Fighting Cybercrime: The Role of Capacity Building - The Policy of Japan -

24 March, 2014

Akino Kowashi

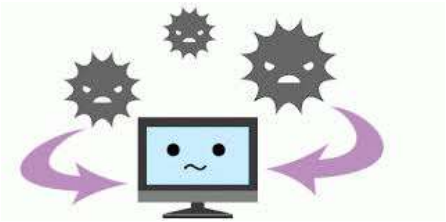
International Safety and Security Cooperation Division

Foreign Policy Bureau, Ministry of Foreign Affairs, Japan

Japan acceded to the Budapest Convention in July 2012 as the first Party from the Asian region

- Total number of Parties = 42 countries (as of March 2014)
  - 36 European + Australia, the Dominican Republic, Japan, Mauritius, Panama and the USA

1. Cybercrime in Japan

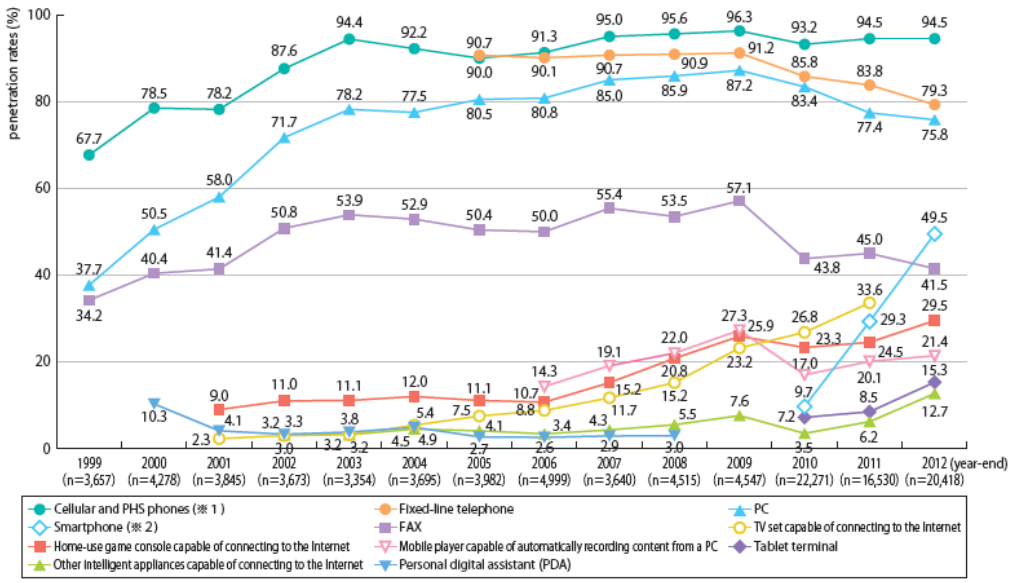


Status of ICT Penetration in Japan

At the end of 2012:

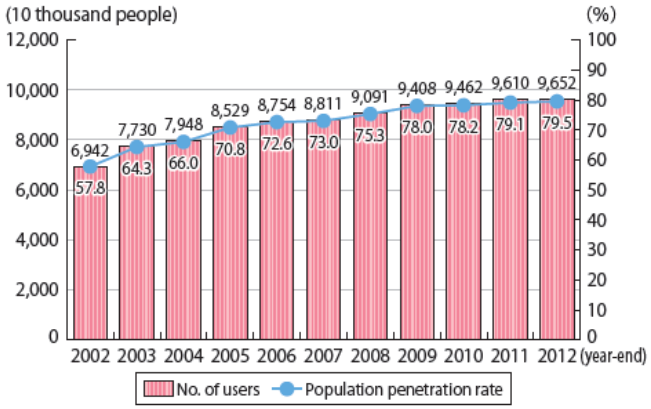
- Holders with cellular phones and PHS = 94.5%
- Households with personal computers = 75.8%
- Internet users = 79.5% of population
  - = 4th in the world (by # of internet users)
  - = 33rd in the world (by penetration rate)

Figure 4-3-1-1 Transitions in household penetration rates for ICT terminals



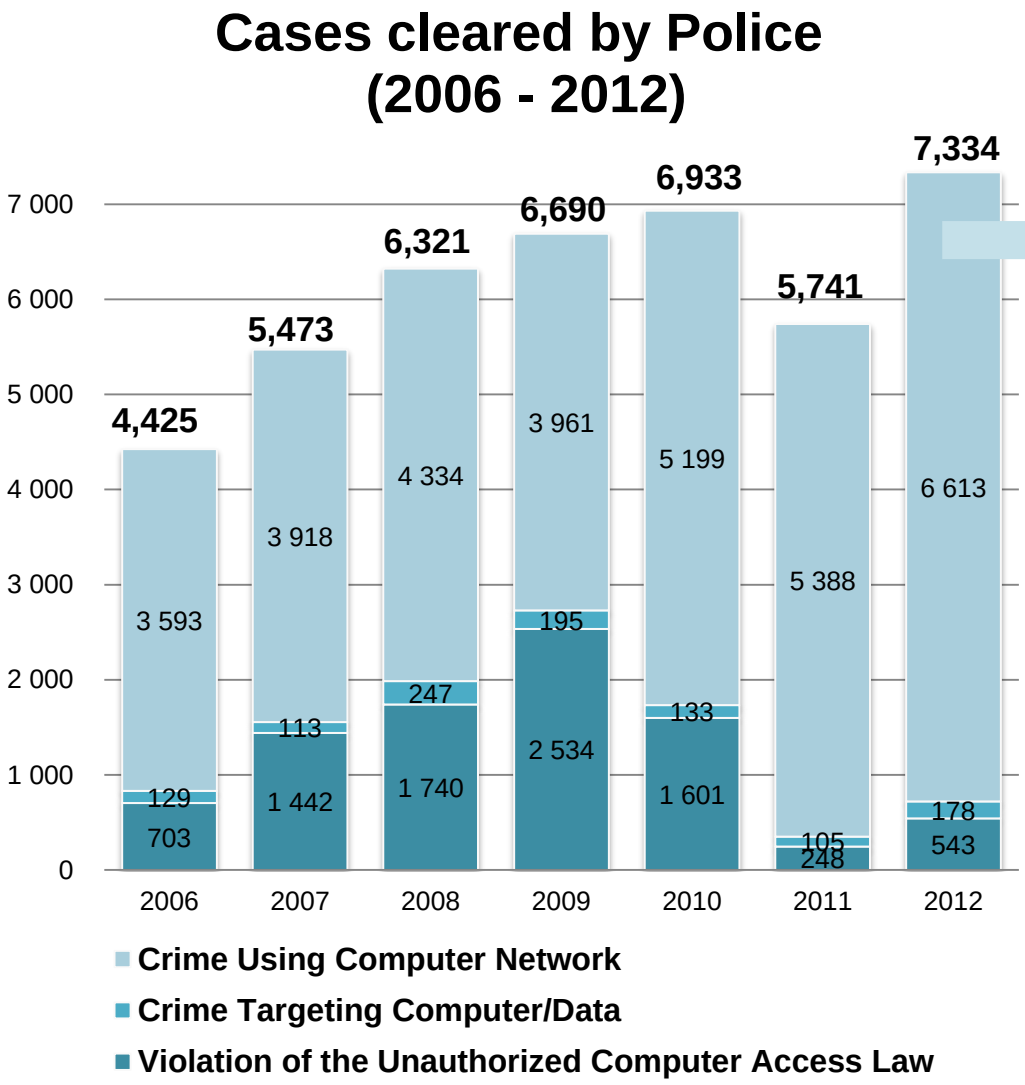
(Source) MIC "2012 Communications Usage Trend Survey"

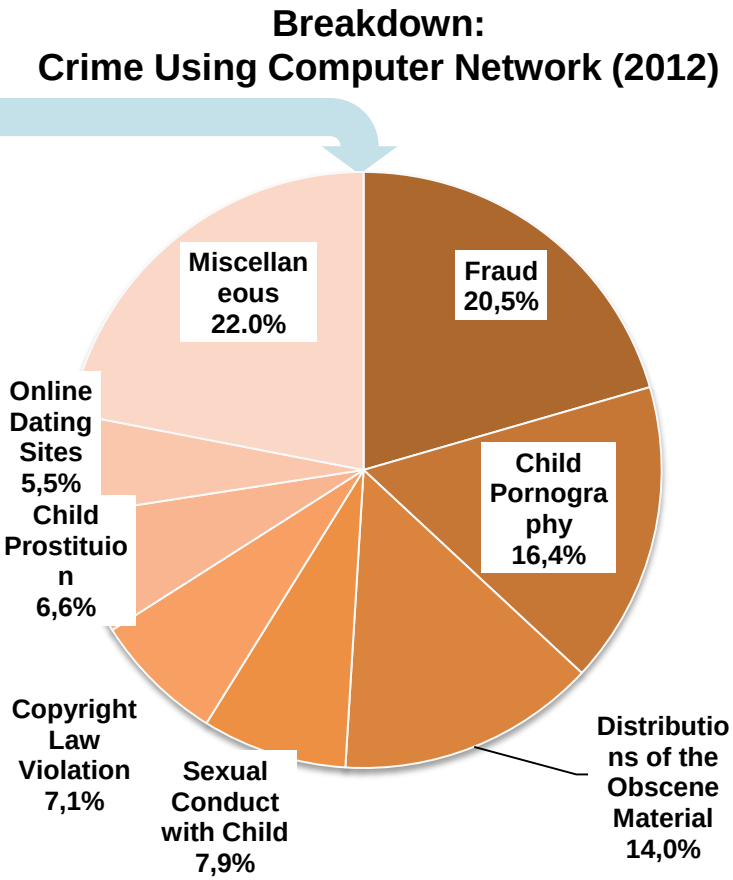
Figure 4-3-1-2 Transitions in the number of Internet users and the population penetration rate



(Source) MIC "2012 Communications Usage Trend Survey"

Status of Cybercrime in Japan





Japan's Cybersecurity Strategy and Measures against Cybercrime

- June 2013: The Government of Japan adopted "**Cybersecurity Strategy**"

Measures against Cybercrime in the Strategy and the related documents

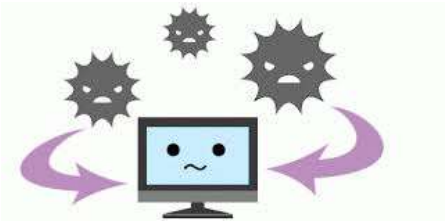
Domestic measures:

- *Development of investigative and analytical capabilities*
- Establishing framework for information-sharing with anti-virus vendors
- Study on preservation of logs (including traffic data)
- *etc…*

International Cooperation:

- "Regarding international cooperation against cybercrime […], Japan will work to strengthen rapid and effective mutual investigations and other cooperation between law enforcement agencies…"
- How? ("**International Strategy on Cybersecurity Cooperation**" adopted in Oct 2013)
  - *By actively participating in the promotion of the Convention on Cybercrime (so-called the Budapest Convention)*
  - *By conducting capacity building activities*

2. The Budapest Convention



Japan's accession to Budapest Convention

- Japan acceded to the Budapest Convention in July 2012 as the first Party from the Asian region

- Japan amended relevant laws in order to accede to the Budapest Convention
  - the Penal Code
  - the Criminal Procedure Law
  - the Act on International Assistance in Investigation and Other Related Matters
  - the Act on Prohibition of Illegal Access
  - Etc.

Common principles for successful international cooperation against cybercrime

1. At least core cybercrime needs to be properly criminalized under substantive criminal law	**Substantive Law**
2. Law enforcement agencies need to have procedural power to investigate	**Procedural Law**
3. Countries should be able to assist with each other on investigation	**International Cooperation**
4. Law enforcement personnel need to have the capacity to investigate	**Investigative Capacity**

Budapest Convention on Cybercrime

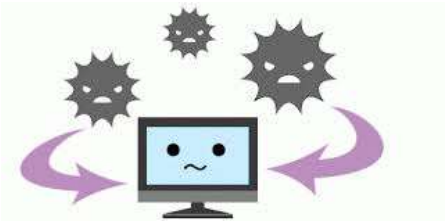
1. Criminalization (Art. 2-13)
• **Offences against computer data and systems:**
  • **illegal access, illegal interception, data interference, system interference, misuse of devices**
• **Offences by means of computers:**
  • **computer-related fraud and forgery, child pornography, intellectual property rights offences**
	Substantive Law

2. Investigative powers (Art. 14-21) • **Electronic evidence in relation to any crime: Expedited preservation, search and seizure of computer data, interception of computer data**	**Procedural Law**
3. Mutual Legal Assistance, Extradition, 24/7 Network (Art. 23-35)	**International Cooperation**
(4. Various capacity building activities conducted by the Parties and the Council of Europe Secretariat)	**Capacity Building**

Avenues for International Cooperation

- Budapest Convention is not the only avenue for international cooperation
- As long as **Substantive Law** and **Procedural Law** are harmonized and law enforcement personnel have the **capacity** to cooperate, other avenues for international cooperation can also be useful
  - Bilateral mutual legal assistance treaties
  - Mutual legal assistance through diplomatic channel (without treaty)
  - Police-to-police cooperation (G8 24/7 network, ICPO)

3. The Role of Capacity Building in the area of Cybercrime



Why capacity building is important?

- Because cybercrime technology evolves constantly
- Because traces and impacts of cybercrime goes beyond one's national borders
- Because we agree on its importance internationally

International Documents on Capacity Building

World Summit on the Information Society 2003: Declaration of Principles

B5) Building confidence and security in the use of ICTs

35 […] A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade. In addition, it must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.

2013 Report of the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security

30. Capacity building is of vital importance to an effective cooperative global effort on securing ICTs and their use. Some States may require assistance in their efforts to improve the security of critical ICT infrastructure; develop technical skill and appropriate legislation, strategies, and regulatory frameworks to fulfil their responsibilities; and to bridge the divide in the security of ICTs and their use.

31. In this regard, States working with international organizations, including UN agencies, and the private sector, should consider how best to provide technical and other assistance to build capacities in ICT security and their use in those countries requiring assistance, particularly developing countries.

2013 G8 Foreign Ministers' Statement

Transnational challenges and opportunities: Cyber

Ministers agreed on the importance of international capacity building efforts to enhance trust, strengthen the fight against cyber crime and improve the security of the global digital environment. They noted that capacity building required the full participation of governments, business and civil society. […]

Ministers agreed that cyber security capacity-building in this area needs to be embedded in the wider context of the economic growth and social benefits derived from the global digital economy. They also agreed to ensure that these efforts are implemented in a way which promotes openness, trust and security, stability and the rule of law in the digital realm.

Different Aspects of Capacity Building in the area of Cybercrime

- Legislation
  - Drafting (substantive law, procedural law)
  - Judiciary
- Law enforcement
  - Basic ICT skill
  - Advanced analytical skill (i.e. digital forensics)
  - Legal understanding
  - Data protection
  - Cooperation with private sector (i.e. ISPs)
  - Establishment of specialized units
- International cooperation
  - Mutual legal assistance
  - Police-to-police cooperation (24/7 network)
  - Cooperation with foreign ISPs

Japan's Capacity Building Activities in the area of Cybercrime

Law enforcement training

- 2002- 2012: "Seminar on Police Info-Communications" (2-week seminar conducted by National Police Agency and JICA [Japan International Cooperation Agency])
- 2008: "The Criminal Justice Response to Cybercrime" (1-month seminar conducted by UNAFEI [UN Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders])

Police-to-police cooperation

- 2000 – annually: "Meeting on Cybercrime Investigative Techniques in the Asia Pacific Region" (NPA)

Workshop (sharing of legislations and good practices)

- May 2013: "Workshop on Effective International Cooperation in the area of Cybercrime Investigation and Prosecution" (MoFA, NPA, MoJ)

Cooperation with International Organizations

- Council of Europe: Octopus Conference
- UNODC (United Nations Office on Drugs and Crime): Global Program on Cybercrime Project for Southeast Asia

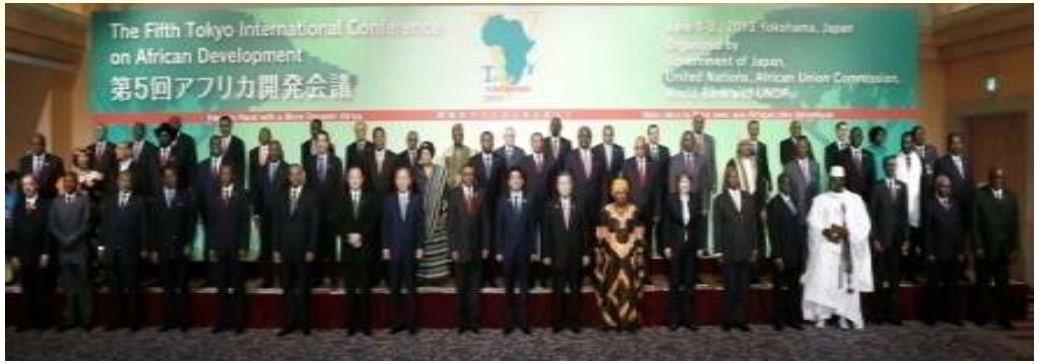
Regional Initiatives

1. Asia Pacific

- **Close cooperation with the Asia Pacific region is crucial due to our geographical proximity and close economic ties**
- **Continue to strengthen cooperation with the ASEAN through Dialogues, Capacity Building and Joint Projects**
  - ✓ ASEAN + Japan Senior Officials Meeting on Transnational Crime (2003-)
  - ✓ ASEAN + Japan Ministerial Meeting on Transnational Crime (2013 -)
  - ✓ **ASEAN + Japan Cybercrime Dialogue (2014 -)**

2. Africa

- **Need to strengthen cooperation with Africa where the use of cyberspace has rapidly progressed**
  - ✓ **TICAD (Tokyo International Conference on African Development) process** since 1993
    - Ministerial Meeting in every 5 years
    - TICAD V held in June 2013 in Yokohama Japan: 51 countries (39 Heads of States level), 72 international organizations and others attended



Thank you!