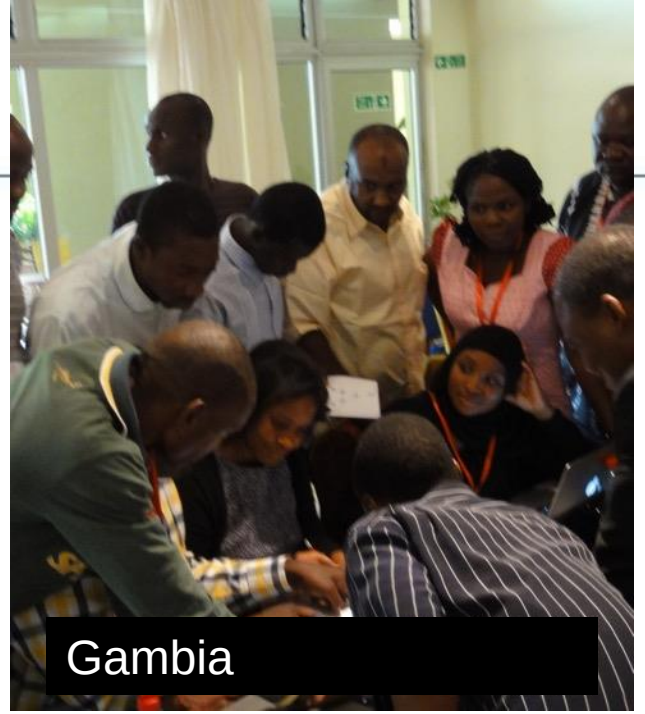
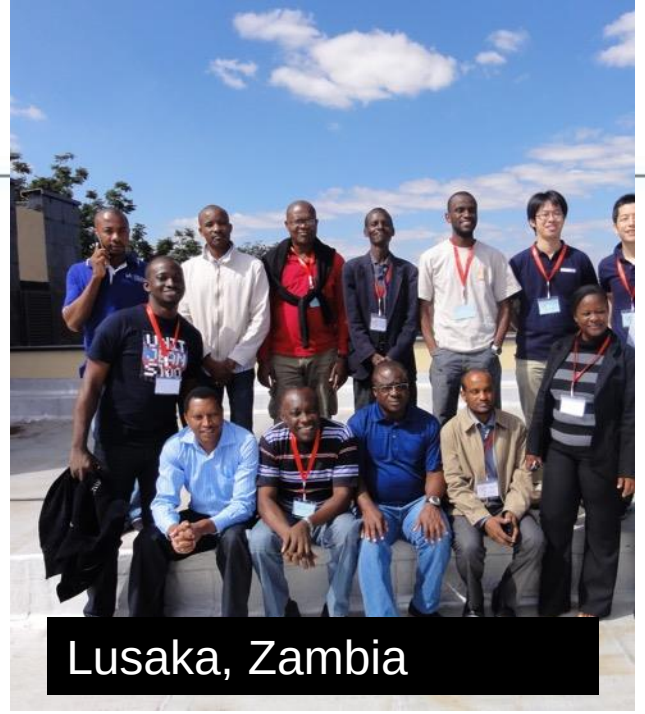
Enhancing national cybersecurity frameworks with international cybersecurity standards

Dr. Koichiro Sparky Komiyama
JPCERT/CC
Director, Global Coordination Division

ITU-T SG17 Mini Workshop on ITU-T X.1060
February 2024



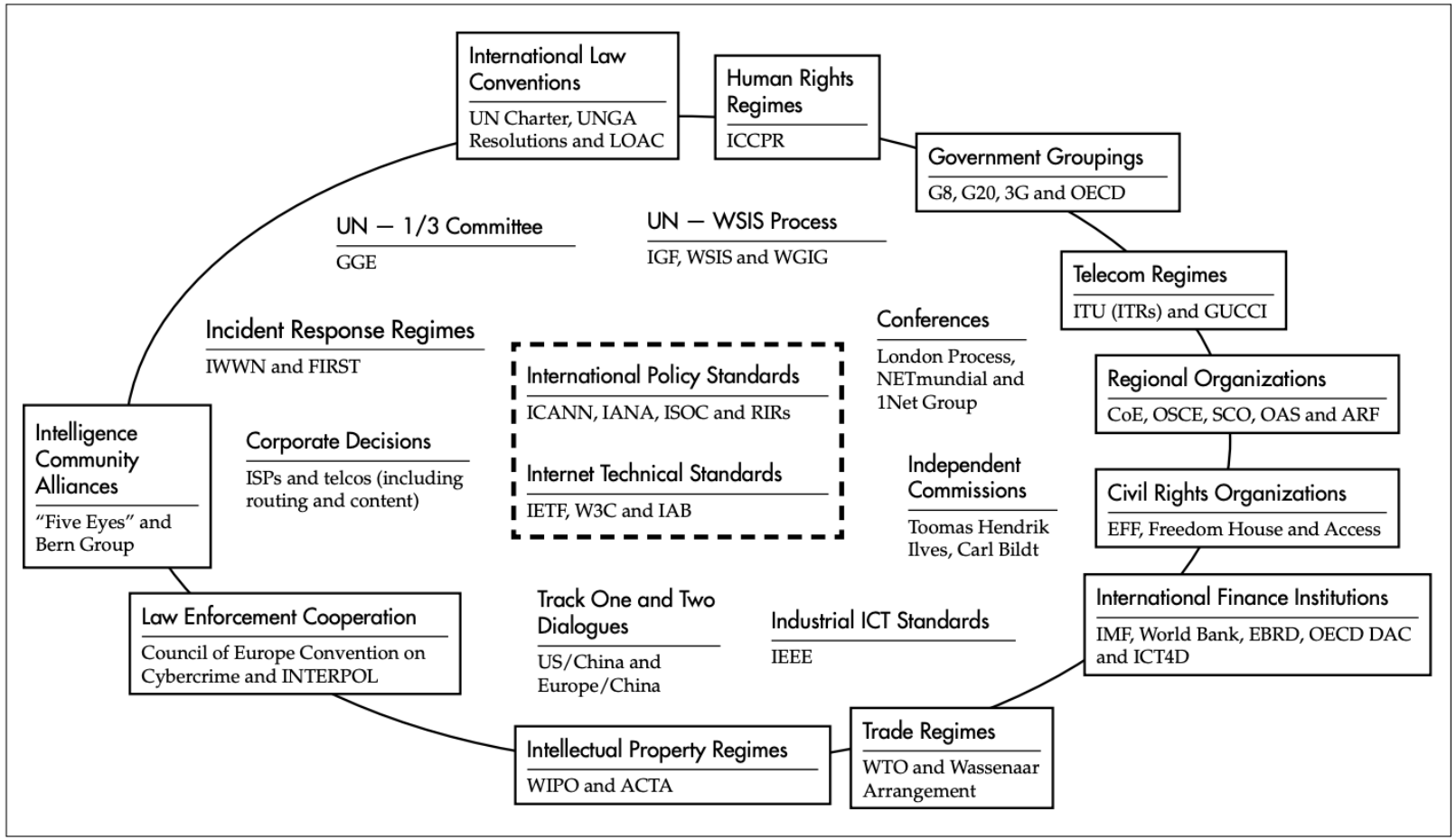


- JPCERT/CC's CSIRT capacity building initiative kicked off in 2009-10.
  - Asia, Pacific island, and Africa

It is not just a technical problem.

- As political science scholars pointed out in 2014, the Regime Complex is still a valid concern for securing cyberspace.
- **Governmental, National and International**
  - *The needs for cooperation 1)within government, 2)with international partners, 3)with Whole of Nation* (Klimburg, Alexander, ed. 2012. *National Cyber Security Framework Manual*. NATO CCD COE Publications.)

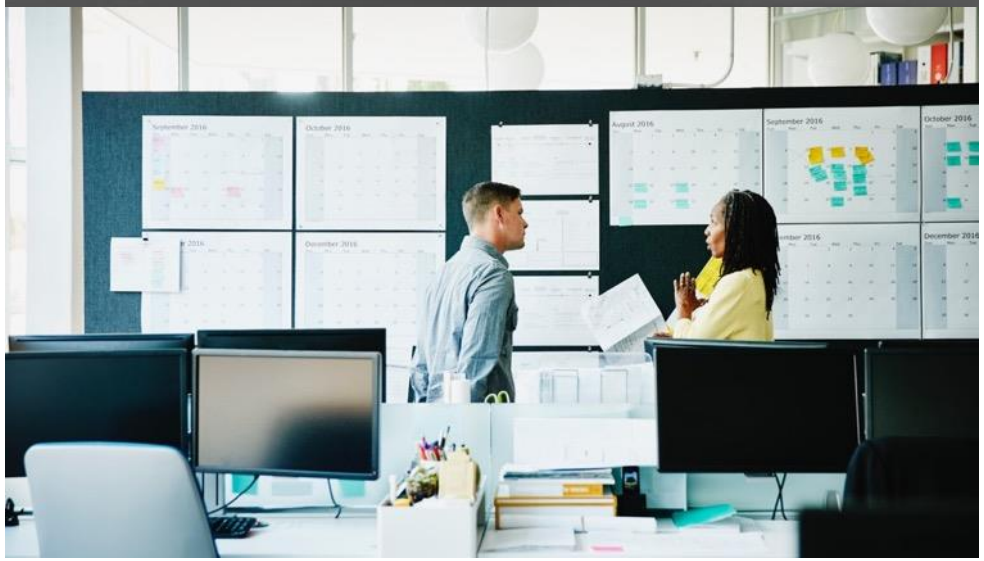
Figure 1: The Regime Complex for Managing Global Cyber Activities



- Nye, Joseph S. 2014. "The Regime Complex for Managing Global Cyber Activities." *Center for International Governance and Innovation (CIGI) Publications* (1): 1–15.

What we see in the field

- *Regional Cooperation is becoming more prominent.*
  - *AfricaCERT / AU*
  - *OIC-CERT*
  - *APCERT / ASEAN Regional CERT*
- Some are regressing
- Diverse stakeholders
  - National Cyber Security Center
  - CSIRT(National, Product, Private, Regional)
  - ISAC (Sectoral, Regional)
  - SOC (National, Private)
  - Academia
  - LE/Police/Justice
  - Military/Intelligence



Framework enables you to do:

1. A jump start
2. More comprehensive approach

ITU-T X.1060 Cyber Defence Centre

- ITU-T standardize it as X.1060 in 2021.
- **CSIRT + SOC + Strategy = Cyber Defence Centre**
- 64 different services in nine different categories


ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

X.1060
(06/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Security management

Framework for the creation and operation of a cyber defence centre

Recommendation ITU-T X.1060

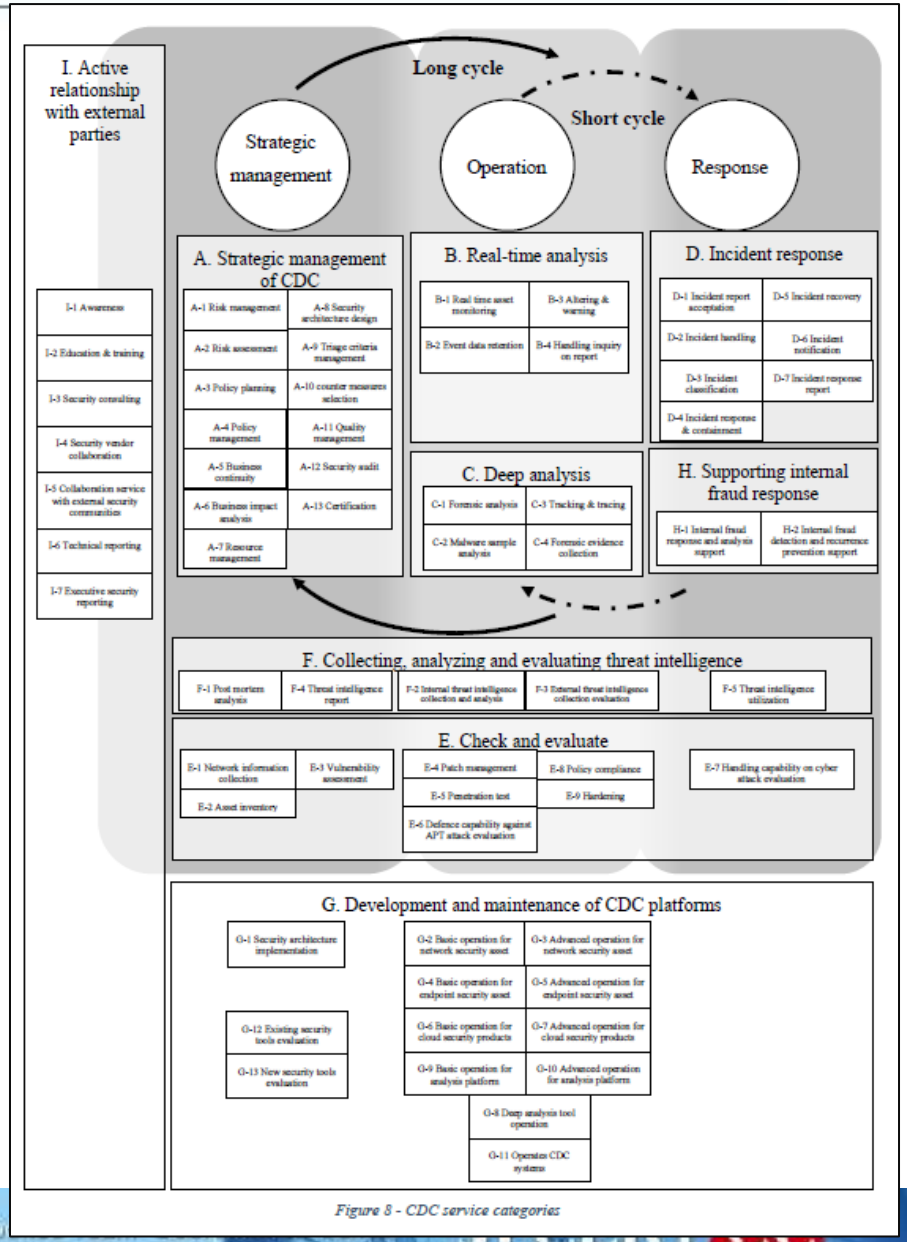


Figure 8 - CDC service categories

Division of roles (Japan)

- No single organization can serve 64 different responsibilities.
- viewed at the national level, the measures have become a patchwork

			Players/Stake holders									
	Category	Work Items	NCSC	National CSIRTs	PSIRT	Private CSIRTs	LE/Justice	ISAC	National SOC	Private SOC	Academia	Certificate Vender
Services	A) strategic management of CDC;	A-1. Risk management The risk management service is to achieve	10						7			3
	B) real-time analysis;	B-1. Real time asset monitoring The real-time asset			10	10	2		10	10		
	C) deep analysis;	C-1. Forensic analysis The forensic analysis service analyses digital	5	8	10	10				8	10	
	D) incident response;	D-1. Incident report acceptance The incident report	5	10	9	10			10			
	E) checking and evaluation;	E-1. Network information collection The network information					2			10	7	
	F) collection, analysis and evaluation of threat intelligence;	F-1. Post-mortem analysis The post-mortem analysis service describes resolution		10	5	10	8			10	5	
	G) development and maintenance of CDC platforms;	G-1. Security architecture implementation The security architecture		5		2			7	7		
	H) support of internal fraud response;	H-1. Internal fraud response and analysis support The internal fraud response					9		5			
	I) active relationship with external parties.	I-1. Awareness The awareness service is to precisely create awareness	5	5	5	3		10				

Division of roles (case of US)

- Private sector
  - help shape policies
  - shoulder much of the technical work

			Players/Stake holders									
	Category	Work Items	NCSC	National CSIRTs	PSIRT	Private CSIRTs	LE/Justice	ISAC	National SOC	Private SOC	Academia	Certificate Vender
Services	A) strategic management of CDC;	A-1. Risk management The risk management service is to achieve	10		1	1	3	1				3
	B) real-time analysis;	B-1. Real time asset monitoring The real-time asset	9		10	10	2			10		
	C) deep analysis;	C-1. Forensic analysis The forensic analysis service analyses digital	5	8	10	10	2			8	10	
	D) incident response;	D-1. Incident report acceptance The incident report	10	1	9	10	2					
	E) checking and evaluation;	E-1. Network information collection The network information	8	2			2			10	7	
	F) collection, analysis and evaluation of threat intelligence;	F-1. Post-mortem analysis The post-mortem analysis service describes resolution	9		9	10	8	1		10	5	
	G) development and maintenance of CDC platforms;	G-1. Security architecture implementation The security architecture	8	5		2				7		
	H) support of internal fraud response;	H-1. Internal fraud response and analysis support The internal fraud response					10					
	I) active relationship with external parties.	I-1. Awareness The awareness service is to precisely create awareness	7	4	7	3		10				

Division of roles (case of Singapore)

- authorities and responsibilities are concentrated in the Cybersecurity Agency.
- outsources fewer tasks than the United States.

			Players/Stake holders									
	Category	Work Items	NCSC	National CSIRTs	PSIRT	Private CSIRTs	LE/Justice	ISAC	National SOC	Private SOC	Academia	Certificate Vender
Services	A) strategic management of CDC;	A-1. Risk management The risk management service is to achieve	10						7			3
	B) real-time analysis;	B-1. Real time asset monitoring The real-time asset	4			10	2		10	10		
	C) deep analysis;	C-1. Forensic analysis The forensic analysis service analyses digital	9			10				8	10	
	D) incident response;	D-1. Incident report acceptance The incident report	10			10			10			
	E) checking and evaluation;	E-1. Network information collection The network information	8				2			10	7	
	F) collection, analysis and evaluation of threat intelligence;	F-1. Post-mortem analysis The post-mortem analysis service describes resolution	10			10	8			10	5	
	G) development and maintenance of CDC platforms;	G-1. Security architecture implementation The security architecture	8			2			7	7		
	H) support of internal fraud response;	H-1. Internal fraud response and analysis support The internal fraud response					9		5			
	I) active relationship with external parties.	I-1. Awareness The awareness service is to precisely create awareness	4			3		10				

Summary

Still in its early stages, X.1060 standard proves effective for organizing the roles of the government, private sector, and academia in Japan, the United States, and Singapore.