Urgent Need to Develop National Cyber Intelligence System In Japan

～The Biggest weakness of the U.S.-Japan alliance～

July 26, 2022

Satoru Tezuka
Keio University

Six Critical Proposals for enhancing cyber capabilities of Japan

1. The threat of hybrid war was realized in Ukraine war. The risk of Taiwan contingency is now real. The weakest point of the US-Japan Alliance is cybersecurity. If the telecommunication networks or the power grids are down in Japan, US forces in Japan and SDF can be defeated by PLA before fighting starts.

2. Japan needs to do a lot of homework to catch up with the US as well as UK and Australia, possible allies of Taiwan contingency.
   (1) Appointment of National Cyber Security Commandant in the Prime Minister's Office with staff including SDF

   (2) Establish legal authority for the Cyber Commandant for:
      (a) Cyber situation awareness; watch dog for cyberspace
      (b) Determination of attribution of cyber attacker beyond the physical border
      (c) Active defense to stop any persistent and repeated attack beyond the physical border

   (3) Establish a government cloud with strong fire wall for:
      (a) Digital integration of intelligence community of Japan
      (b) Including sensitive high-tech companies and defense industry into the government cloud
      (c) Taking advantage of AI with effective search engine for producing good intel materials
      (d) Establish an OSINT center for cyber intelligence with AI and a super computer
      (e) Storing the whole data flow in a super computer for open-source intelligence analysis

   (4) Establish the Intel Intra-Net of the government with a high-level encryption, possibly with quantum technology

   (5) Establish the clearance system to scrutinize the government employees against possible corruption with the foreign agents

   (6) Establish a Quantum Cyber research center/town in Yokosuka for synergy of military, intelligence, industrial and scientific technologies
      (a) Open to foreign researchers
      (b) With Substantial Government/Private fund

Contents

1. Challenges facing Japan
2. Attribution Overview
3. Five Eyes and U.S. Situation
4. National Cyber Intelligence System in Japan
5. Summary

1. Challenges facing Japan

- On two occasions, in December 2015 and December 2016, cyber attacks caused major power outages.
- With the help of the U.S. military and the NSA, Ukraine has strengthened its cyber defenses for its power system.
- In February 2022, during the invasion of Ukraine, no major power outages due to cyber-attacks have been confirmed.

December 2015: 6 hours to restore, 220,000 people affected.
December 2016: a little over an hour to restore

Affected Areas

February 2022: No major power outages were observed.

https://www.ipa.go.jp/files/000076755.pdf
https://www.ipa.go.jp/files/000076756.pdf

1. Challenges facing Japan

- **Two months before the start of the military invasion of Ukraine (2/24), Russia spread disinformation about the production of biological weapons.**
- **U.S. Cyber Intelligence System Detected Disinformation, Sealed Russia's Intent to Use Biological Weapons**
- **Cyber intelligence systems are essential as a defense against the cyber weapon of disinformation.**

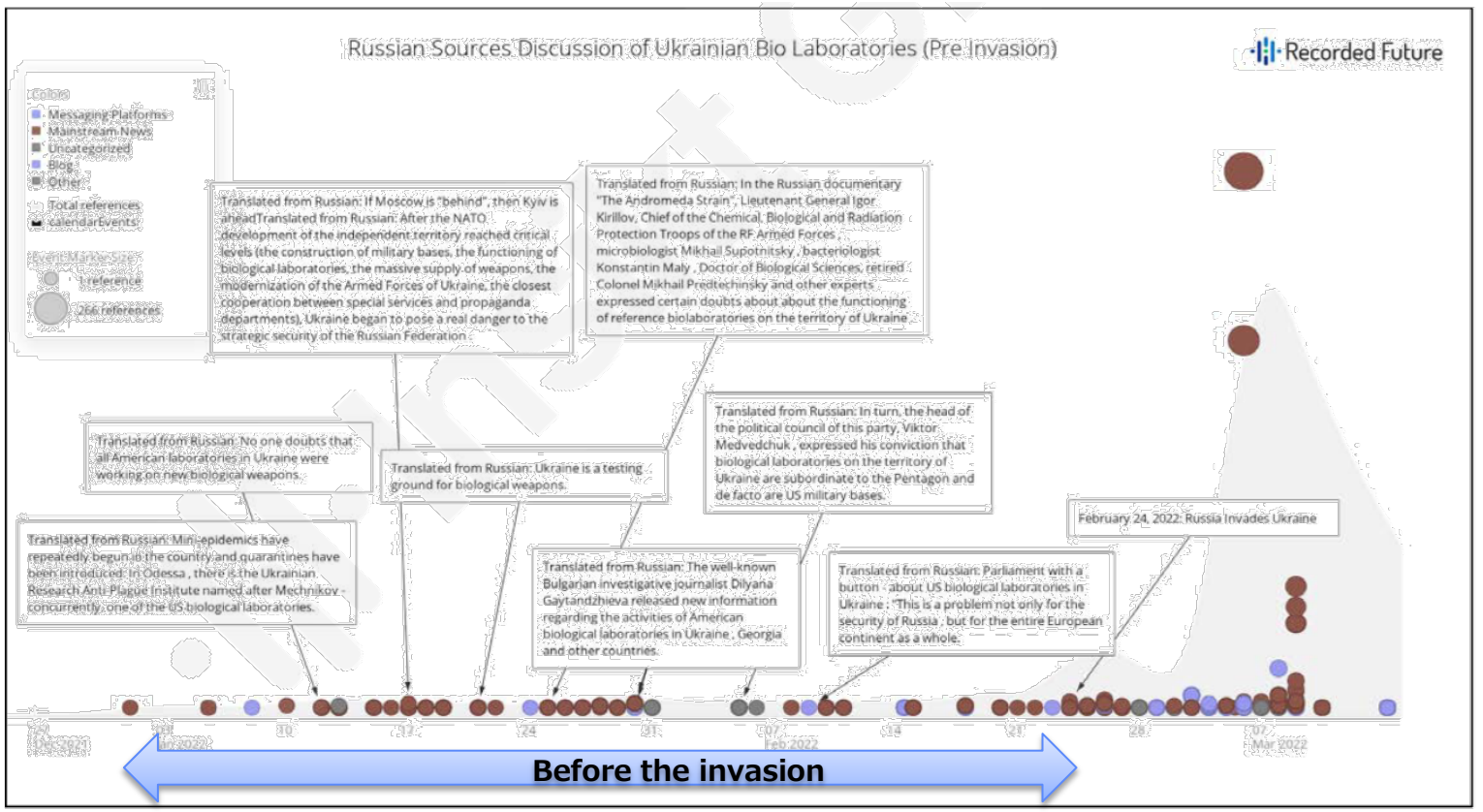


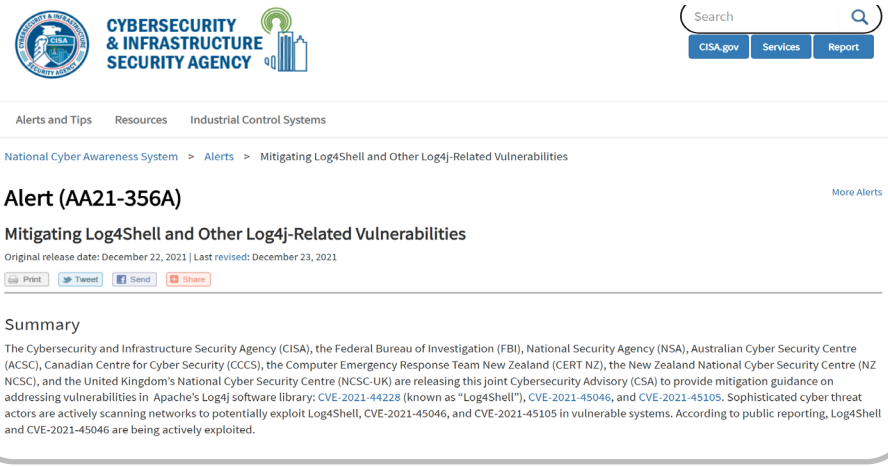
Figure 4: *Russian sources discussion of Ukrainian bio laboratories pre-February 24, 2022 invasion of Ukraine (Source: Recorded Future)*

1. Challenges facing Japan

- Japan has not been able to participate in international cooperation against threats and vulnerabilities in cyberspace
- There is an urgent need to establish a national cyber intelligence system, which Japan does not yet have, as soon as possible.
- In the event of a future Taiwan contingency, although there is a Japan-U.S. alliance, the absence of a national cyber intelligence system makes rapid information sharing between the U.S. and Japan regarding national security impossible.

2021 Emotet (Malware) Infection Expansion 8 Countries Collaborate to Create Takedowns
Netherlands / Germany / France
Lithuania / Canada / USA
United Kingdom / Ukraine

2021 Log4j (destructive vulnerability) exploit
U.S. CISA joins five countries in issuing emergency directive
United States (CISA, the FBI, NSA)
Australia (ACSC)
Canada (CCCS)
New Zealand (CERT NZ, NZ NCSC)
United Kingdom (NCSC-UK)



Source: https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global- action
https://www.cisa.gov/uscert/ncas/alerts/aa21-356a

Contents

1. Challenges facing Japan
2. Attribution Overview
3. Five Eyes and U.S. Situation
4. National Cyber Intelligence System in Japan
5. Summary

2. Attribution Overview

- Characteristics of cyberspace
  - High degree of anonymity
  - Evidence can be tampered with.
  - No geographic or time constraints
  - Damage can be easily spread to an unspecified number of people

- Attribution in cyber attacks
  - Identifying the attacker
  - Identifying the methods used and the purpose of the project

- Asymmetry between attackers and defenders
  - Attackers use malicious tools that are easily available to anyone on the Internet and then you can make a single breakthrough
  - Defenders must be able to respond to cyber attacks in all directions

2. Attribution Overview

- **Mandiant's 2013 report triggered deep state involvement**

Table: Major APT (Advanced Persistent Threat) Activities

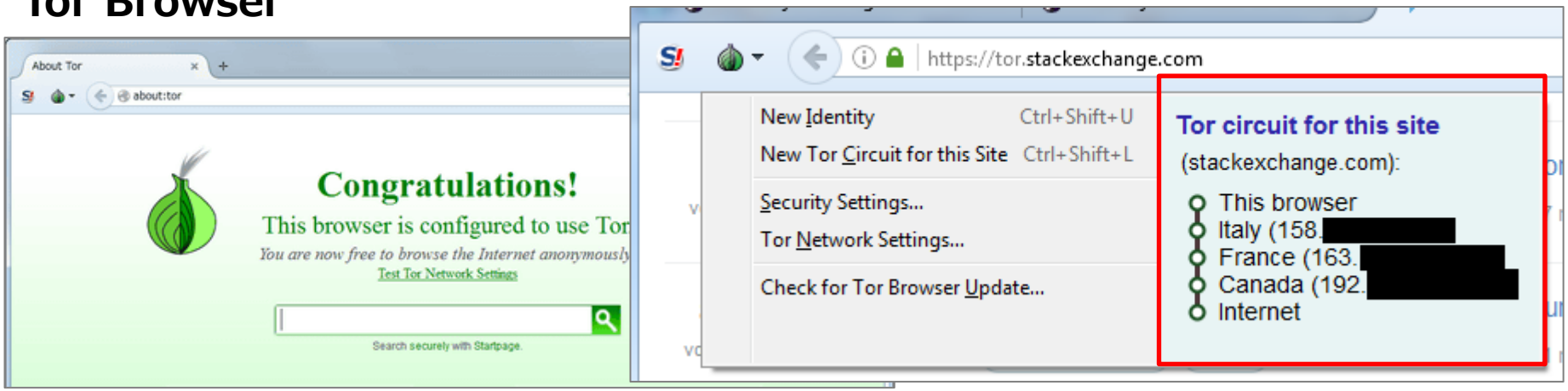
period	Name of activity	Contents
2005	Titan Rain	Attacks that have penetrated U.S. defense firms and other companies since 2003
2009	GhostNet	Attacks targeting the Tibetan government in 2008-2009
2010	Operation Aurora	Attacks targeting several U.S. companies, including Google, that occurred at the end of 2009
2010	Shadow Network	2009 attacks targeting India, Tibet, and other countries.
2011	Night Dragon	Attacks targeting the global energy industry and other sectors since 2009
2011	Attacks on RSA, Lockheed Martin	A series of attacks in 2011 that broke into RSA and used illegally obtained product information to subsequently attempt to break into Lockheed Martin
2011	Operation Shady RAT	Attacks against organizations in the U.S. and around the world since 2006
2011	Nitro Attacks	2011 attacks targeting several organizations, including the chemical industry
2011	Sykipot	Attacks targeting U.S. and U.K. military and other industries since 2011
2012	LuckyCat	Attacks targeting India, Japan, and other Asian countries since 2011
2012	Elderwood	Attacks against defense companies and other organizations around the world since 2009
2013	APT1	Attacks against organizations in the U.S. and around the world since 2006

Source: https://atmarkit.itmedia.co.jp/ait/articles/1305/09/news004_2.html

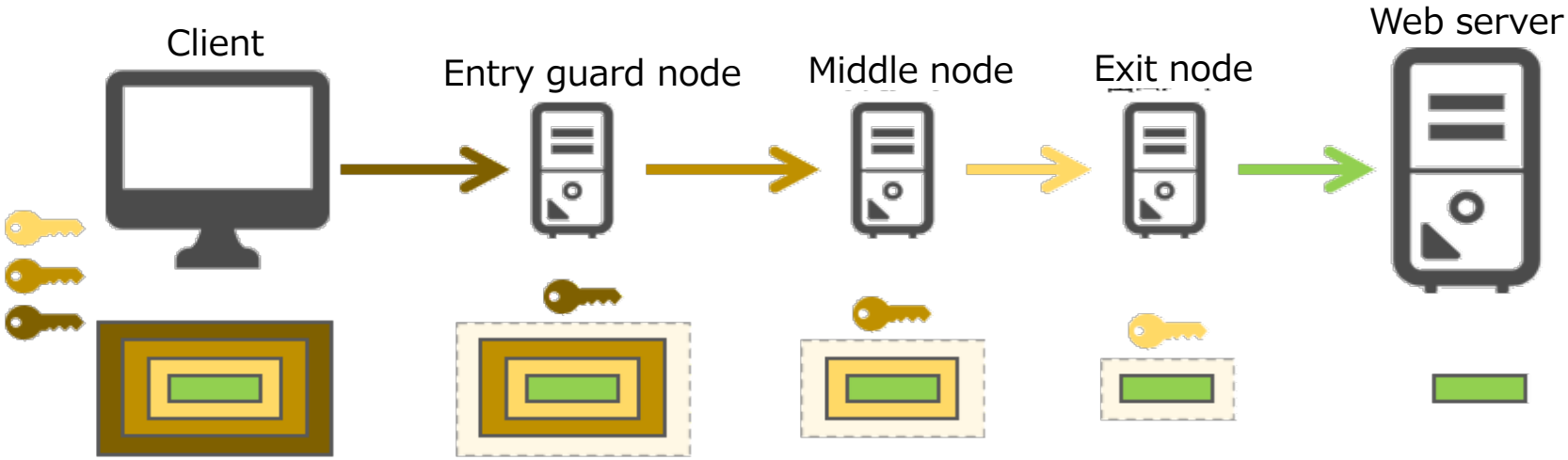
2. Attribution Overview

- **Tor (The Onion Router)**

Tor Browser



Packets are sent multiply encrypted, and decrypted "like peeling an onion" each time they cross a node.



Source: https://phantomcryptomining.com/deepweb/tor-browser/

2. Attribution Overview

- **Information used for attribution**
  - Information on the recipient
  - Information on means of attack
  - Information on attacker behavior

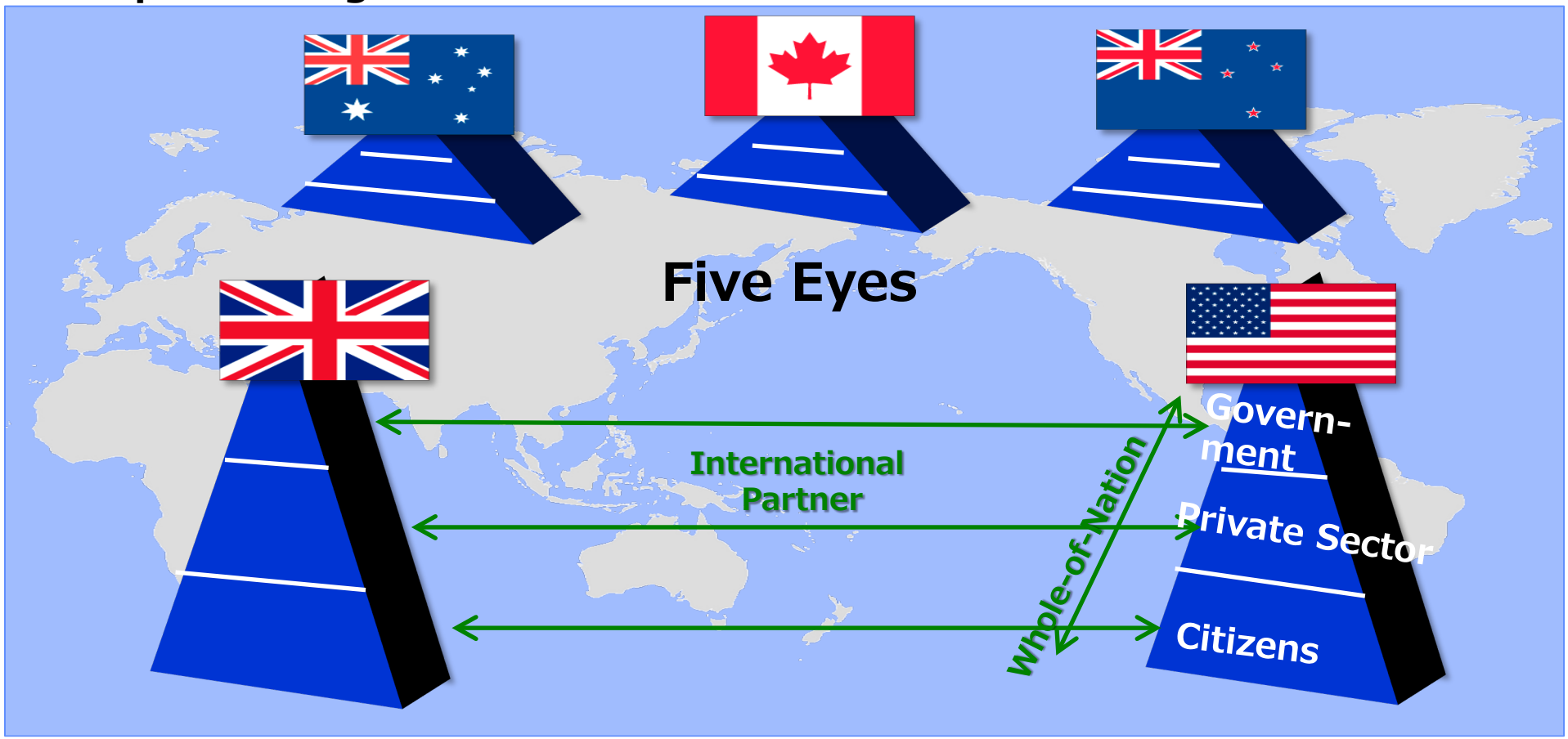
- **Urgent need to establish a national cyber intelligence system for attribution as soon as possible**
  - The National Cyber Intelligence System needs to be managed and operated with appropriate defenses.
  - Establishment of optimal technologies, operations, and systems for protection and defense is necessary.

Contents

1. Challenges facing Japan
2. Attribution Overview
3. Five Eyes and U.S. Situation
4. National Cyber Intelligence System in Japan
5. Summary

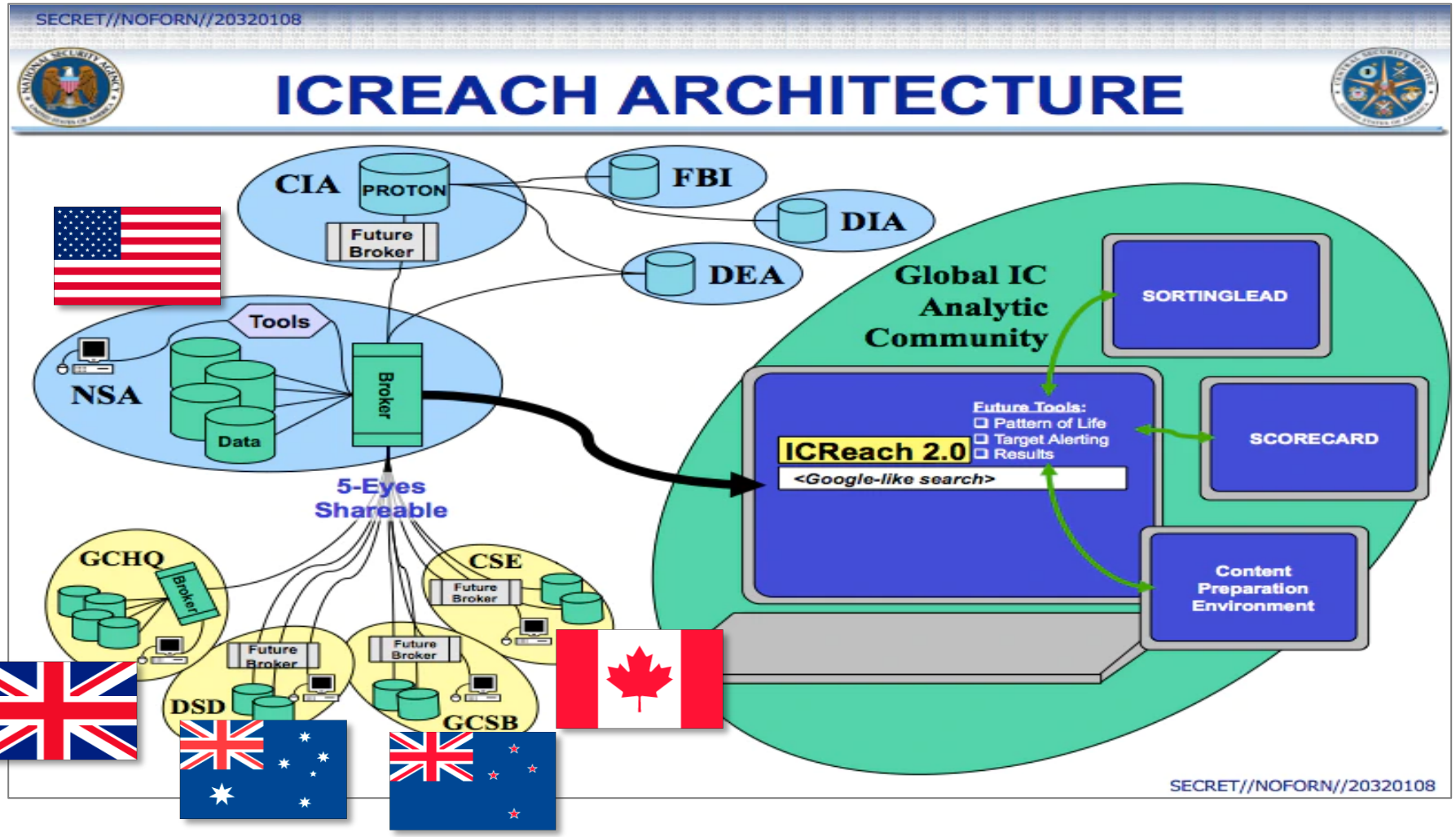
3. Five Eyes and U.S. Situation

- Five Eyes has a Give&Take information sharing framework through the International Cyber Intelligence Circle (ICIC : International Cyber Intelligence Circle)
- Countries are building national cyber intelligence systems and implementing international collaboration



3. Five Eyes and U.S. Situation

- U.S. NSA manages intelligence sharing among the Intelligence Community (IC) in the U.S.
- U.S. NSA also manages information sharing with Five Eyes



3. Five Eyes and U.S. Situation

Data classification: Classification Levels (EO 13526)

- **Controlled Unclassified Information (CUI)** is an information category defined by **Executive Order 13556 (2010)**
- In response to those instructions, NARA took on the role of creating CUI protection guidelines for the entire federal government
- Under NARA's direction, NIST formulated the SP800-171 standard for the protection of CUI
- CUI can be regarded as a category similar to "sensitive information" as defined by Japan's Ministry of Defense

Executive order
EO 13556
Controlled Unclassified Information
November 4, 2010.

NARA

NATIONAL ARCHIVES

NIST

Confidentiality

US	Classified Information Top Secret · Secret · Confidential	CUI	Unclassified information
Japan	Secret (gokuhi) / top secret (kimitsu) / confidential (hi)	Sensitive information	General information

3. Five Eyes and U.S. Situation

Human classification: Security Clearance (EO 13526)

- Personal Identity Verification (PIV) card: Owned by federal agency employees
- PIV- I (Interoperable) card: Owned by private contractors who have passed security clearance
  - Ticket information (for face-to-face identity verification)
  - Digital certificate (LoA4)
  - Encryption key
  - FASC-N (Federal Agency Smart Credential Number)
  - Biometric information (fingerprint, iris)

Face-to-face identity verification
Use of ticket information

Electronic authentication
Use of digital certificates
Biological information
Card authentication key

Physical access control
Use of digital certificates and PIV card readers
Verification of certificate validity during physical access

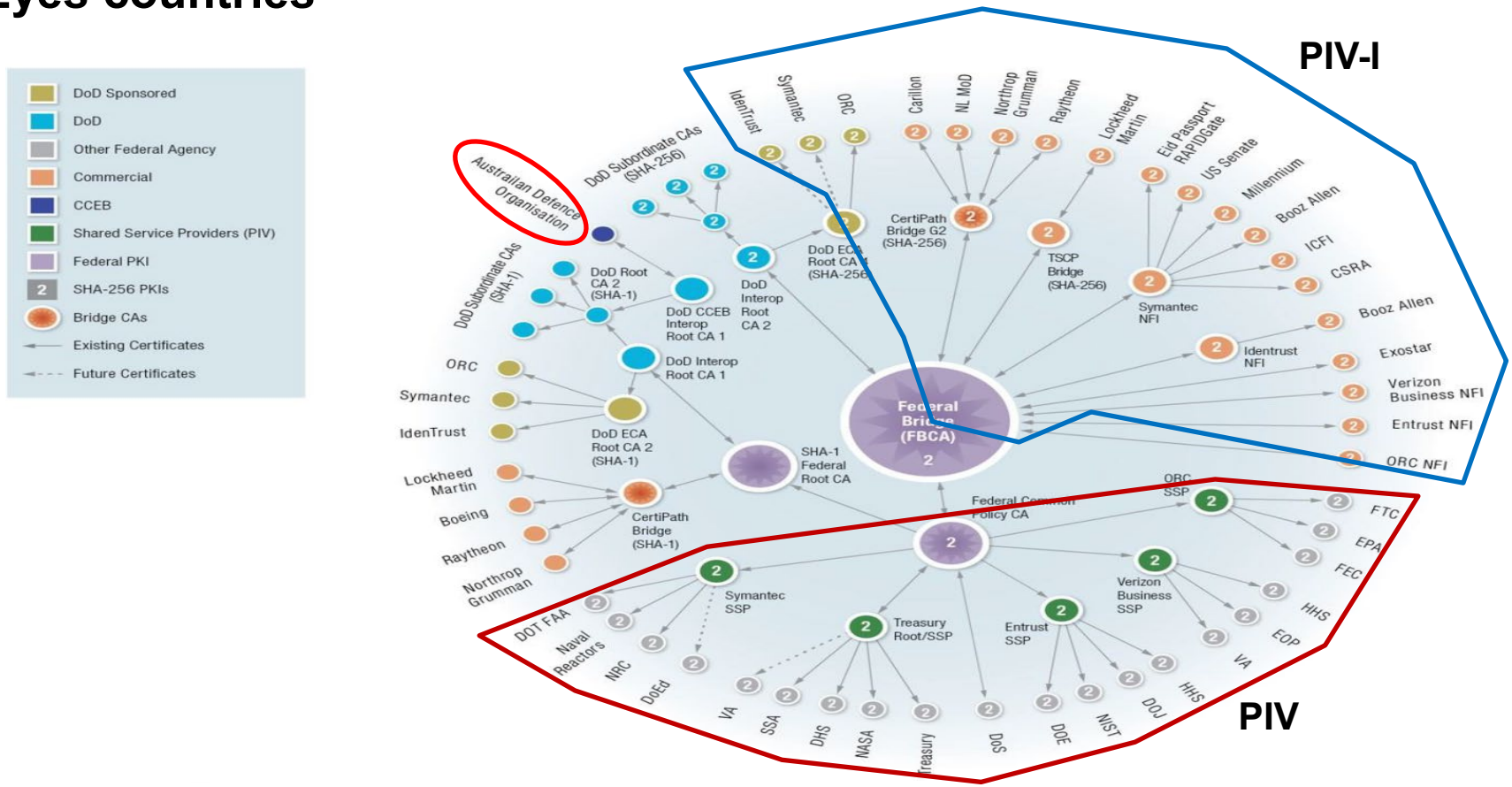
Electronic signatures
Use of digital certificates

Encryption
Use of digital certificates

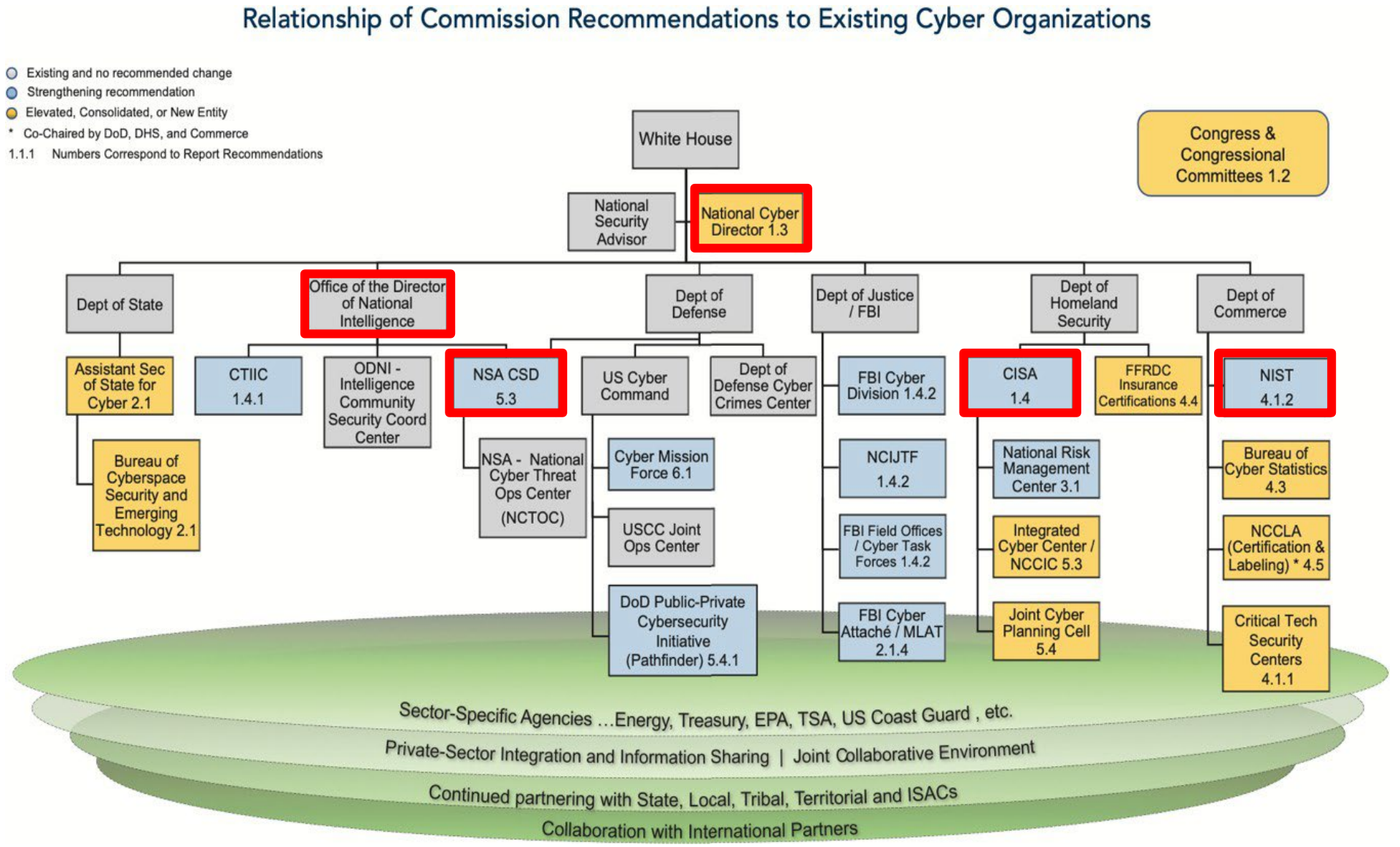
Logical access control
Use of digital certificates
Biological information
Card authentication key

3. Five Eyes and U.S. Situation

- Overview of Cyber Intelligence Systems in the U.S. Government
- Topology of Certification Authorities rooted in the U.S. PIV and FBCA issued by PIV-I
- International collaboration between the U.S. government and Five Eyes countries



3. Five Eyes and U.S. Situation



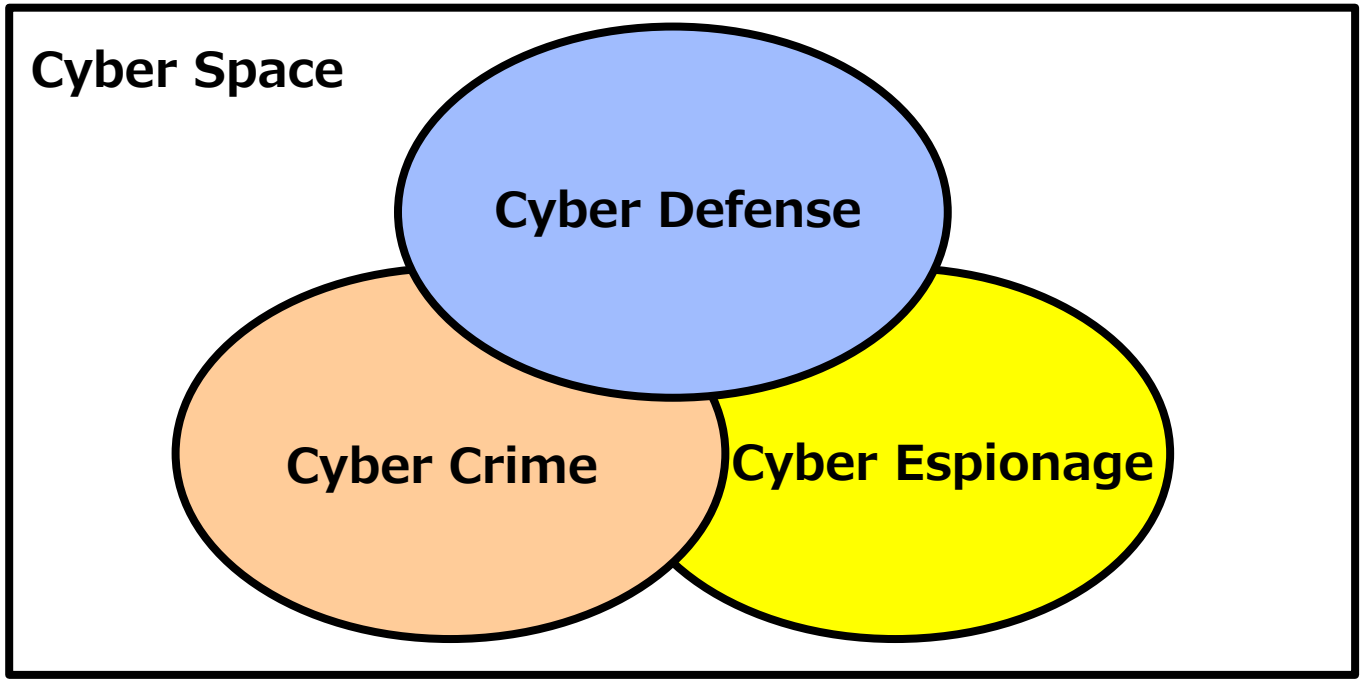
Source: The Cyberspace Solarium Commission

Contents

1. Challenges facing Japan
2. Attribution Overview
3. Five Eyes and U.S. Situation
4. National Cyber Intelligence System in Japan
5. Summary

4. National Cyber Intelligence System in Japan

- In the physical space, defense, crime, and intelligence have advanced separately
- In cyberspace, defense, crime, and intelligence occur without necessarily clear boundaries
- In Japan, there is an urgent need to establish a national cyber intelligence system in cyberspace as soon as possible.



4. National Cyber Intelligence System in Japan

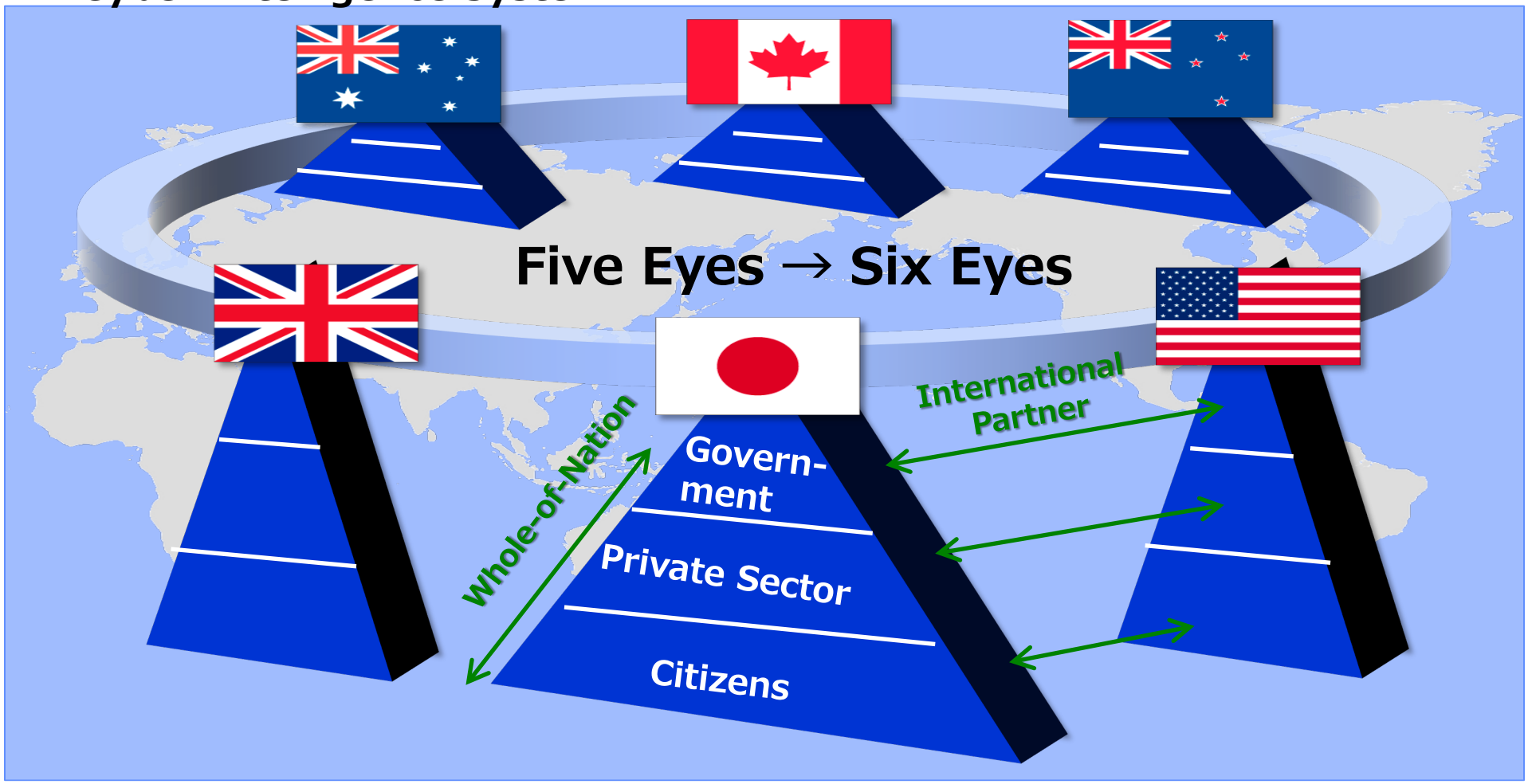
- **National Cyber Intelligence System**
  NCIS : National Cyber Intelligence System

  - **Cyber Threat Intelligence**
    CTI : Cyber Threat Intelligence

  - **Cyber Vulnerability Intelligence**
    CVI : Cyber Vulnerability Intelligence

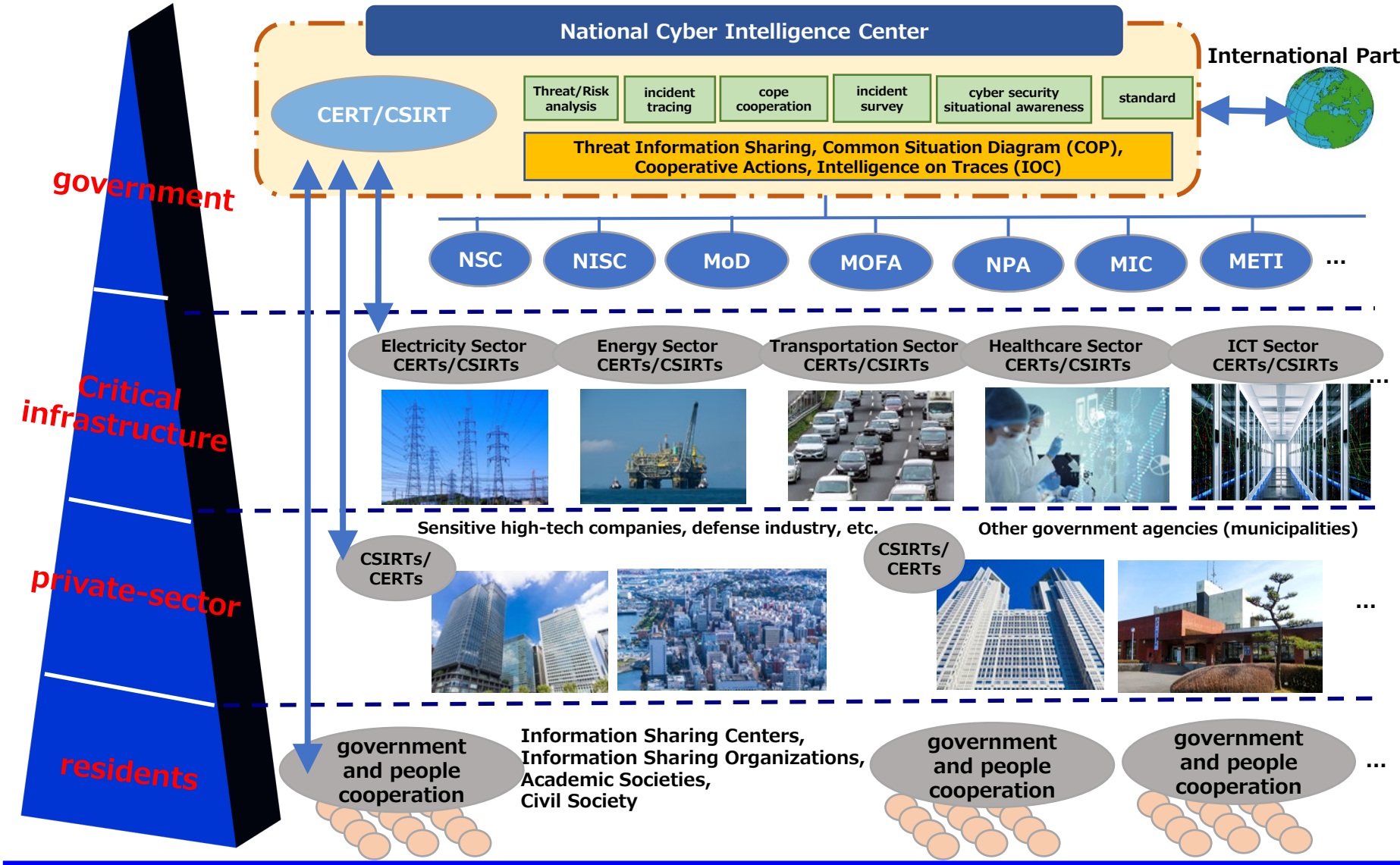
4. National Cyber Intelligence System in Japan

- International Cyber Intelligence Circle (ICIC : International Cyber Intelligence Circle) Give&Take framework is essential
- Establish international collaboration with Five Eyes in the National Cyber Intelligence System



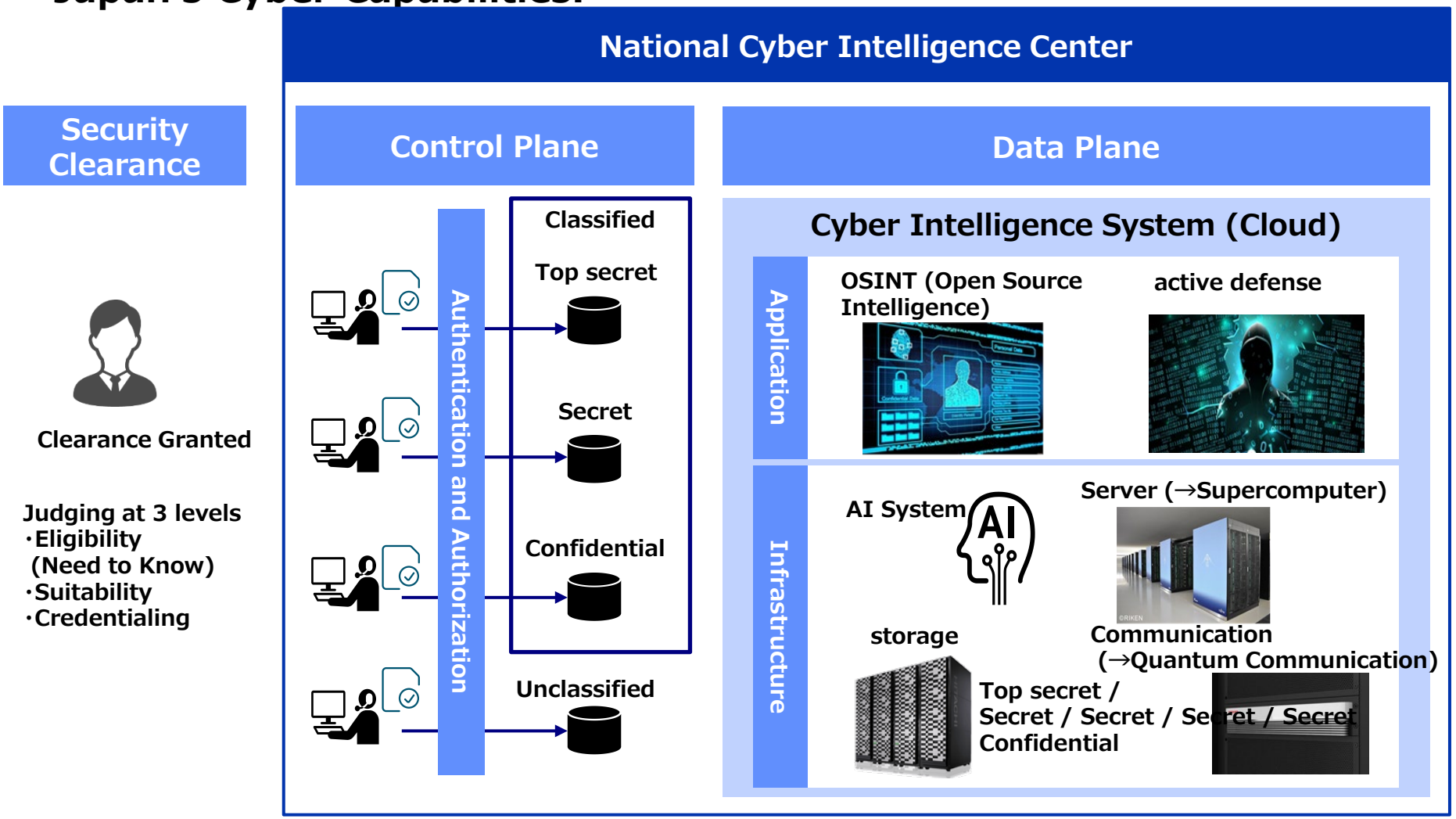
4. National Cyber Intelligence System in Japan

- **Overview of the National Cyber Intelligence System in Japan**



4. National Cyber Intelligence System in Japan

- **It is essential to build a cyber intelligence system that meets the requirements of the "Six Key Recommendations for Strengthening Japan's Cyber Capabilities.**

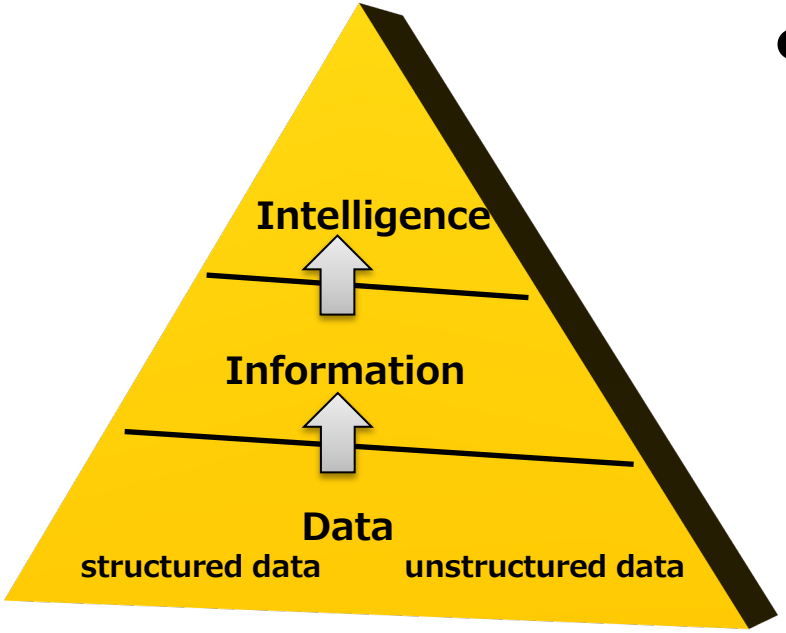


4. National Cyber Intelligence System in Japan

- **Purpose of AI Application**
  - **From Data to Information**

    ⇒Collect a wide variety and large volume of OSINT data and turn it into information that AI systems can understand.
  - **From Information to Intelligence**

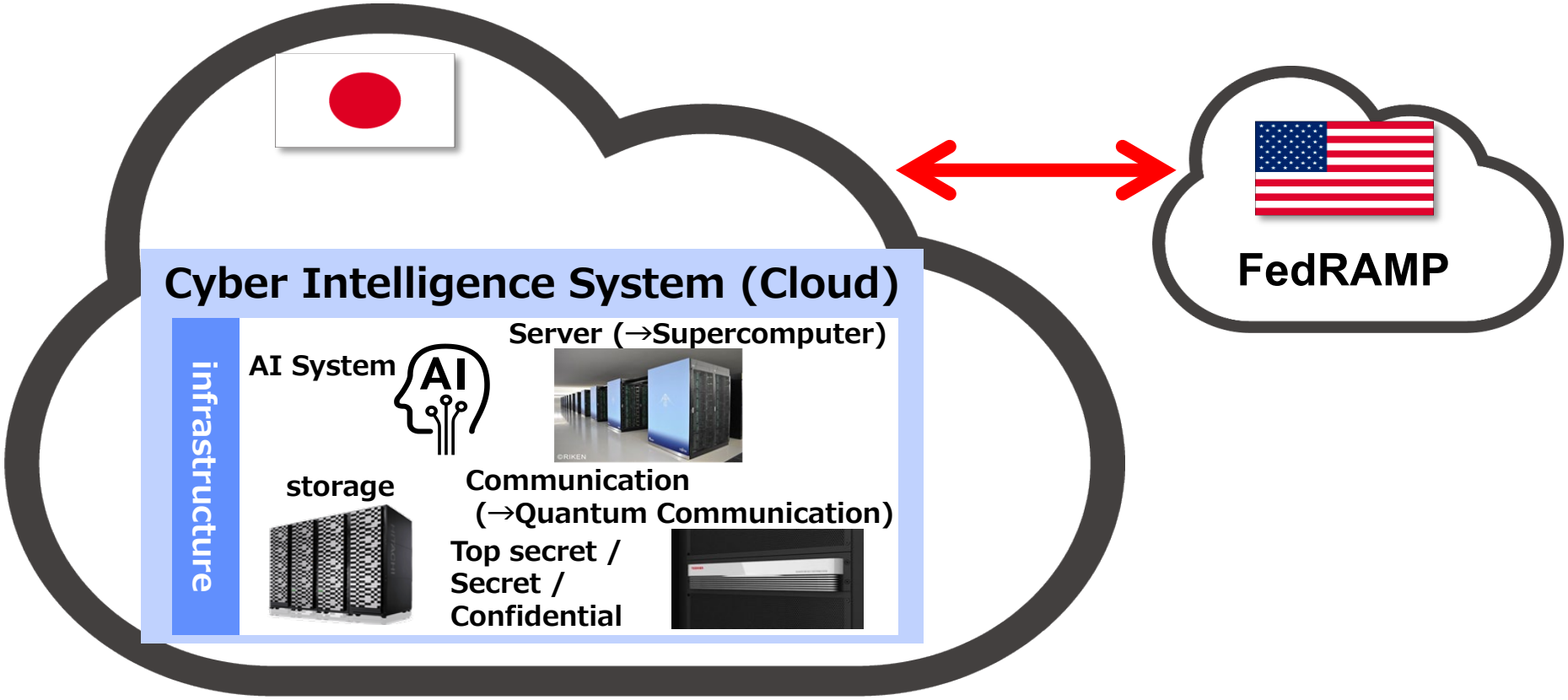
    ⇒ AI systems process the information gathered and present information that contributes to national security.



- **state-of-the-art**
  - **AI: Generating Intelligence from Data**
  - **Supercomputers: Process at ultra-high speed**
  - **Storage: Stores OSINT data**
  - **Communication: Quantum communication ensures security**

4. National Cyber Intelligence System in Japan

- National Cyber Intelligence System Needs to be Enabled by Government Cloud
- In order for Japan to participate in the Five Eyes Give & Take information sharing framework, it is necessary for Japan to develop the equivalent of the FedRAMP (Cloud Security Accreditation System) in the United States.



4. National Cyber Intelligence System in Japan

point of view	How it is done in the U.S.	Specific things to do in Japan
Protecting People	PIV (Personal Identity Verification) FICAM (Federal Identity, Credential, and Access Management)	Classify who should and should not know information → Establishment of security clearances
Protecting Data	Principles of Need to Know Classified / Unclassified CUI (Controlled Unclassified Information)	Classify the information which should be known and which should not be known → Revision of data classification
Protecting the System	FedRAMP* (also looking at Zero Trust)	Government Cloud Certification System → Revision of ISMAP*.

ISMAP : Information system Security Management and Assessment Program
FedRAMP : Federal Risk and Authorization Management Program

Contents

1. Challenges facing Japan
2. Attribution Overview
3. Five Eyes and U.S. Situation
4. National Cyber Intelligence System in Japan
5. Summary

5. Summary

- In the Ukraine situation, Russia spread disinformation that the U.S. and Ukraine are producing biological weapons. Without a National Cyber Intelligence System to defend against such disinformation, cyber attacks from Russia cannot be prevented.

- In the event of a contingency in Taiwan, it would be impossible to detect an attack from the PLA due to the lack of rapid information sharing between Japan and the U.S. regarding national security matters without a National Cyber Intelligence System, despite the Japan-U.S. alliance.

- Without a National Cyber Intelligence System in Japan, we would not be able to share information quickly with Five Eyes and others, and we would be left out of the circle.

- The absence of a National Cyber Intelligence System in Japan is an issue of most importance concerning Japan's very existence.

5. Summary

- In order to further deepen the Japan-U.S. alliance, there is an urgent need to develop a National Cyber Intelligence System in Japan immediately.

- With regard to "protecting people," "protecting data," and "protecting systems" in Japan’s National Cyber Intelligence System, we need a system that can work with U.S. systems on an equal footing.

- Only by developing a Japanese National Cyber Intelligence System equal to the U.S., Japan can enter the Five Eyes framework, which will enable information sharing related to national security among nations.