states address the challenges presented by cyber threats it is necessary for them to take into account the actions of other states as well as organizations operating in the international arena
 - (3) If threats can emerge from any level of a nation-state then those levels need to be included in the response strategies