Digital Economy and Cybersecurity in Japan

November 1\textsuperscript{st}, 2016

Yasu TANIWAKI

Director-General, Global ICT Strategy Bureau, Ministry of Internal Affairs & Communications (MIC)

http://www.mic.go.jp/
Data Driven Society

“The 4th Industrial revolution”

Cyber Space

Data transfer from real world

Stored data

Big data

Data analysis

Control by data analysis

Real World

Sensing, digitalization, transformation of data etc.

AI

IoT

Feedback to the real world

Increasing medical service cost

Increasing nursing cost

Lack of labor

Natural resource scarcity

Solving social problems

Services

healthcare

Smart factory

EMS

Autonomous drive
Evaluation on Global Risks

Most Serious Risk Factor by Country

(Needs citation)

Major Policy Issues on Cybersecurity

✔ Enforcement of national cybersecurity strategy

✔ Cybersecurity on IoT systems

✔ International discussion on cyber space
Major Policy Issues on Cybersecurity

✔ Enforcement of national cybersecurity strategy

✔ Cybersecurity on IoT systems

✔ International discussion on cyber space
Cybersecurity Strategy
(decided by the Cabinet in Sep. 2015)

1 Understanding of cyberspace

2 Objective

3 Basic principles

4 Policy measures towards achieving the objective

- Improvement of Socio-economic vitality and sustainable development
- Building a safe and secure society for the people
- Peace and stability of international community and Japan’s national security

Promotion of R&D / Deployment of human resources

5 Promotion and implementation of cybersecurity strategy
Basic principles

- Free flow of information
- Rules of law
- Ensuring openness
- Ensuring self-governance
- Collaboration among multistakeholders
(4) Risks to Global Commons

In recent years, risks that can impede the utilization of and free access to global commons, such as the sea, outer space, and cyberspace, have been spreading and become more serious.

(Snip)

Cyberspace, a global domain comprised of information systems, telecommunications networks and others, provides a foundation for social, economic, military and other activities. Meanwhile, risks of cyber-attacks with the intent to steal classified information, disrupt critical infrastructure and obstruct military systems, are becoming more serious.

In Japan, with an increasing level of connecting networks of social systems and various other elements, cyberspace is necessary for promoting both economic growth and innovation through the free flow of information in cyberspace. Protecting cyberspace from the above-mentioned risks is vital to secure national security.
Framework of Cybersecurity Basic Act (Jan 2015)

Cabinet
- Submission of “Cybersecurity Strategy” to a Cabinet meeting for approval
- Formulates a draft “CSS”
- Offers opinions on direction and supervision of ministries

IT Strategic HQs
- Views on CSS
- Close cooperation on important issues

Cybersecurity Strategic Headquarters
1. Formulate the “Cybersecurity Strategy” (CSS) and its implementation
2. Formulate common standards for information security measures for national administrative organs and incorporated administrative agencies. Evaluate (including audit) and promote the implementation of such measures
3. Evaluate the measures taken by national administrative organs in the event of significant cybersecurity incidents (including examinations for cause).
4. In addition, perform the following functions:
   a. Research and deliberate on the planning of major cybersecurity policies;
   b. Formulate: inter-governmental implementation plan for such major policies; the national administrative organs’ expense budgeting plan for cybersecurity; guidelines on the implementation of such policies. Promote and evaluate these policies.
   c. Lead comprehensive coordination of cybersecurity policies.

The Prime Minister
- Views on CSS

National Security Council
1. Flexible and substantial discussions on foreign and defense policies related to national security.
2. Discussion on important issues regarding national defense: e.g. measures against an armed attack situation.
3. Responsive discussions on important issues regarding measures against critical incidents; provide advice about what measures the Gov. should take.

Local governments, Independent Administrative Agencies, National Universities, Corporations with special semi-governmental status, Relevant organizations, etc.
- Asks cooperation (e.g. necessary materials)
- May request HQs cooperation (e.g. provision of information, etc.)
- Make an effort to satisfy the request
- Obliged to submit materials, etc.
- Report collection about measures based on the recommendation

National Administrative Organizations, etc.

Legislation required to enable the Cabinet Secretariat to appropriately address these functions.
Major Policy Issues on Cybersecurity

- ✔ Enforcement of national cybersecurity strategy
- ✔ Cybersecurity on IoT systems
- ✔ International discussion on cyber space
IoT as a System of Systems (SoS)

Necessity of dealing with systemic risk (security by design)
Integration between OT and IT (mission assurance)
Information sharing mechanism among multi stakeholders
Major Policy Issues on Cybersecurity

✔ Enforcement of national cybersecurity strategy

✔ Cybersecurity on IoT systems

✔ International discussion on cyber space
Major Issues to be Discussed on Cyber Space

- Applicability of international laws
- International norms
- Confidence building measures (CBM)
- Capacity building assistance
- Awareness raising activities
Applicability of International Laws in Cyberspace (GGE, June 2015)

“In their use of ICTs, States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful measures, and non-intervention in the internal affairs of States.”

“Existing obligations under international law are applicable to State use of ICTs and States must comply with their obligations to respect and protect human rights and fundamental freedoms.”

“States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts.”

“The UN should play a leading role in promoting dialogue on the security of ICTs in their use by States, and in developing common understandings on the application of international law and norms, rules and principles for responsible State behavior.”

(Source) UN General Assembly, Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security (June 2015)
Major Policy Issues on Cybersecurity

✔ Enforcement of national cybersecurity strategy

✔ Cybersecurity on IoT systems

✔ International discussion on cyber space
Policy Issues on CPS (Cyber Physical System)

- Realization of “trust” in cyberspace
- Conversion between cyberspace and real space
- Super globalization of social economic system
- Realization of data driven society

- Digital inclusion (realization of social equality)
- Ensuring network neutrality
- Strengthening network availability (implement SDN/NFV in the society)

- Global coordination of legal systems (avoidance of data localization)
- Realization of global connectivity
- National security in cyberspace

- Internet freedom (internet governance)
- Appropriate balance between security and privacy
- Ensuring “integrity” of data

- Digital inclusion
- Ensuring network neutrality
- Strengthening network availability

- Global coordination of legal systems
- Realization of global connectivity
- National security in cyberspace

- Internet freedom
- Appropriate balance between security and privacy
- Ensuring “integrity” of data
Thank you!