NISC National Information Security Center

Japan's Cybersecurity Strategies

Reiko Kondo
National Information Security Center
Cabinet Secretariat
Japan
December 3rd, 2013

Contents

NISC

1. Overview of Japanese Government Strategies and Policies on Cybersecurity
2. Cybersecurity Strategy (June 10, 2013)
3. International Strategy on Cybersecurity Cooperation - j-initiative for Cybersecurity - (October 2, 2013)

Contents

NISC

1. Overview of Japanese Government Strategies and Policies on Cybersecurity
2. Cybersecurity Strategy (June 10, 2013)
3. International Strategy on Cybersecurity Cooperation - j-initiative for Cybersecurity - (October 2, 2013)

2

Overview of Government Strategies and Guidelines on Cybersecurity

NISC

2005 2006 2007 2008 2009 2010 2011 2012 2013 2014

☆ April 2005: Establishment of National Information Security Center (NISC)
☆ May 2005: Establishment of Information Security Policy Council (ISPC)

[Cybersecurity Strategies]

Information Security Strategy for Protecting the Nation (ISPC, May 2010)

First National Strategy on Information Security (ISPC, February 2006)

Second National Strategy on Information Security (ISPC, February 2009)

Cybersecurity Strategy (ISPC, June 2013)

[Annual Action Plans based on the Strategies]

Secure Japan: SJ 2006 | SJ 2007 | SJ 2008 | SJ 2009
Information Security: IS 2010 | IS 2011 | IS 2012
Cybersecurity: CS 2013 | CS 2014

[Standards for Information Security Measures for the Central Government Computer Systems]

Guideline	First to Third edition (ISPC, December 2005)	Forth edition (ISPC, February 2009)	To be revised

[Action Plan on Information Security Measures for Critical Infrastructures]

action plan for cyber terrorism	First edition (ISPC, December 2005)	Second edition (ISPC, February 2009)	To be revised

3

Coordination of the National Information Security Policies

NISC

The Information Security Policy Council (ISPC)

- Chair: Chief Cabinet Secretary
- Deputy Chair: Minister of State for Science and Technology Policy
- Members: MIC (Ministry of Internal Affairs and Communications), METI (Ministry of Economy, Trade and Industry), NPA (National Police Agency), MOFA (Ministry of Foreign Affairs) & MOD (Ministry of Defense) Ministers and experts from academia and industries
- Formulate and endorse policy documents pertaining to cross-ministerial information security policy

The National Information Security Center (NISC)

- Secretariat of the Information Security Policy Council

Facilitator of information security efforts of the governmental agencies | *Coordinator for Public-Private Partnerships* | *Point of Contact for International Affairs*


Government Agencies


Critical Infrastructure, Businesses and Individuals


Foreign governments and international organizations

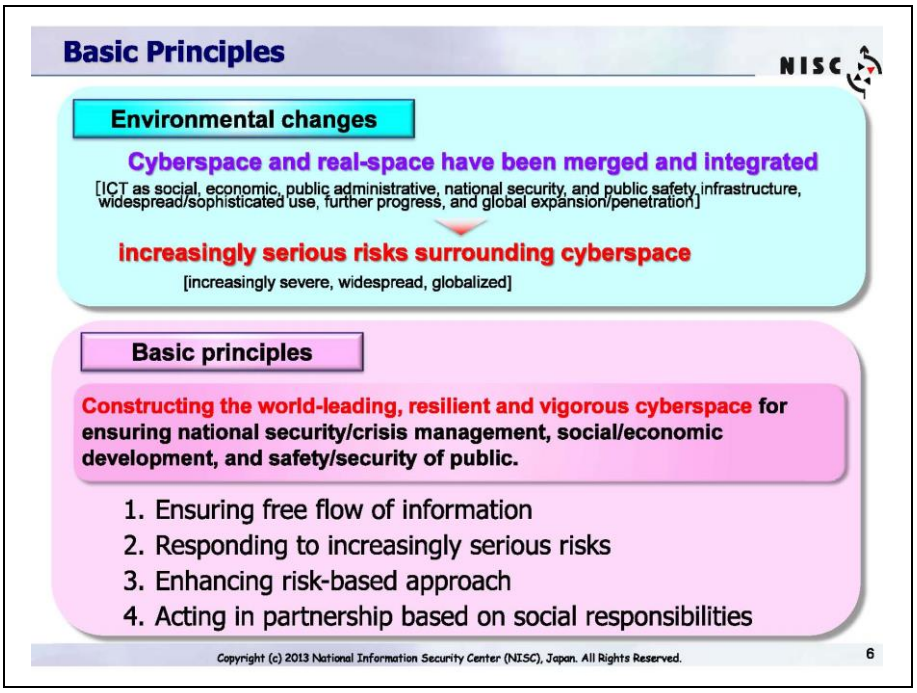
4

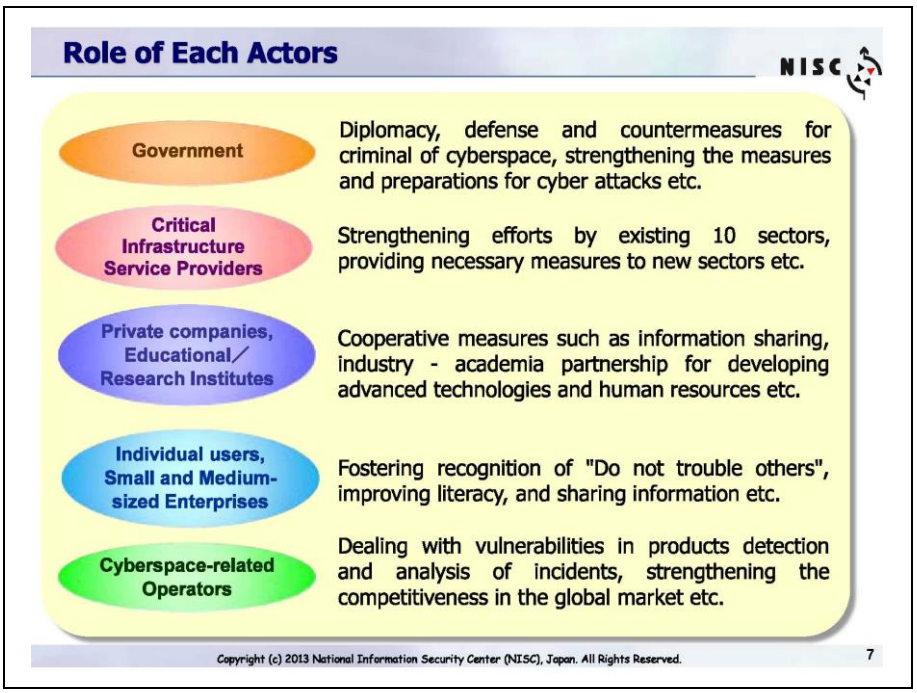
Contents

NISC

1. Overview of Japanese Government Strategies and Policies on Cybersecurity
2. Cybersecurity Strategy (June 10, 2013)
3. International Strategy on Cybersecurity Cooperation - j-initiative for Cybersecurity - (October 2, 2013)

5


Basic Principles
NISC
Environmental changes
Cyberspace and real-space have been merged and integrated
[ICT as social, economic, public administrative, national security, and public safety infrastructure, widespread/sophisticated use, further progress, and global expansion/penetration]
increasingly serious risks surrounding cyberspace
[increasingly severe, widespread, globalized]
Basic principles
Constructing the world-leading, resilient and vigorous cyberspace for ensuring national security/crisis management, social/economic development, and safety/security of public.
1. Ensuring free flow of information
2. Responding to increasingly serious risks
3. Enhancing risk-based approach
4. Acting in partnership based on social responsibilities
Copyright (c) 2013 National Information Security Center (NISC), Japan. All Rights Reserved.
6


Role of Each Actors
NISC
Government
Diplomacy, defense and countermeasures for criminal of cyberspace, strengthening the measures and preparations for cyber attacks etc.
Critical Infrastructure Service Providers
Strengthening efforts by existing 10 sectors, providing necessary measures to new sectors etc.
Private companies, Educational／Research Institutes
Cooperative measures such as information sharing, industry - academia partnership for developing advanced technologies and human resources etc.
Individual users, Small and Medium-sized Enterprises
Fostering recognition of "Do not trouble others", improving literacy, and sharing information etc.
Cyberspace-related Operators
Dealing with vulnerabilities in products detection and analysis of incidents, strengthening the competitiveness in the global market etc.
Copyright (c) 2013 National Information Security Center (NISC), Japan. All Rights Reserved.
7

Main Efforts based on the "Cybersecurity Strategy" (1)

NISC

Resilient Cyberspace — Government ministries and agencies, Independent administrative organizations etc.

- ✓ Review of the Standards for Information Security Measures for the Central Government Computer Systems and establishment of the methods of risk assessment in order to protect sensitive information 【This fiscal year】
- ✓ Strengthening GSOC, accurate and quick response through cooperation with CYMAT and CSIRT
- ✓ Conducting incident response drills, specifying roles of related organizations such as the police and the Self Defense Forces 【This fiscal year】
- ✓ Measures for new threats pursuant to new services, including SNS and group mail

GSOC: Government Security Operation Coordination team
CYMAT: Cyber incident Mobile Assistant Team

8

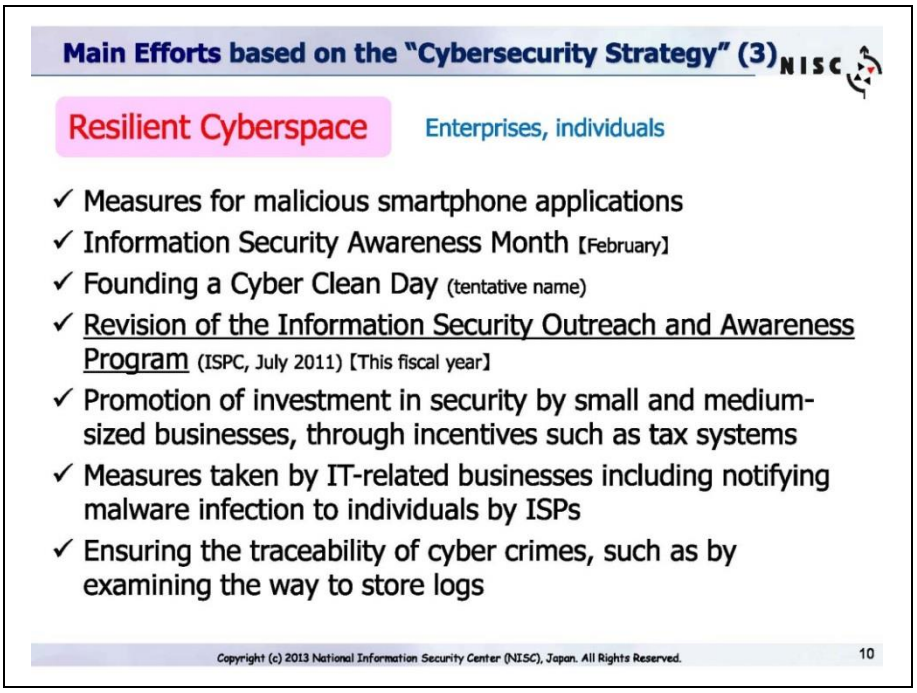
Main Efforts based on the "Cybersecurity Strategy" (2)

NISC

Resilient Cyberspace — Critical Infrastructure Service Providers

- ✓ Review of the Action Plan including expanding the scope of critical infrastructure and review of the Safety Standards 【This fiscal year】
- ✓ Strengthening information sharing with government organizations and system vendors, etc.
- ✓ Conducting cross-sectoral exercises for ensuring business continuity
- ✓ Building a platform for evaluation and authentication of such systems as control systems used by critical infrastructure, in compliance with international standards 【This fiscal year】

9


Main Efforts based on the "Cybersecurity Strategy" (3)
NISC
Resilient Cyberspace
Enterprises, individuals
✓ Measures for malicious smartphone applications
✓ Information Security Awareness Month 【February】
✓ Founding a Cyber Clean Day (tentative name)
✓ Revision of the Information Security Outreach and Awareness Program (ISPC, July 2011) 【This fiscal year】
✓ Promotion of investment in security by small and medium-sized businesses, through incentives such as tax systems
✓ Measures taken by IT-related businesses including notifying malware infection to individuals by ISPs
✓ Ensuring the traceability of cyber crimes, such as by examining the way to store logs
Copyright (c) 2013 National Information Security Center (NISC), Japan. All Rights Reserved.
10


Main Efforts based on the "Cybersecurity Strategy" (4)
NISC
Vigorous Cyberspace (Building Fundamentals)
✓ Revision of the Information Security Human Resource Development Program (ISPC, July 2011) 【This fiscal year】
✓ Review of the Information Security Research and Development Strategy (ISPC, July 2011)
World-leading Cyberspace
International Strategy on Cybersecurity Cooperation
- j-initiative for Cybersecurity -
(ISPC, October 2013)
Copyright (c) 2013 National Information Security Center (NISC), Japan. All Rights Reserved.
11

Contents

NISC

1. Overview of Japanese Government Strategies and Policies on Cybersecurity
2. Cybersecurity Strategy (June 10, 2013)
3. International Strategy on Cybersecurity Cooperation - j-initiative for Cybersecurity - (October 2, 2013)

Basic Principles

NISC

Basic Principles

Summarized the importance of international cooperation with regards to 4 basic principles described in the Cybersecurity Strategy

1. Ensuring free flow of information

Countries around the world can enjoy freedom of expression and vibrant economic activities, innovation, economic growth and solutions for social issues

2. Responding to increasingly serious risks

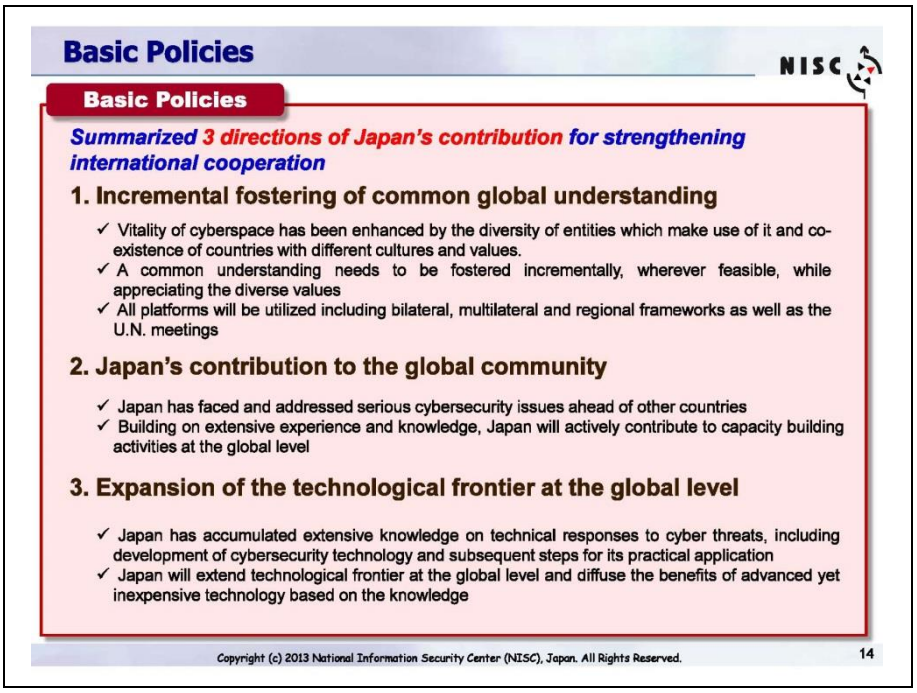
A new mechanism based on enhanced international cooperation in addition to the existing measures and initiatives against increasingly serious, widespread and globalized risks is necessary.

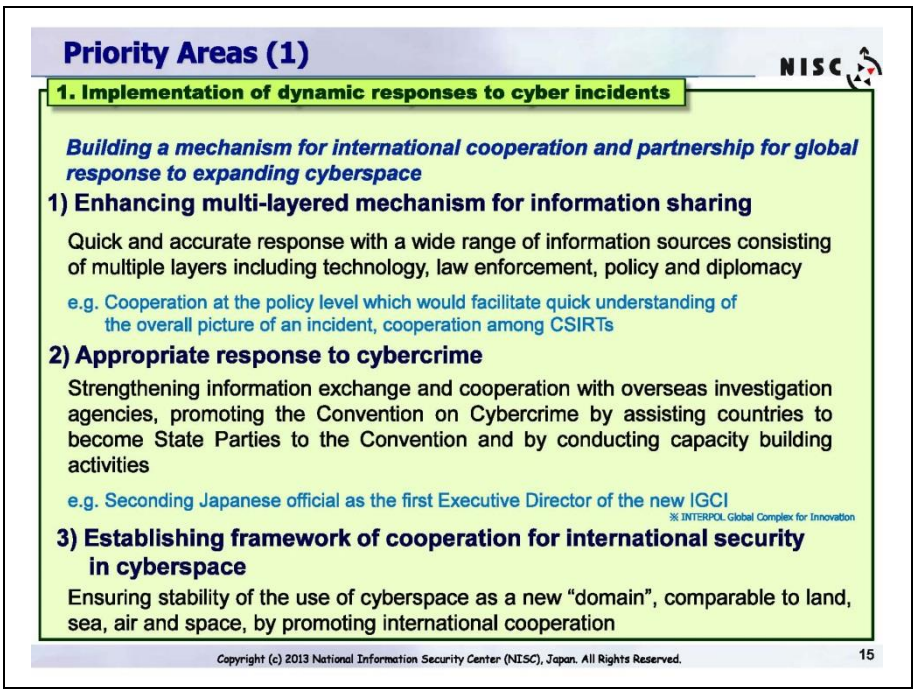
3. Enhancing risk-based approach

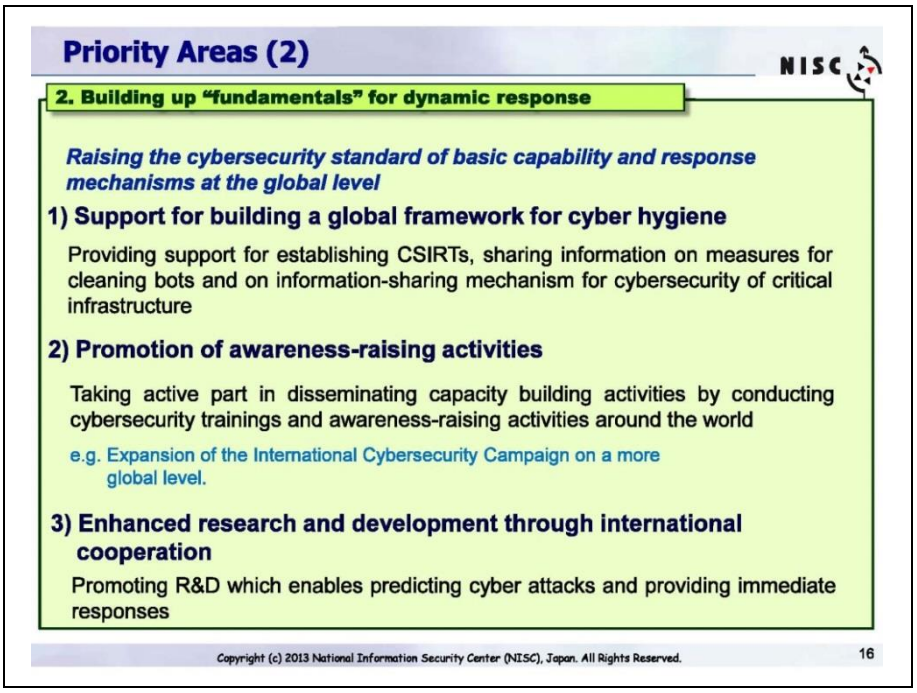
Establishing a mechanism to implement a risk-based approach, whereby risks are quickly and appropriately identified as they evolve and responded to dynamically in accordance with their characteristics is urgent for the international community

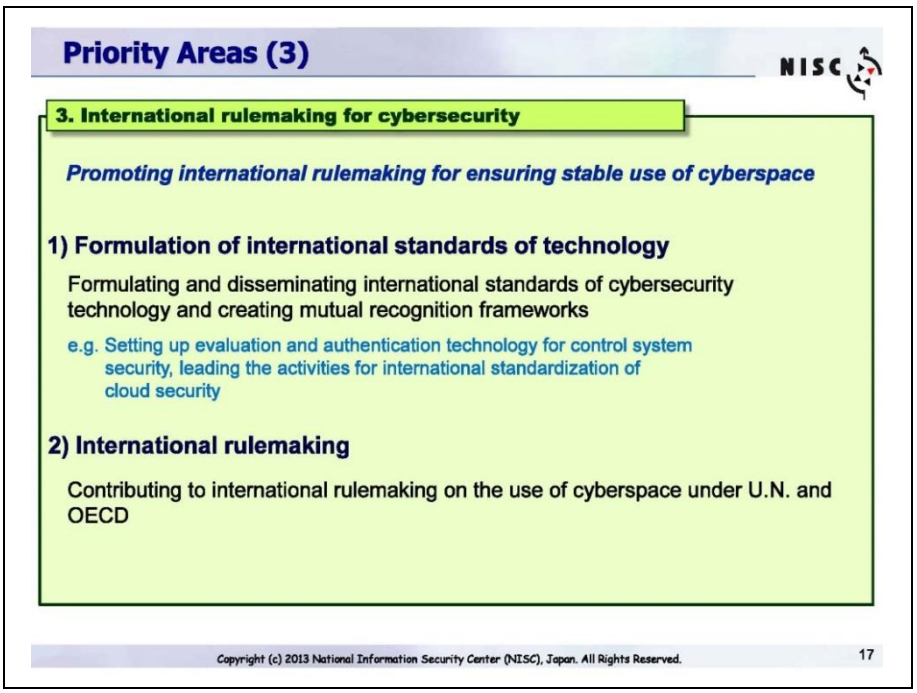
4. Acting in partnership based on social responsibilities

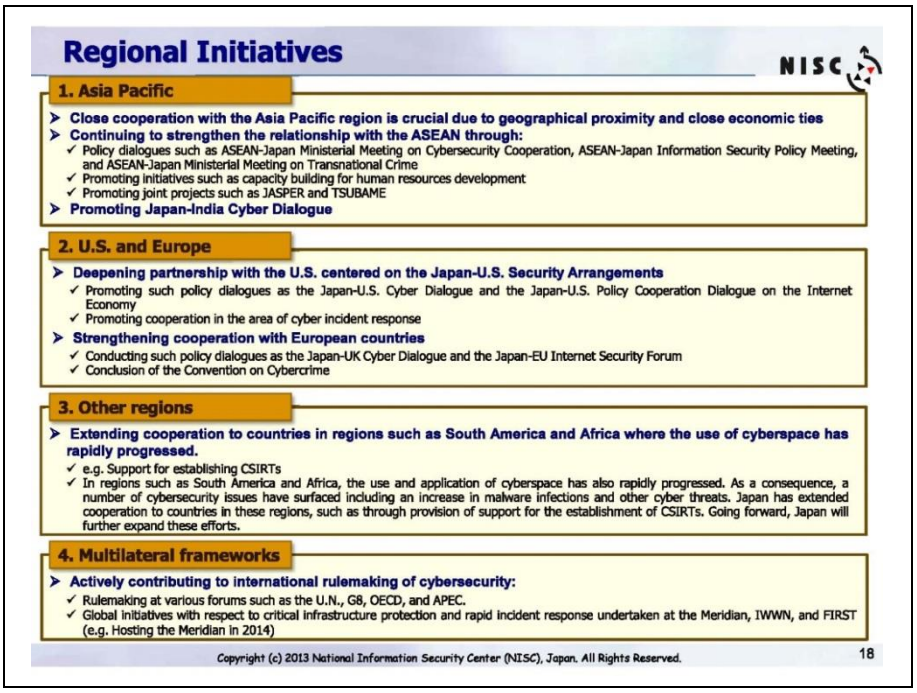
All stakeholders in the global cyberspace need to cooperate and assist with each other while fulfilling the responsibilities corresponding to their respective roles in the society


Basic Policies
NISC
Basic Policies
Summarized 3 directions of Japan's contribution for strengthening international cooperation
1. Incremental fostering of common global understanding
✓ Vitality of cyberspace has been enhanced by the diversity of entities which make use of it and co-existence of countries with different cultures and values.
✓ A common understanding needs to be fostered incrementally, wherever feasible, while appreciating the diverse values
✓ All platforms will be utilized including bilateral, multilateral and regional frameworks as well as the U.N. meetings
2. Japan's contribution to the global community
✓ Japan has faced and addressed serious cybersecurity issues ahead of other countries
✓ Building on extensive experience and knowledge, Japan will actively contribute to capacity building activities at the global level
3. Expansion of the technological frontier at the global level
✓ Japan has accumulated extensive knowledge on technical responses to cyber threats, including development of cybersecurity technology and subsequent steps for its practical application
✓ Japan will extend technological frontier at the global level and diffuse the benefits of advanced yet inexpensive technology based on the knowledge
Copyright (c) 2013 National Information Security Center (NISC), Japan. All Rights Reserved.
14


Priority Areas (1)
NISC
1. Implementation of dynamic responses to cyber incidents
Building a mechanism for international cooperation and partnership for global response to expanding cyberspace
1) Enhancing multi-layered mechanism for information sharing
Quick and accurate response with a wide range of information sources consisting of multiple layers including technology, law enforcement, policy and diplomacy
e.g. Cooperation at the policy level which would facilitate quick understanding of the overall picture of an incident, cooperation among CSIRTs
2) Appropriate response to cybercrime
Strengthening information exchange and cooperation with overseas investigation agencies, promoting the Convention on Cybercrime by assisting countries to become State Parties to the Convention and by conducting capacity building activities
e.g. Seconding Japanese official as the first Executive Director of the new IGCI
※ INTERPOL Global Complex for Innovation
3) Establishing framework of cooperation for international security in cyberspace
Ensuring stability of the use of cyberspace as a new "domain", comparable to land, sea, air and space, by promoting international cooperation
Copyright (c) 2013 National Information Security Center (NISC), Japan. All Rights Reserved.
15


Priority Areas (2)
NISC
2. Building up "fundamentals" for dynamic response
Raising the cybersecurity standard of basic capability and response mechanisms at the global level
1) Support for building a global framework for cyber hygiene
Providing support for establishing CSIRTs, sharing information on measures for cleaning bots and on information-sharing mechanism for cybersecurity of critical infrastructure
2) Promotion of awareness-raising activities
Taking active part in disseminating capacity building activities by conducting cybersecurity trainings and awareness-raising activities around the world
e.g. Expansion of the International Cybersecurity Campaign on a more global level.
3) Enhanced research and development through international cooperation
Promoting R&D which enables predicting cyber attacks and providing immediate responses
Copyright (c) 2013 National Information Security Center (NISC), Japan. All Rights Reserved.
16


Priority Areas (3)
NISC
3. International rulemaking for cybersecurity
Promoting international rulemaking for ensuring stable use of cyberspace
1) Formulation of international standards of technology
Formulating and disseminating international standards of cybersecurity technology and creating mutual recognition frameworks
e.g. Setting up evaluation and authentication technology for control system security, leading the activities for international standardization of cloud security
2) International rulemaking
Contributing to international rulemaking on the use of cyberspace under U.N. and OECD
Copyright (c) 2013 National Information Security Center (NISC), Japan. All Rights Reserved.
17



Regional Initiatives

NISC

1. Asia Pacific

- **Close cooperation with the Asia Pacific region is crucial due to geographical proximity and close economic ties**
- **Continuing to strengthen the relationship with the ASEAN through:**
  - ✓ Policy dialogues such as ASEAN-Japan Ministerial Meeting on Cybersecurity Cooperation, ASEAN-Japan Information Security Policy Meeting, and ASEAN-Japan Ministerial Meeting on Transnational Crime
  - ✓ Promoting initiatives such as capacity building for human resources development
  - ✓ Promoting joint projects such as JASPER and TSUBAME
- **Promoting Japan-India Cyber Dialogue**

2. U.S. and Europe

- **Deepening partnership with the U.S. centered on the Japan-U.S. Security Arrangements**
  - ✓ Promoting such policy dialogues as the Japan-U.S. Cyber Dialogue and the Japan-U.S. Policy Cooperation Dialogue on the Internet Economy
  - ✓ Promoting cooperation in the area of cyber incident response
- **Strengthening cooperation with European countries**
  - ✓ Conducting such policy dialogues as the Japan-UK Cyber Dialogue and the Japan-EU Internet Security Forum
  - ✓ Conclusion of the Convention on Cybercrime

3. Other regions

- **Extending cooperation to countries in regions such as South America and Africa where the use of cyberspace has rapidly progressed.**
  - ✓ e.g. Support for establishing CSIRTs
  - ✓ In regions such as South America and Africa, the use and application of cyberspace has also rapidly progressed. As a consequence, a number of cybersecurity issues have surfaced including an increase in malware infections and other cyber threats. Japan has extended cooperation to countries in these regions, such as through provision of support for the establishment of CSIRTs. Going forward, Japan will further expand these efforts.

4. Multilateral frameworks

- **Actively contributing to international rulemaking of cybersecurity:**
  - ✓ Rulemaking at various forums such as the U.N., G8, OECD, and APEC.
  - ✓ Global initiatives with respect to critical infrastructure protection and rapid incident response undertaken at the Meridian, IWWN, and FIRST (e.g. Hosting the Meridian in 2014)

18