Cyber Security Policy in Japan

Prof. HASHIMOTO, Yasuaki
The National Institute for Defense Studies
Tokyo, Japan

(The views expressed in this presentation are those of the author and do not represent the ones of any organization.)

Self Introduction

Prof. HASHIMOTO, Yasuaki

Director, Department of Policy Studies

The National Institute for Defense Studies (NIDS)

International Law (Sea, Air, Space, Cyberspace)

NIDS

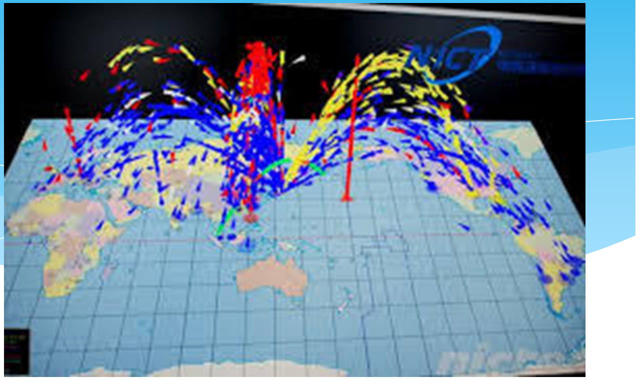
National Institute focusing on Security Studies

The Highest Educational Organization for Military Officers and Government Officials

East Asian Strategic Review

NIDS China Security Report

1. Present Our Situation –Increasing Cyber Attacks



Cyber Attacks Observed in Japan

2005	2010	2012	2013	2014	2015	2016	2017
3.0B.	5.8B.	7.8B.	12.8B.	25.6B.	54.5B.	128B.	150B.

Rapidly Increase of Cyber Attacks to IoT Devices

2015 26% → 2017 54%

2015 15B. Devices → 2020 30B. Devices!

（NICT: National Institute of Information and Communication Technology）

Clear and Present Danger

How Many Attacks in 2020 Tokyo Olympiad?

2. Actual Cyber Attacks –My Cases-

(1) 2011 SJAC (The Society of Japanese Aerospace Com.)

Targets: Aerospace/Defense Companies (MHI, IHI, KHI…)

By 2 Mails (The 1st :True → The 2nd :Spoofing, ATP)

From Correct Address to Target Business Address

Attached MS WORD Document with Virus

Through Back Doors Leaking Information

(2) 2018 Spoofing Mail from Me to One Retired Colonel

Target: Retired Colonel (Cyber Defense Unit Commander)

From Different Address to Target Private Address

Attached MS WORD Document with Virus

Digital Forensic → APT10

pixta.jp - 15239735

3. National Security Strategy and Cyber

Recognizing Importance of Cyber Security in Japan

National Security Strategy (December, 2013)

Global Commons (Ocean, Outer Space & Cyber Space)

"Protecting Cyber Space …

is Vital to Secure National Society"

4. Basic Act on Cybersecurity

Basic Act on Cybersecurity (November, 2014)

Bipartisan Proposal

(Liberal Democratic Party, New Komeito, Democratic Party, etc.)

☆ National Leadership for Cyber Security in Japan

☆ Respecting Freedom of Information

☆ Setting Cyber Security Policy by Government

☆ Cooperation of All Infrastructure Providers and Cyber Related Companies

☆ Development of Human Resources

5. Cyber Security Strategy (2015 & 2018)

Much Attention to Global Commons

2007 Basic Act of Ocean

2008 Basic Act of Outer Space

2013 (The First) National Security Strategy

2014 Basic Act of Cybersecurity

2015 The First Cybersecurity Strategy

2018 The Second Cybersecurity Strategy

6. Background of Cybersecurity

2015 Strategy: Real Space –Interconnected- Cyberspace
but Separated

↓

2018 Strategy: Real Space –Unification- Cyberspace

Society 5.0:

Paradigm Shift which No One Have Experienced Before

Need to Response to TOKYO 2020 Olympic/Paralympic Games

7. Objective and Policy Approaches

Understanding

AI, IoT, Fintech, Robotics, 3D Printers, VR are Established in the Society.

⇒ Society 5.0

So Many Benefits from Cyberspace Services

⇕

Threats (Control Loss, Interruptions, Financial Damages, National Security…)

Objectives

For Sustainable Development for Society 5.0
(Cybersecurity Ecosystem)

Policy Approaches

1. Mission Assurance
2. Risk Management
3. Commitment to a Free, Fair and Secure Cyberspace

8. Policy I: Mission Assurance (1)

Multi-layered Cybersecurity

- Governmental Bodies (Real Time Management)
- Local Governments
- Cyber-related Enterprises

Critical Infrastructure Operators

Educational and Research Institutions

Every People

Promoting Information Sharing/Collaboration Framework

- Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR)

9. Policy I Mission Assurance (2)

Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR): 19 Fields

1. Telecommunications, 2. Cable TV, 3. Broadcast,
4. Bank, 5. Securities, 6. Life insurance, 7. Property insurance,
8. Aviation, 9. Airport, 10.Railroad,
11. Electricity supply service, 12. Gas supply service, 13. Water supply service,
14. Medical care, 15. Logistics, 16. Chemical, 17. Credit, 18. Oil,
19. Governmental administrative services

CEPTOAR Council (Information Sharing between CEPTOARs)

Exercise for Critical Infrastructure

(Once a Year, Over 2,000 Participants)

10. Policy II: Risk Management

Cybersecurity as Value Creation Driver

From Passive Attitude

⇨ To Active Attitude for Business Executives

From Cost ⇨ To Investment

Better Supply Chain

Frameworks (Across Industrial Categories)

Focusing on Small and Medium-sized Enterprises

Secured IoT Systems

Improving Security Framework for IoT Systems

Establishing Models for Improving IoT Device Security

(Especially for Small Companies)

11. Policy III: Commitment to a Free, Fair and Secure Cyberspace

Japan Herself

Defense, Deterrence, Cyber Situational Awareness

Resilience (Mission Assurance, Defending Japan’s High Technologies)

Deterrence (Effective Deterrence, Confidence Building Measures)

Situational Awareness (Capability Increasing, Threat Information Sharing)

Regional and International Cooperation

Sharing Expertise, Coordination Policy

International Collaboration for Incident Response

Capacity Building (Especially for Developing Countries)

12. Cross-cutting Approaches for Policy I, II & III

Human Resources for Cybersecurity

Need 200,000 Engineers in 2020 (METI, 2016)

RISS (Registered Information Security Specialist)

National Qualification for Cybersecurity: 18,000 at Present

Core Engineers for Necessary Security Arrangement

National Cyber Training Center (April 2017)

CYDER: CYber Defense Exercise with Recurrence

100 Training/Year, 3,000 Participants

Action Plan for Public Awareness

Moral Education (in School), Cybersecurity Awareness Month (Whole Society)

Stardust Project (Honey Network and Honeypot)

Special Network for Researching Cyberattacks
and Digital Forensics

13. New Defense Program Guidelines

December 2018 Cabinet Decision

New Domains:

Space, Cyber Space and Electromagnetic Spectrum

Multi-domain Defense

Cross-Domain Operations:

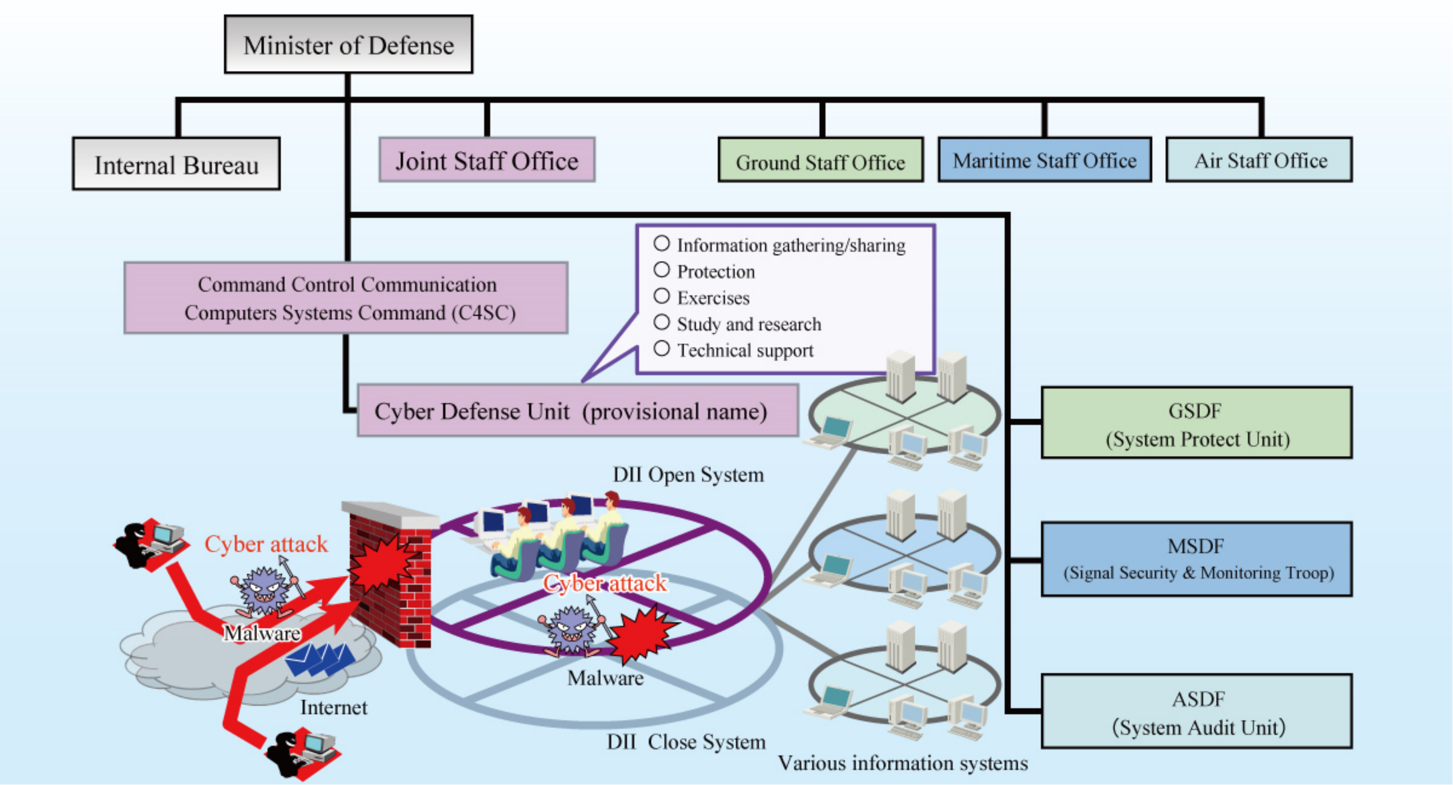
Even when Inferiority exists in Individual Domains, such Inferiority will be overcome

Bigger Cyber Defense Unit of JSDF

14. Japan Self Defense Forces

Cyber Defense Unit (From March, 2014)

Joint Organization 120 ⇒ 150 (⇒ 500:2023)



Conclusion

Japan now faces much harder Cyberattacks.
(Machine Translation Effect)

Secured Cyberspace is necessary for New IoT Devices and 5G Telecom world.

One of the Problems is Lack of Enough Human Resource.

Japan still tries to improve our Cyberspace.
Information Sharing, Counter Measures,
International Cooperation