

CSIRT Capacity-Building and the Private Sector: A Universal Standard

By Vanessa Collins, Chen Han, Carrie Jabs,
Amanda Tobey, and Adalberto Trujillo

May 6,
2021

Bottom Line Up Front

CSIRTs, also known as **Computer Security Incident Response Teams**, are dedicated groups that handle national computer security incidents.

- critical to **protect and defend** national internet communication technology.
- Poor integration and information-sharing with Private-Sector partners

A Universal Standard will be created that will consist of a working group and will be managed by the International Telecommunications Union to promote CSIRT private-sector cooperation.

Environmental Framing

Current State

Intelligence

There is no effective communications plan and protocol between the government and private sectors for information sharing and build up trust.

Military

There are very few cyber government-private sector information sharing platforms to receive incident information from CSIRTS. The military has poor relations with private sector and poor domestic-level response capabilities.

Financial

Minimal collaboration between government and private sector to better protect global financial systems and infrastructure from cyber criminals

Information

Programs have been established that can be leveraged for collaboration between public and private stakeholders.

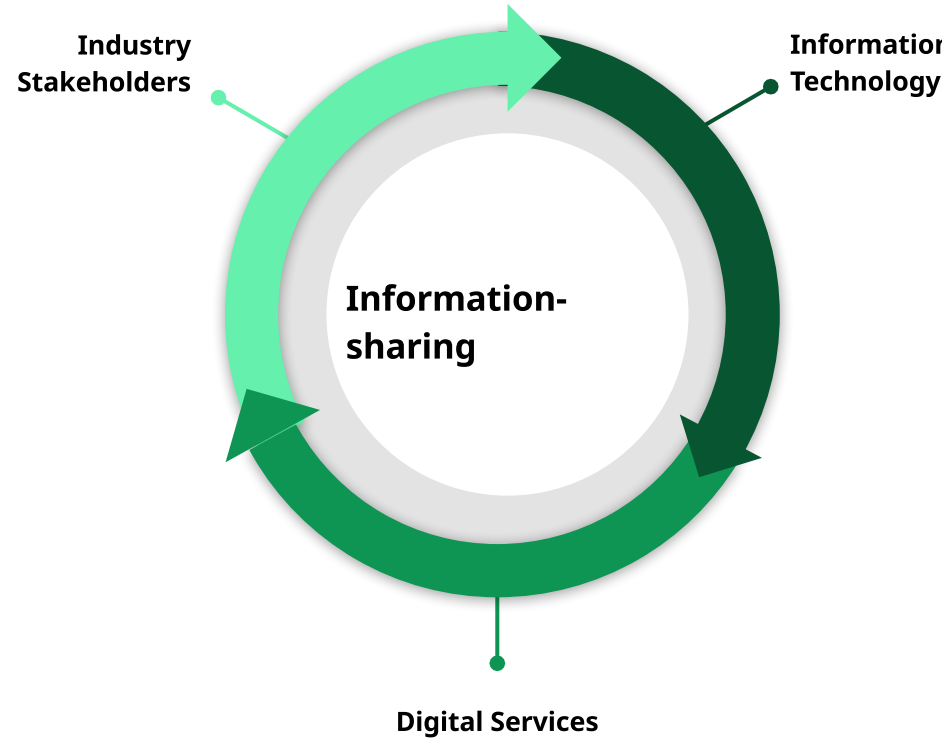
Law Enforcement

Investigations are impacted due to lack of information sharing. There are not enough resources to effectively participate in the establishment of a new CSIRT.

Desired End State

A CSIRT that has private sector engagement built into its DNA and has effective local and global information sharing partnerships.

Problem Statements



Overview

Military



The focus of the military IOP is to oppose external coercion and win conflict through the application of force or threat of force to compel an adversary or protect the nation from force.

Information



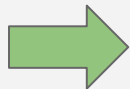
The focus of the information IOP is to affect decision making in the cognitive, informational, and physical dimensions of the target audience—whether friendly, neutral, or adversary—to create a desired effect.

Finance



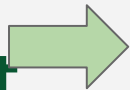
The focus of the Financial IOP is to protect financial services infrastructure and prevent intentional or unintentional funding of cyber criminal activity.

Intelligence

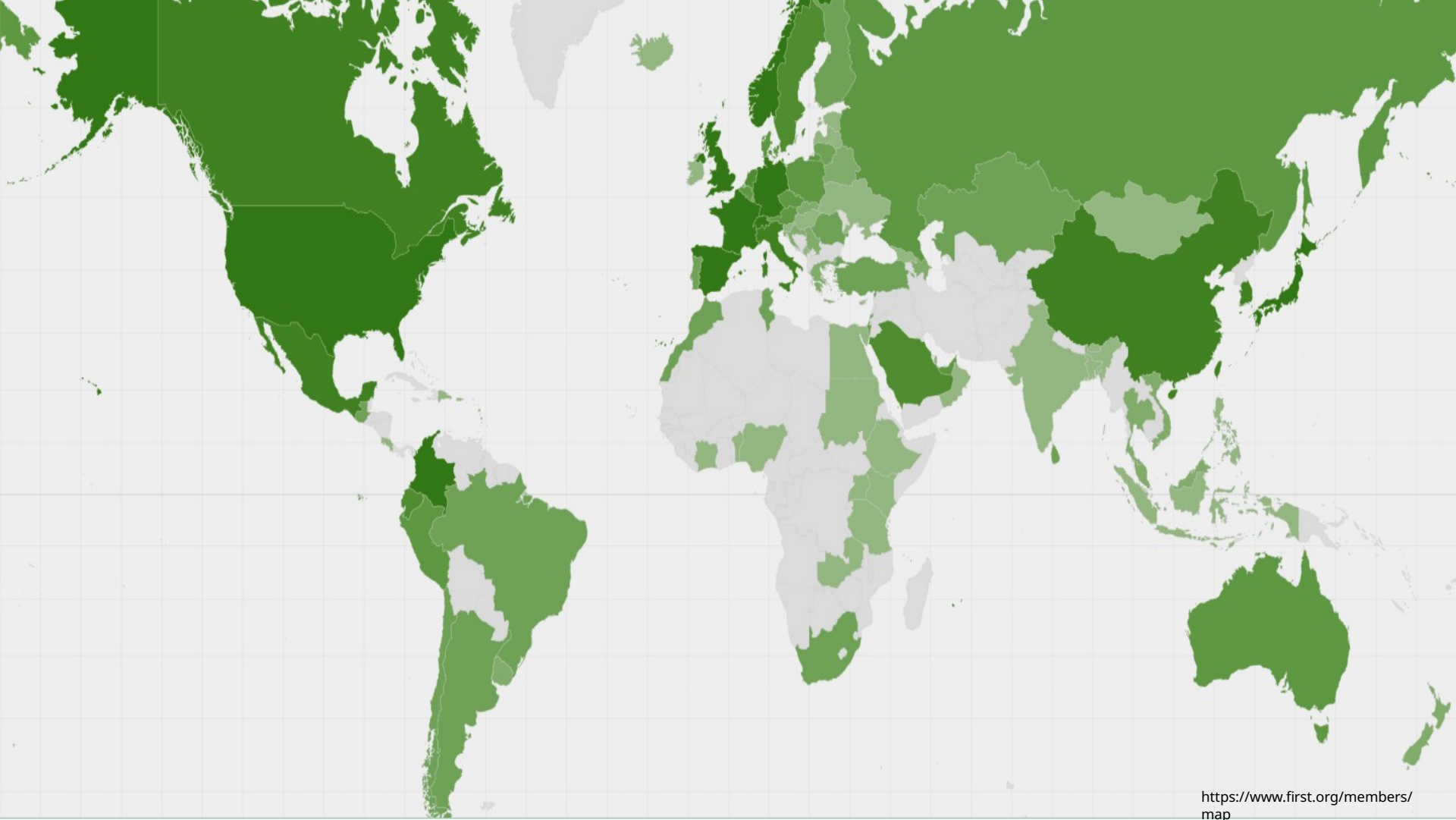


The focus of the intelligence IOP is the production of value-added data for the decision maker to make informed decisions.

Law Enforcement



The focus of Law Enforcement IOP is prosecute crimes and conduct activities at the tactical level through the military IOP or local law enforcement.

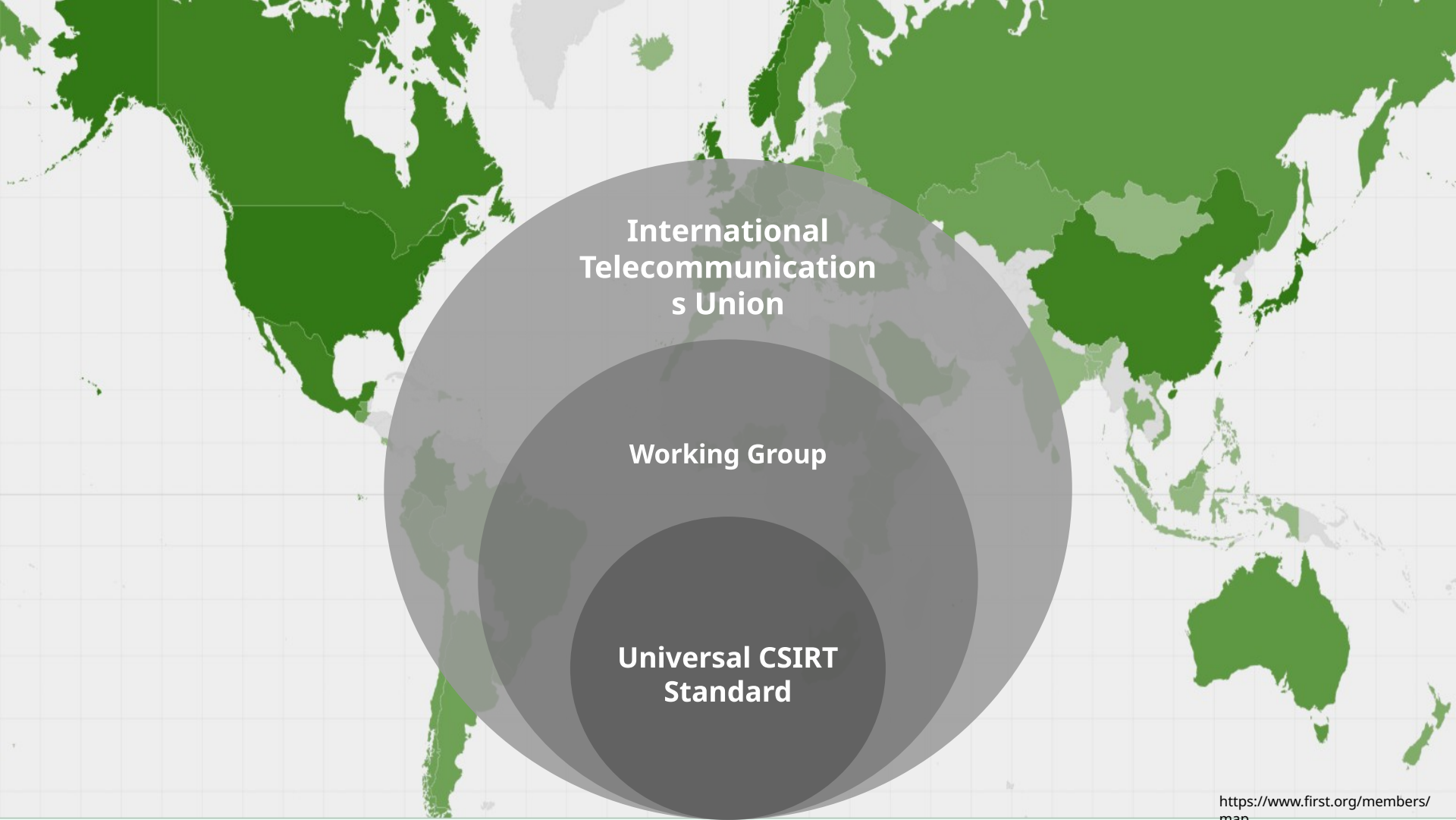


Diplomatic Framing

A world map with a green overlay, showing the distribution of organizations and stakeholder countries. The overlay is a semi-transparent green rectangle with rounded corners, centered over the Atlantic Ocean and parts of Europe, Africa, and the Americas. The map is overlaid with a light gray grid.

Organizations

- ITU
- US-CERT
- EU-CERT
- AfricaCERT
- Stakeholder Countries
 - Nigeria
 - Philippines
 - South Africa



**International
Telecommunication
s Union**

Working Group

**Universal CSIRT
Standard**

Military Problem Statement

The military **does not reliably share information** with the private sector, particularly around cyber threats.

Since CSIRTs are first-line responders, it is important to **incorporate private sector and military perspectives** in their conception

Working Group Organizations

- NATO's Cyber Defence Rapid Reaction Team
- International Defense Contractors
- U.S. National Guard Members

Military LOE

The Military is important to the Universal Standard because much of the information CSIRTs gather from the private sector is needed by the military.

Why?

Representation from Military and Private Sector stakeholders is important to build a CSIRT that can share important information across the government

Universal Standard

Escalation Ladder- Guidance for what is and is not a military issues

Framing for different types of military institutions

Recommended legal protections

The relationship formed between the CSIRT and Private-Sector is key to national-security so CSIRTs, private sector companies, and the Military will regularly coordinate for cyber capacity building and crisis prevention,.

Information Problem Statement

- Cooperation, Integration and Coordination between information sharing communities and networks have been ineffective.

Orgs

- European Union Agency for Cybersecurity (ENISA)
- Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)



Why?

- Information sharing is essential to the protection of critical infrastructure and to furthering cybersecurity for the nation.

Universal Standard

- Develop partnerships and share substantive information with the private and public sector.
- Share information with state, local, tribal, and territorial governments and with international partners.

Information LOE

- The informational instrument deals with both the protection of information and the distribution of information.

Financial Problem Statement

- Cyber criminal activity with significant impacts to the global financial sector in increasing

Financial Sector Partner Organizations

- Financial Services - Information Sharing and Analysis Center (FS-ISAC)
- Bank of International Settlements (BIS)
- International Monetary Fund (IMF)
- United States Secret Service Cyber Fraud Task Force (CFTF)
- United States Treasury - Financial Crimes Enforcement (FinCEN)



Why?

- An information sharing program will provide smaller and less financially established countries to gain earlier access to information and resources that can help protect them from the consequences of cyber criminal activity

Universal Standard

- Develop and strengthen key areas needed
- Align stakeholders across public and private sectors
- collaborate on and implement best practices related to the protection of the financial services and the systems and technologies it uses.

Financial LOE

The Financial IOP deals with intercepting and preventing cyber criminals from using global financial systems and services to fund their organization and illegal operations

Intelligence Problem Statement

Enable to collect information, the agreed sharing policies and limitations of what data can be used in which context or for what form of processing must be accepted and adhered to between private sectors

Orgs

- NATO Communications and Information Agency (NCI)
- Defense Intelligence Agency (DIA)
- Cyber security and Infrastructure Security Agency (CISA)
- National Cyber security and Communication Integration Center (NCCIC)

Intelligence LOE

Collection, processing, integration, analysis, and interpretation of available information

Why?

It is important to establish a trusted information-sharing platform between government and private sector to evaluate and respond any cyber crisis.

Universal Standard

Convert disparate data about the environment, future capabilities and intentions, and relevant actors into coherent information to provide decision advantage for decision makers and policymakers

Law Enforcement- Specific Problem Statement

Enhance the sharing of cyber threat intelligence and information about attacks that private sectors are seeing to the government/law enforcement agencies.

Orgs

- FBI Cyber Division
- National Investigative Joint Task Force
- Europol
- Joint Cybercrime Action Taskforce (J-CAT)



Why?

To strengthen the CSIRT whole of the Government/Private sector and for the law enforcement to respond to and apprehend cyber criminals around the world based on the type of cyber attacks that are reported.

Universal Standard

Inform each individual country who is part of the Universal Standard and inform they should have this program so that Private sector entities can record threats and everyone who reports these threats can have access to this data. The Program will be structured around the MITRE ATT&K Framework.

Law Enforcement LOE

The Law Enforcement LOE deals with the collection of information, coordination, and the prosecution of cyber criminals.

Outcomes and Objectives

To strengthen CSIRT capacity building with the private sector and improve information sharing to combat cyber attacks.

The Universal Standard will consist with various organizations that are experienced with cyber. It will help developing countries combat and deter cyber crimes from happening.

LOE	Orgs	Objectives
Intelligence	Cybersecurity and Infrastructure Security Agency - Defense Intelligence Agency	- Integrate foreign, military, and domestic capabilities through policy, personnel, and technology actions - Provide decision advantage to policymakers, diplomats, financiers and economists, strategic communicators, warfighters, homeland security officials, and law enforcement.
Information	European Union Agency for Cybersecurity --- DHS Cybersecurity and Infrastructure Security Agency	- Shape strategy, policy, events and international perceptions. - Achieve a comparative advantage and create a desired effect in the target audience. - Enable leaders to shape or react to national or international cyber events.
Finance	Financial Svcs Info Sharing and Analysis Center US Treasury - Financial Crimes Enforcement --- US Secret Service - Cyber Fraud Task Force	- Become a member of FS-ISAC to leverage their existing global cyber intelligence sharing program for financial services - Obtain earlier access to intelligence and information, enabling the financial sector to respond quicker to cyber threats - Financial and Cyber Crimes Investigations and Cyber Task Forces
Military	NATO's Cyber Defence Rapid Reaction Team --- International Defense Contractors --- U.S. National Guard Members	- Produce SOP for escalation from Private Sector intel to CSIRT to Military - Develop frameworks for different types of Military structures - Leverage volunteer/ temporary military personnel to build Private Sector-Military trust
Law Enforcement	FBI Cyber Division's National Cyber Investigative Joint Task Force --- Europol's Joint Cybercrime Action Taskforce	- Develop cyber-threat reporting program for private-sector and government/law enforcement to use in cooperation with helping with investigations to cyber-crime. - During distribution of the Universal Standard, help countries develop cyber-threat reporting program through training and organization.

Phases

Approval

Meetings

Distribution

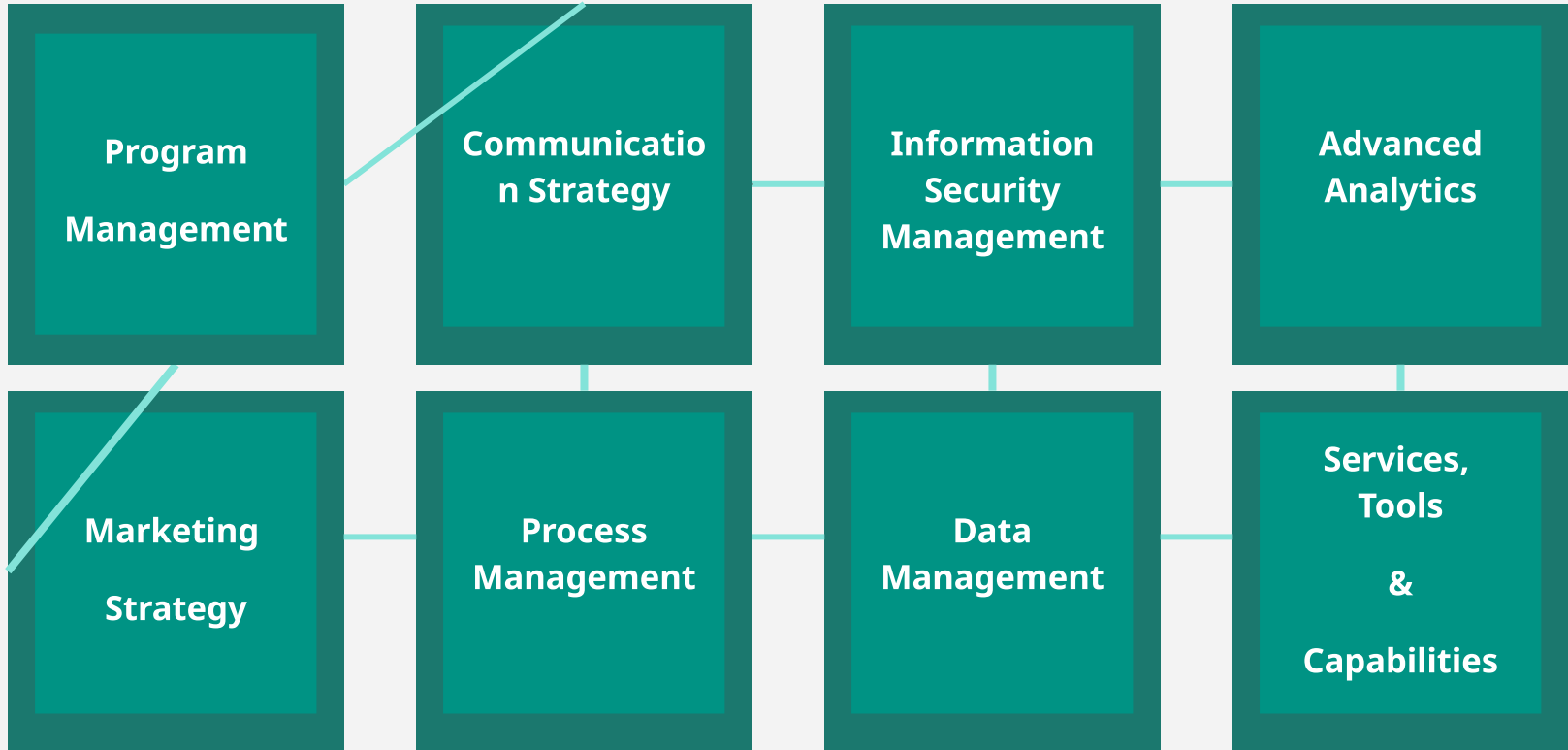


Working Group
Creation

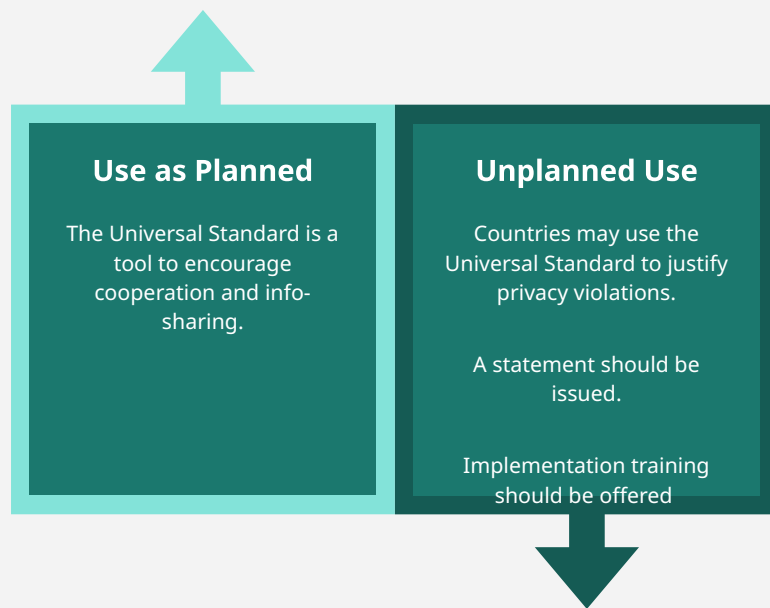
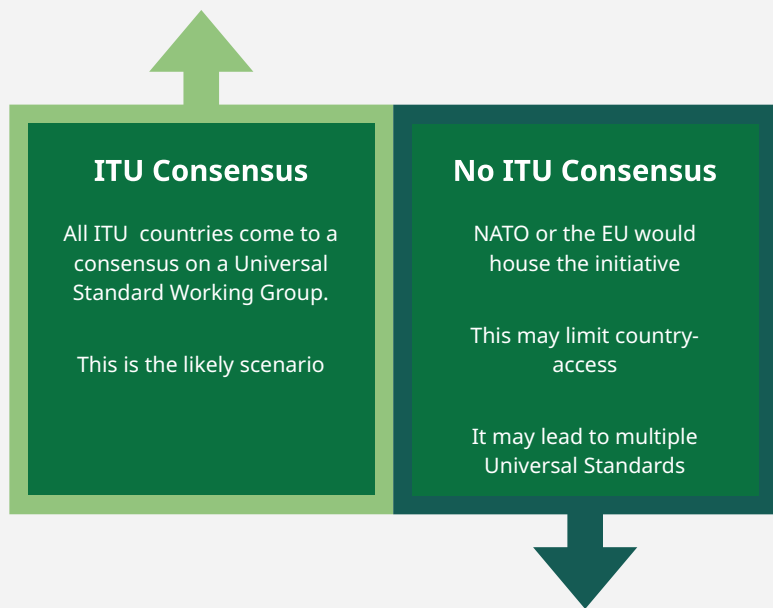
Draftin
g



Resources



Contingencies



Recap

A CSIRT Capacity building can be accomplished by using this Framework which can protect nation's internet infrastructure to cyber attacks.

Significantly improve information sharing across private sector entities and protect countries who are starting to develop CSIRT.

Universal Standard will be served as a tool to encourage private sector information sharing and assist countries who are developing CSIRTS.

The Universal Standard will also consists of a working group and will be managed by the International Telecommunications Union.

