The Present and The Future ISAC in Taiwan

TWNCERT

(National Center for Cyber Security Technology)

Outline

- The Present: G-ISAC
- The Future: N-ISAC
- Tasks for the Future

The Present: G-ISAC

Framework of Government ISMS

5 Perspectives / 30 Key Services

Early Warning
- Honeypot R&D and Deployment
- Botnet Tracing
- GSN Backbone Intel. Gathering
- **Domestic Intel Exchange**
- **International Intel Exchange**
- Threat and Alert Light

G-ISAC

Incident Response
- 2nd Tier G-SOC for Co-defense
- Incident Handling
- Alert Projects for National Celebrations
- Special Projects for Critical Incidents
- Digital Forensic Services

System Security
- National Software Asset Control Database
- IT System Defense Baseline
- Government Configuration Baseline
- Secure Software Development
- Penetration Testing
- Cyber Health Check
- Cyber Offensive and Defensive Exercise
- Government Mobile App Security Test

Mgmt Process
- Agency Responsibility Ranking
- IT System Risk Classification
- Annual Government IS Audit
- Security Governance Maturity and Defense Index

Awareness Training
- Training of IT/IS Officials
- Certification of IT/IS Officials
- IS Competence Training Certification/Accreditation Scheme
- Awareness Raising Workshop
- IS Legal Case Study Booklet

Situation Awareness

Detection Rules
Alert Intelligences

Incident Tickets
Security Logs

Incident Response Services

Incident Report

System Security Services

System Security Status

Customized Controls

Management and Audit Results

Training and Campaigns

Test and Accreditation

3,372 Agencies

Security Appliances

SIEM Platform

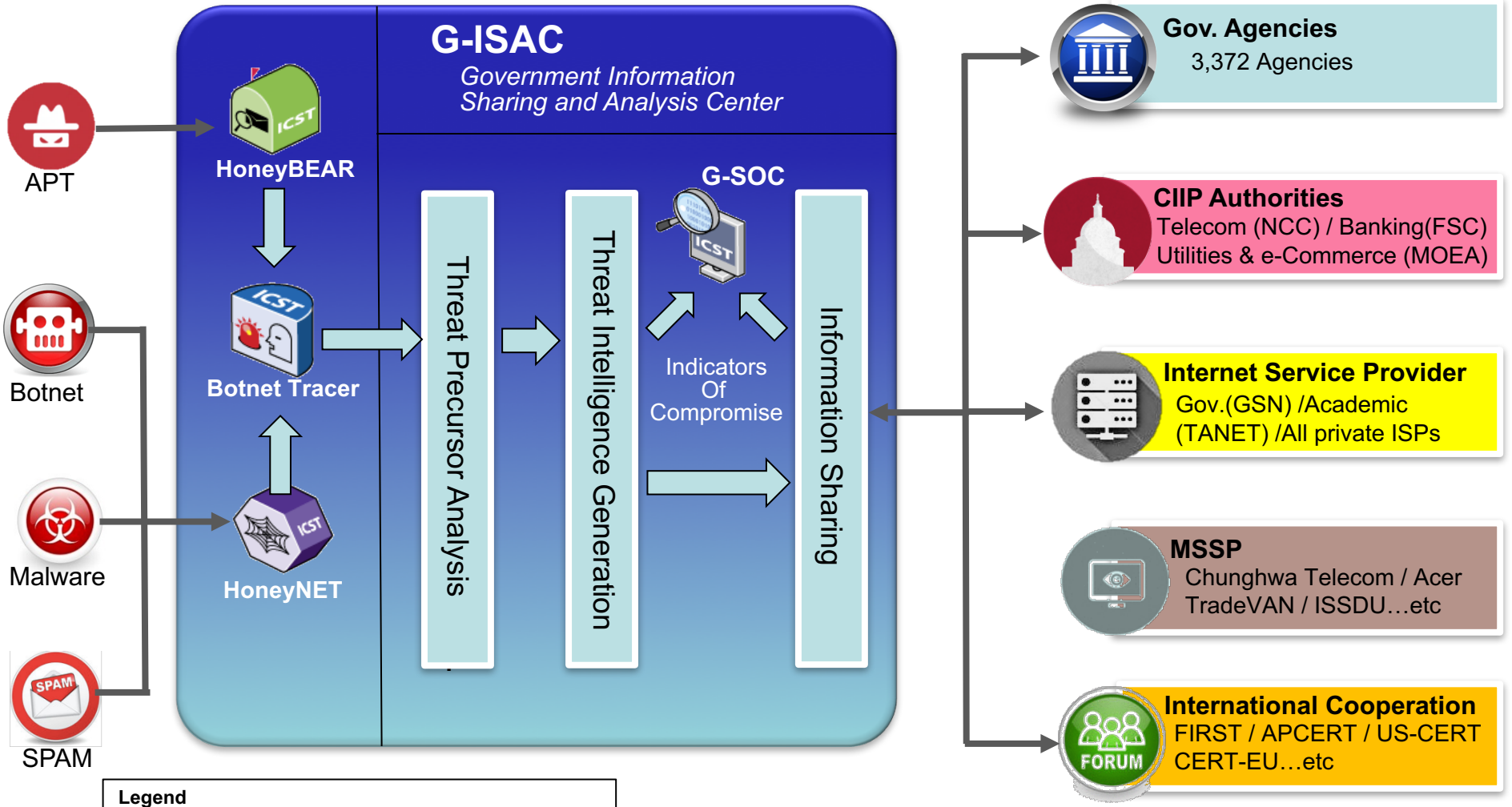
Point of Contact CSIRT Team

IT Assets

ISMS

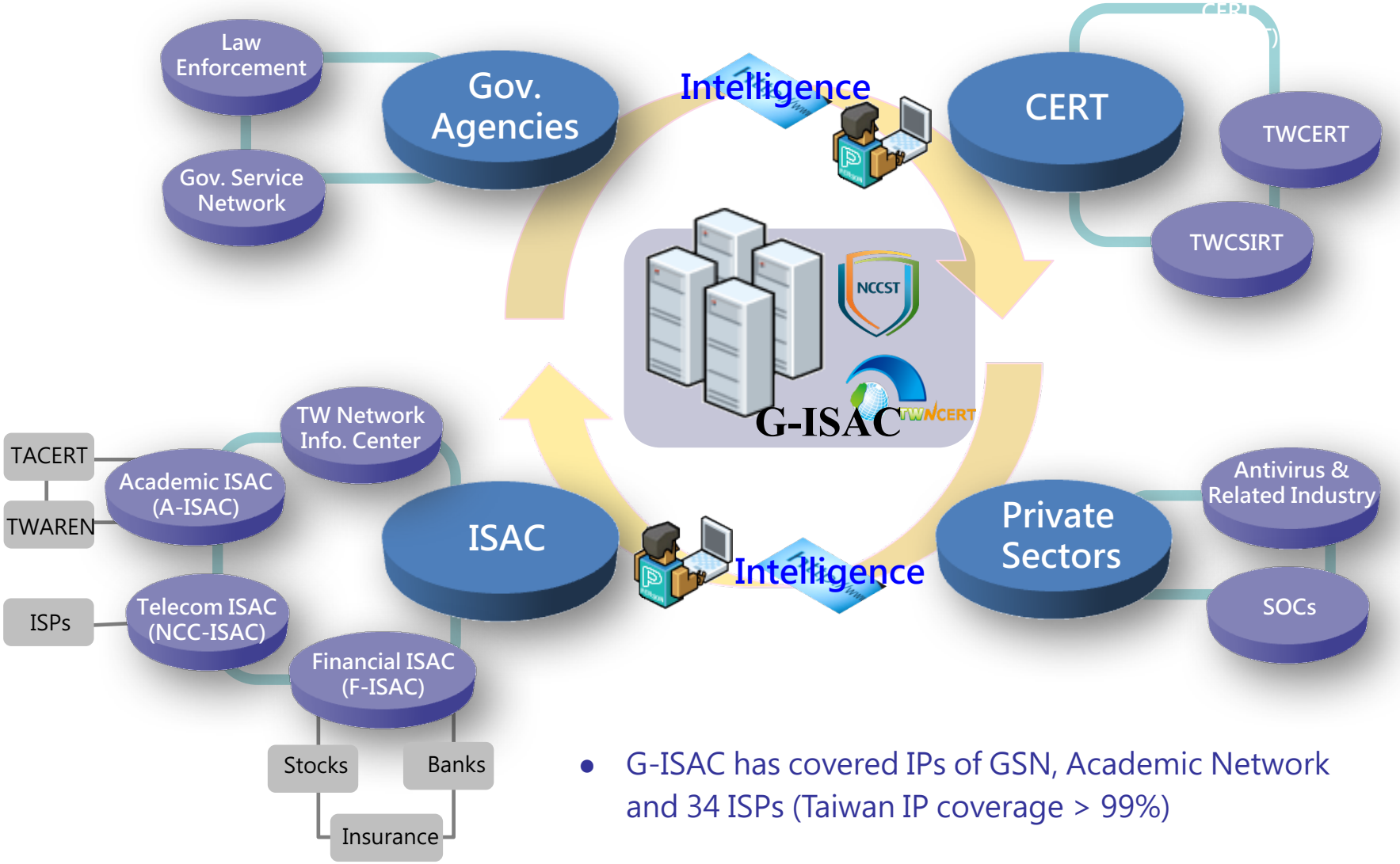
Government Officials

G-ISAC for Early Warning



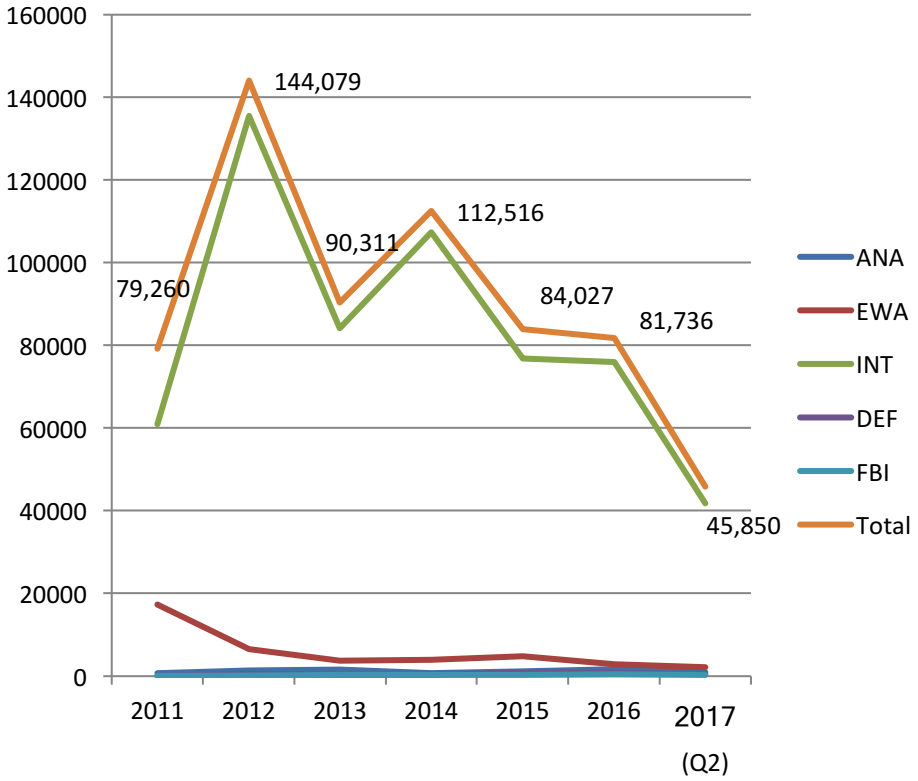
Legend
HoneyBEAR: Behavior-based Email Anomaly Reconnaissance
NCC：National Communication Commission
FSC：Financial Supervisory Commission
MOEA：Ministry of Economic Affairs
GSN：Government Service Network
MSSP: Managed Security Service Provider
FIRST: Forum for Incident Response and Security Teams

G-ISAC Intelligence Sharing



- G-ISAC has covered IPs of GSN, Academic Network and 34 ISPs (Taiwan IP coverage > 99%)

Domestic Information Sharing Status



	2011	2012	2013	2014	2015	2016	2017 (Q2)
ANA	720	1,432	1,646	756	1,222	1,686	1,045
EWA	17,327	6,455	3,710	3,865	4,782	2,944	2,174
INT	60,980	135,527	84,210	107,405	76,757	75,915	41,803
DEF	69	507	407	225	867	755	594
FBI	164	158	338	265	399	455	234
Total	79,260	144,079	90,311	112,516	84,027	81,736	45,850

From： 2011/1/1 ~ 2017/6/30

Current Situation Review

- Public-Private-Partnership now is weighted more on public sectors
- There are only four ISACs established in Taiwan (G-ISAC, NCC-ISAC, F-ISAC and A-ISAC), although all operate and collaborate smoothly, but the sector coverages are limited

The Future: N-ISAC

The Fifth National IC Security Development Plan (Draft)

National Security

1. Develop national cyber security risk assessment mechanism
2. Establish national network and communication emergency recovery mechanism
3. Build national network defensive and offensive capabilities

Cyber Security Management

4. Complete national cyber security policies, regulation & standards
5. Enhance cyber security defense among gov. and CI & CII sectors
6. More International collaborations
7. Increase cyber crime prevention and solve effectiveness

Industry Development

8. Promote related policies and development of cyber security industries
9. Reduce cyber security risks for industry supply chains

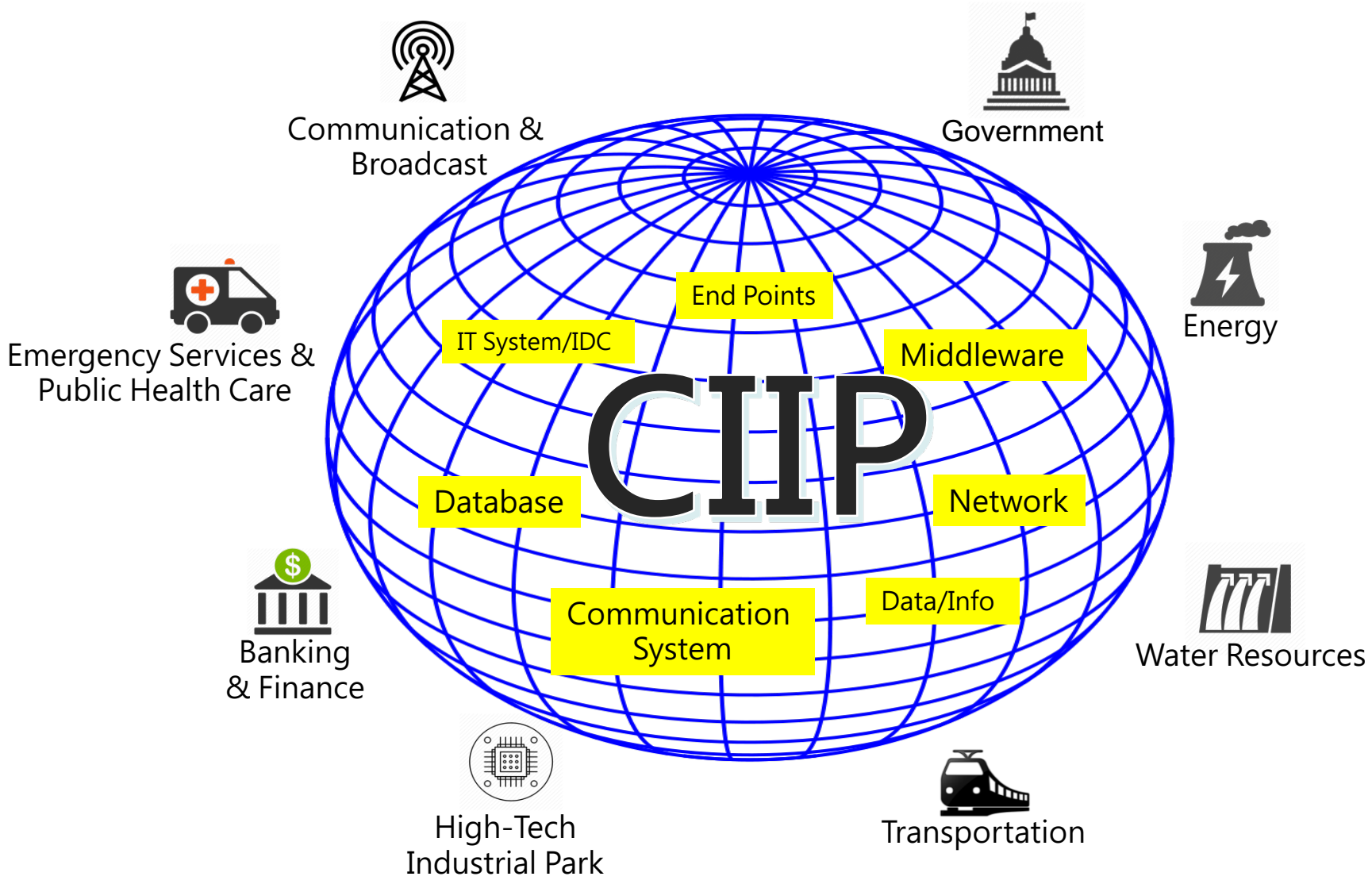
Technology R&D

10. Combine and raise the values of academic and industrial cyber security R & D capabilities
11. Develop a privacy protected digital identification framework

Talent Incubation

12. Perfect the incubation and demand of cyber security professionals
13. Promote cyber security awareness and child online protection

Critical Infrastructure Sectors



National Cyber Security Defense

- Push all 8 CI & CII Sectors to complete 4 aspects of cyber security domain in order to establish intelligence-based National Cyber Security Defense Framework

4 Aspects

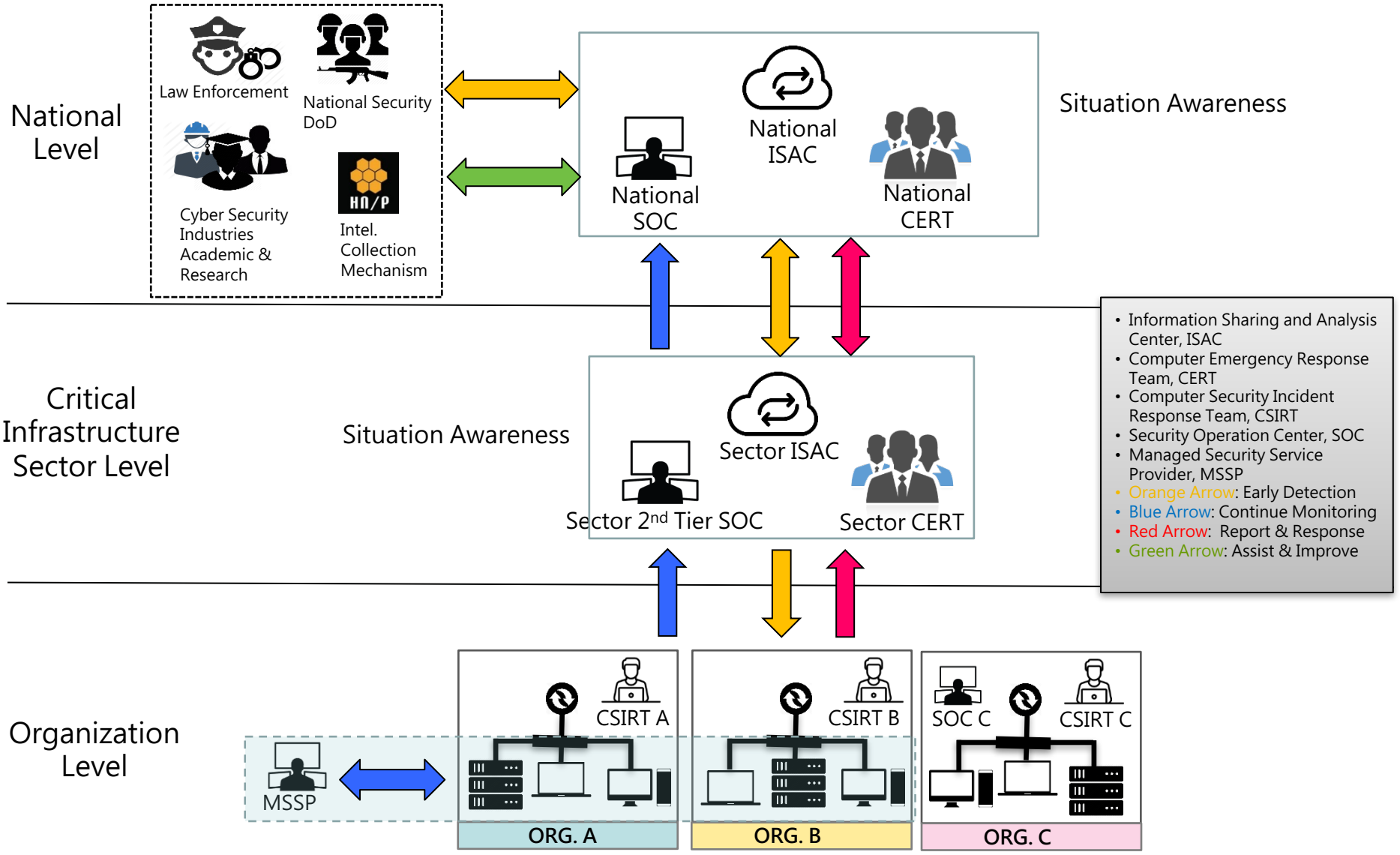
X

8 Sectors

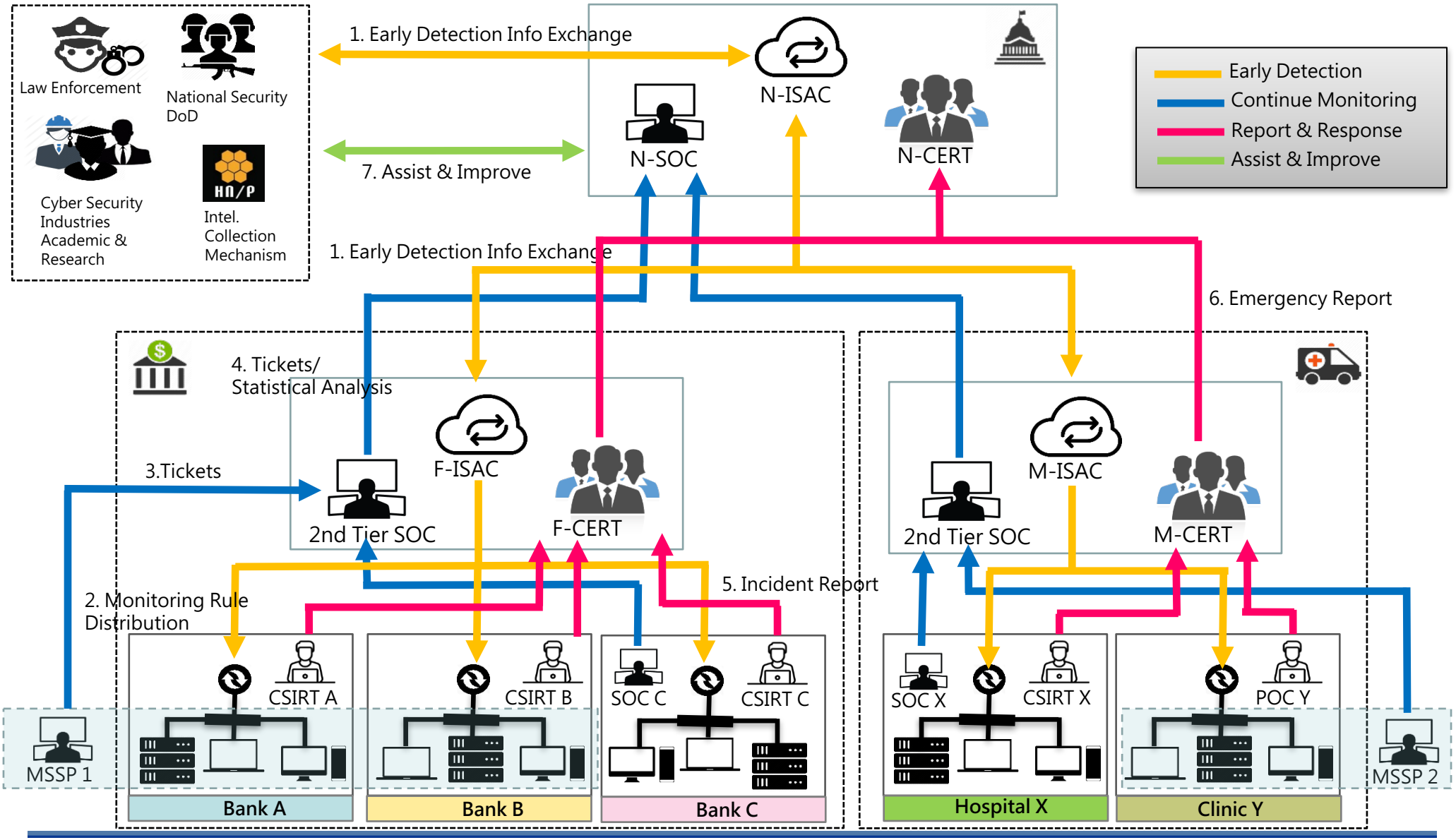
=

National Cyber Security Defense Framework

Roles and Relations



How It Works?



Tasks for the Future

- Establish the promote organization, strengthen the capabilities of ISACs, CERTs and SOCs
  - Establish CI & CII cyber security guidance and promotion group, assist competent authorities to establish sector cyber security taskforce
  - Expand capabilities of G-ISAC, CERT and G-SOC to become National ISAC, CERT and National SOC, and promote CI & CII sectors to establish sector ISACs and sector CERTs
- Develop Cyber Security Laws & Regulations
  - Promote to legislate Information and Communication Security Management Act
  - Develop Critical Infrastructure Cyber Security Management Baseline
  - Develop national standards for national cyber security defense technologies, management, and maturity evaluations
- Strengthen Cyber Security Professional Development and R&D Capabilities
  - Promote cyber security professional certification systems and training programs in order to incubate talents needed for national cyber security defense
  - Integrate the power of industries and academic & research facilities, to develop technical solutions needed for national intelligence integration and cyber security defense framework

Thank You