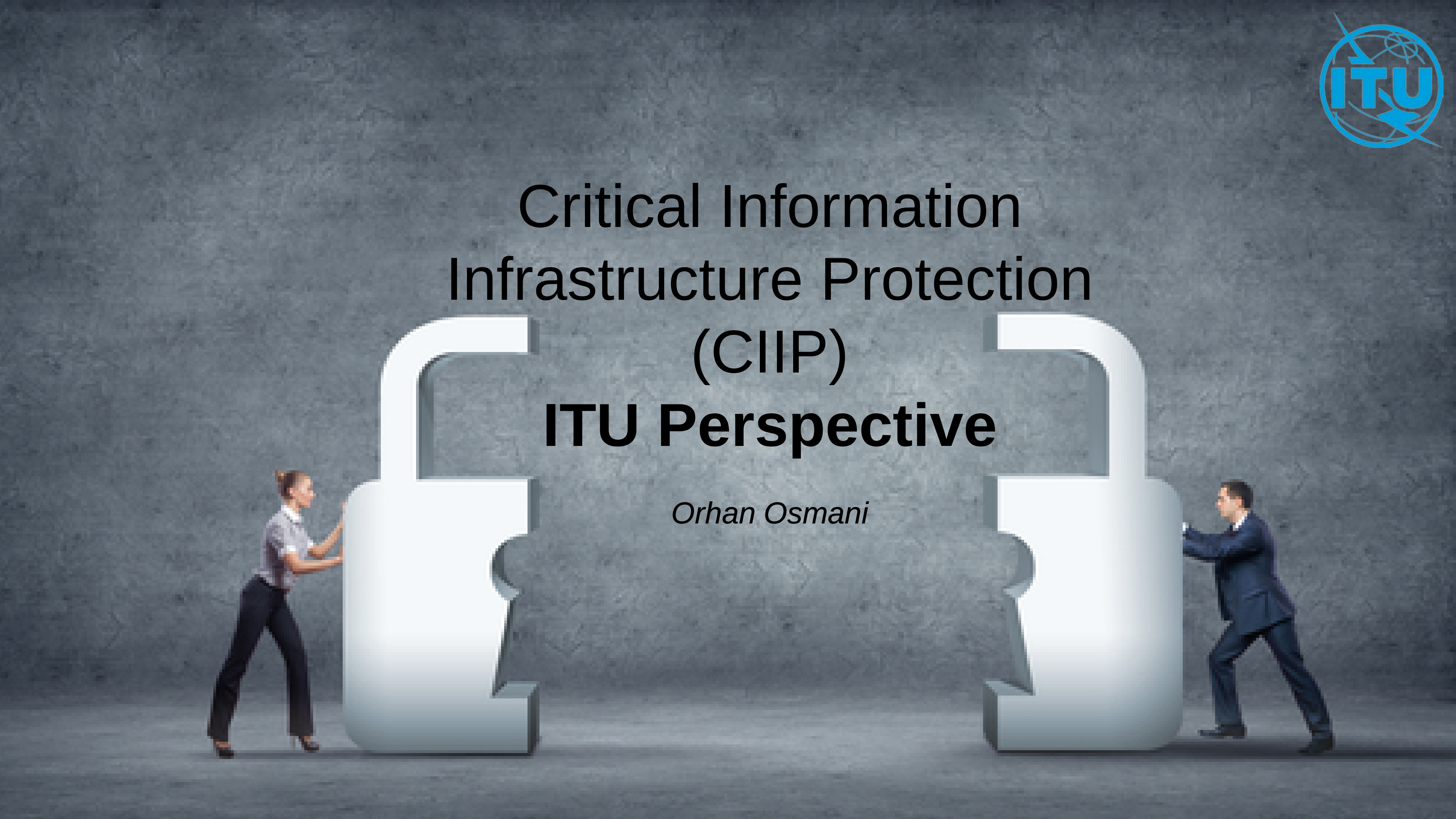


Critical Information Infrastructure Protection (CIIP)

ITU Perspective

Orhan Osmani

Critical Information Infrastructure Protection ITU Perspective

The Global Risks Report states that “Offensive cyber capabilities are developing more rapidly than our ability to deal with hostile incidents”

WORLD ECONOMIC FORUM

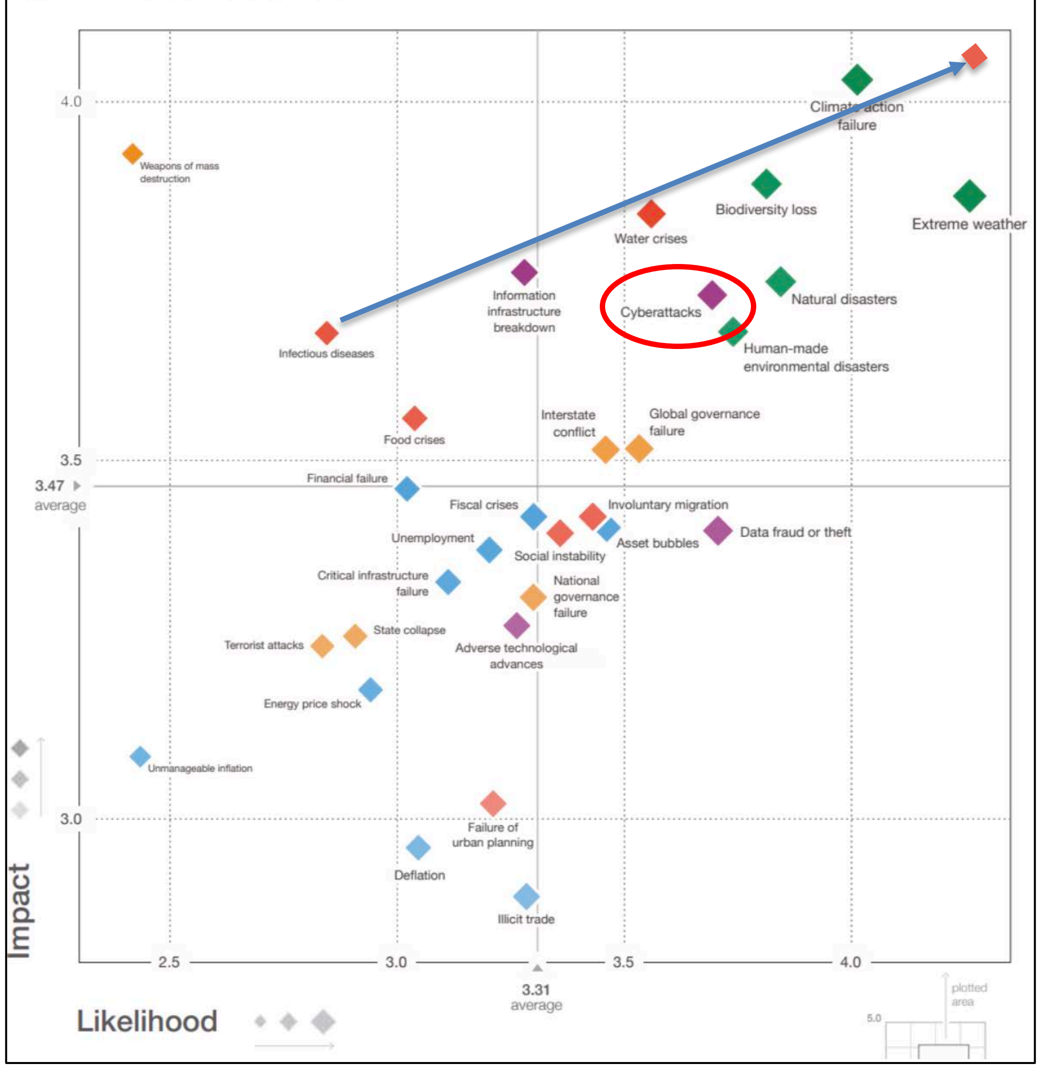
COMMITTED TO IMPROVING THE STATE OF THE WORLD

The Global Risks Report 2020

In partnership with Marsh & McLennan and Zurich Insurance Group

In recent years the Global Risks Report has identified cyberattacks as very likely to happen with a very high impact.

Figure II: The Global Risks Landscape 2020



Critical Information Infrastructure Protection ITU Perspective

6 Trillion

The predicted annual cost of cybercrime globally by 2021

– CSO Online

58%

58% of CISOs said their IT systems were definitely or probably under attack without them knowing it

– Core Security

3.5 Million

The number of unfilled cyber security positions globally by 2021

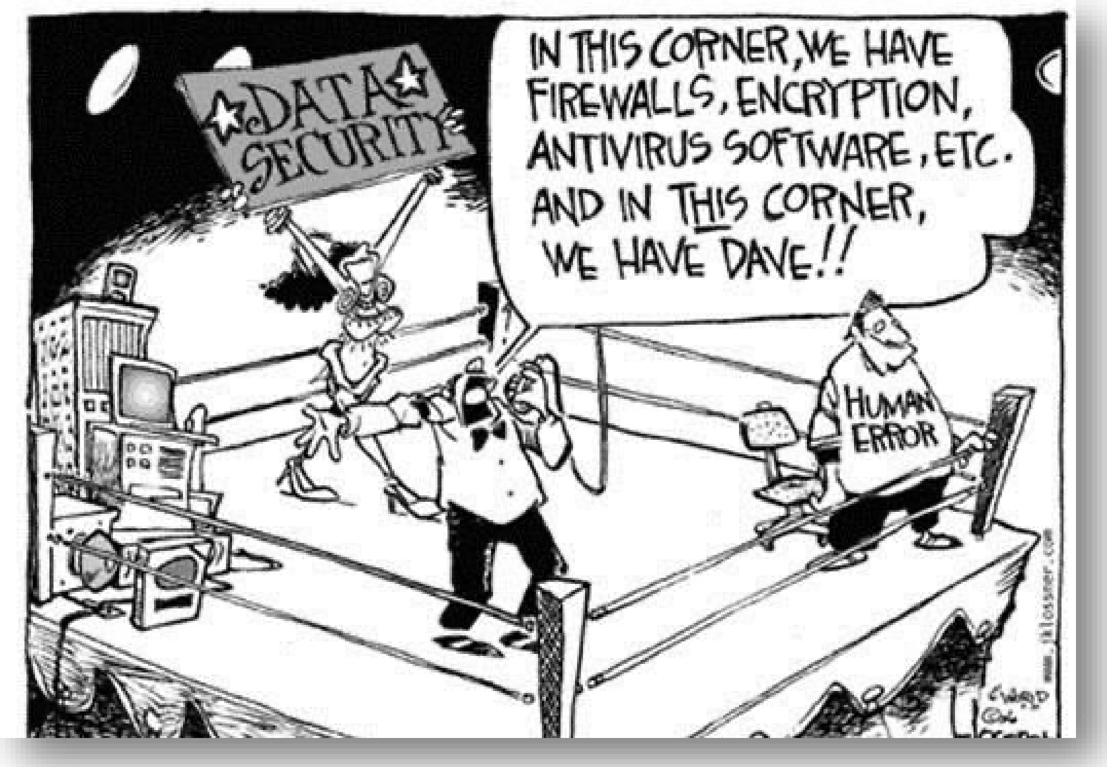
– Cybersecurity Ventures

Critical Information Infrastructure Protection ITU Perspective

95%

of cybersecurity compromises are triggered by human errors

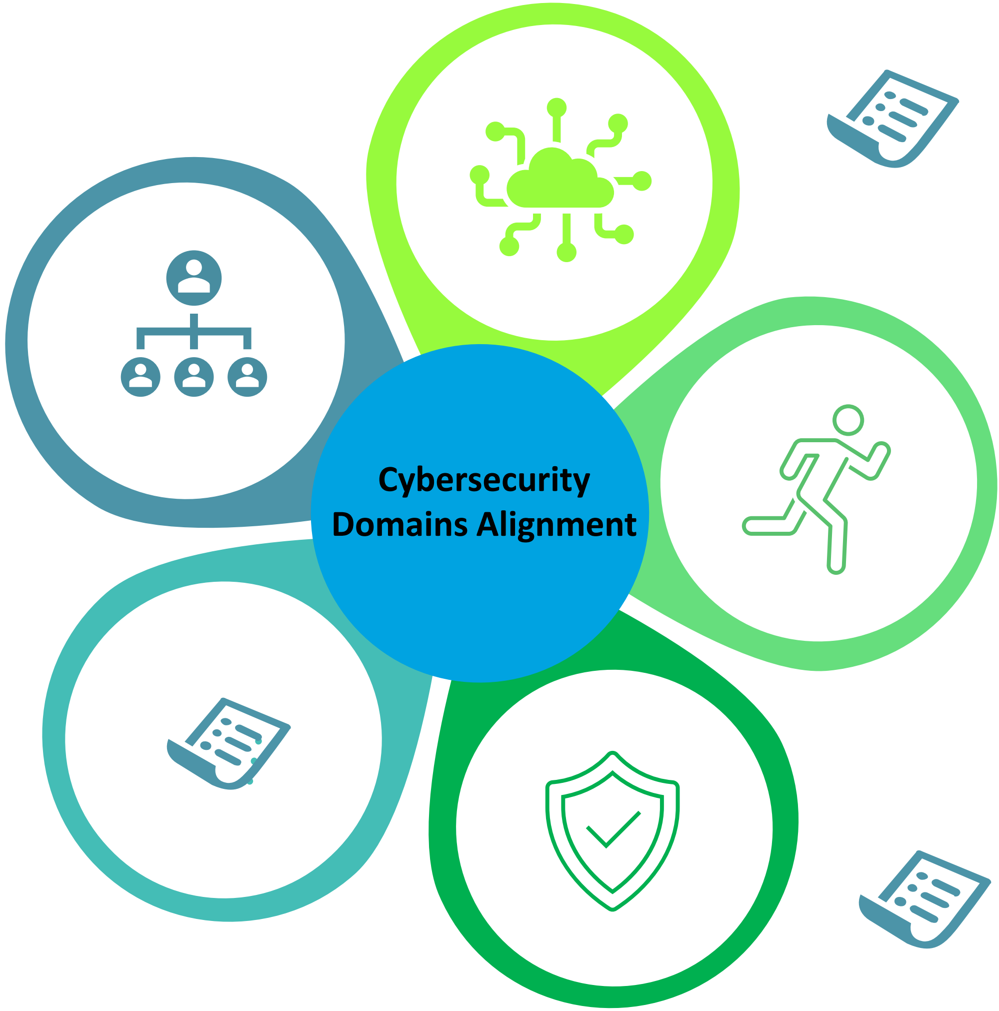
(IBM Cybersecurity Intelligence Report)


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

Exploiting Trust

Someone who can leverage the trust of their victim to gain access to sensitive information or resources or to elicit information about those resources (via phone, office/data center walk in, email or instant messaging)

Critical Information Infrastructure Protection ITU Perspective



Governance

Policy and Strategy
Risk Management
Compliance

Technology

Systems and Infrastructure Security (IT and OT)
Communication Security (IT and OT)
Data Security

People

Strengthening Organizations
Human Resources Development
Supply Chain and 3rd Party Security Service Providers

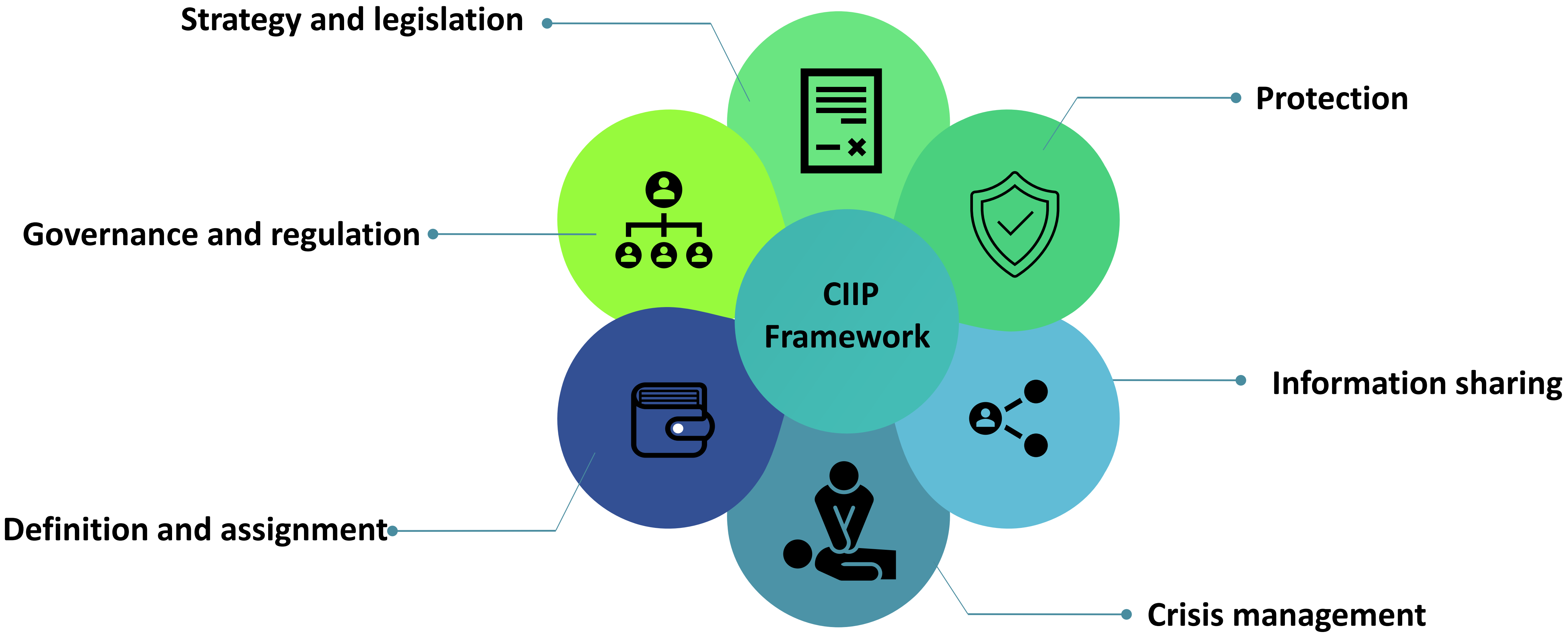
Processes

CERT & Incident Response
Threat Intelligence
Cybersecurity SOPs
Logical Access Control
Monitoring and Evaluation

Physical Security

Physical Separation of Critical Systems
Social Engineering Prevention – Physical Access to critical Systems

Critical Information Infrastructure Protection ITU Perspective



Strategy and legislation

Protection

Governance and regulation

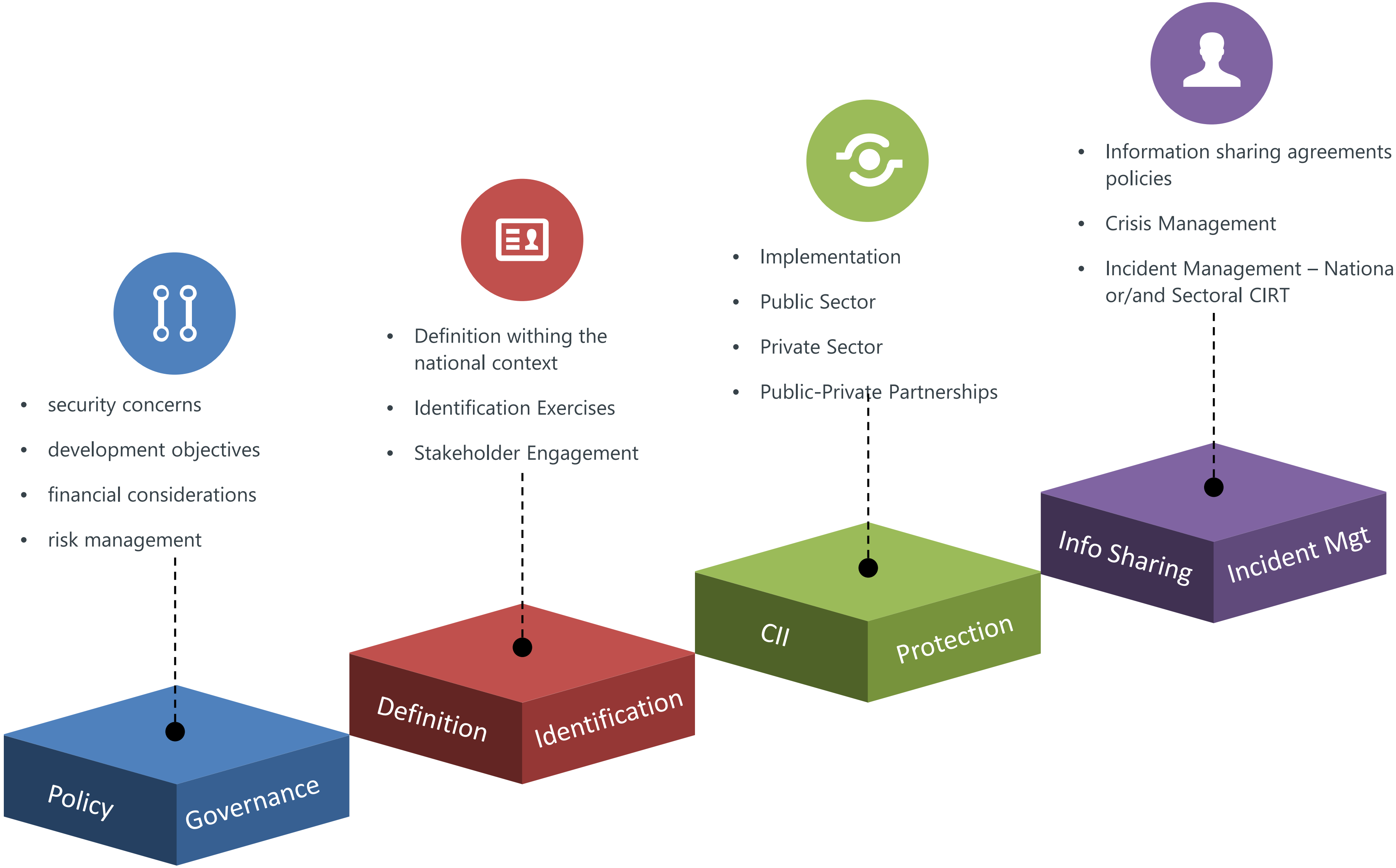
CIIP Framework

Information sharing

Definition and assignment

Crisis management

Critical Information Infrastructure Protection ITU Perspective



- security concerns
- development objectives
- financial considerations
- risk management

- Definition withing the national context
- Identification Exercises
- Stakeholder Engagement

- Implementation
- Public Sector
- Private Sector
- Public-Private Partnerships

- Information sharing agreements and policies
- Crisis Management
- Incident Management – National or/and Sectoral CIRT

International Telecommunication Union: The key systems, services, and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of these.

ITU’s Role in CIIP

CYBERSECURITY PRIORITY AREAS

FOCUS ON DELIVERING IMPACT

TECHNICAL AND POLICY MEASURES

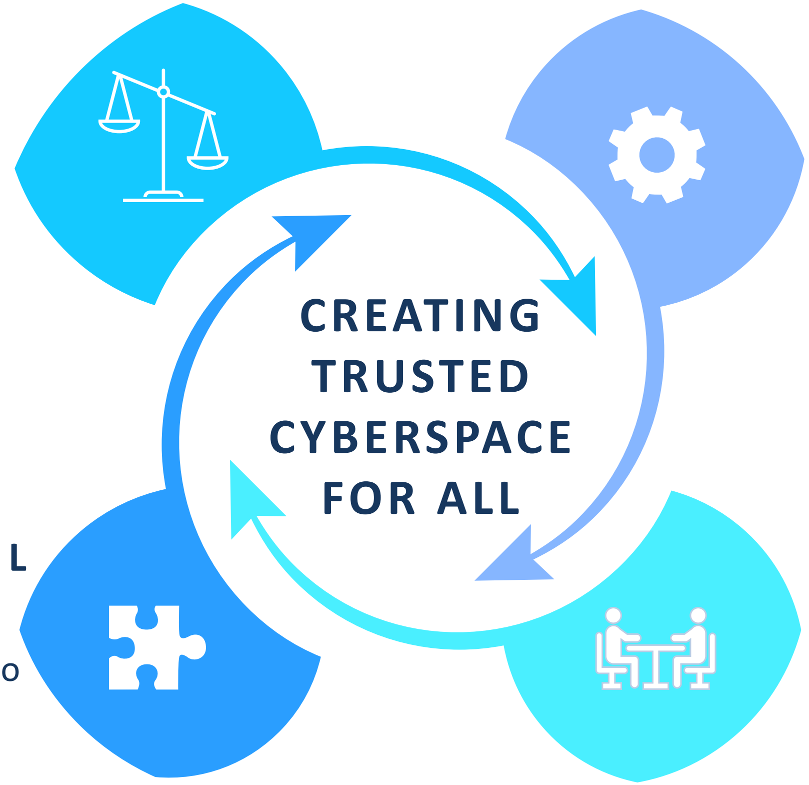
Accelerating the development and adoption of sound national cybersecurity strategies and comprehensive action plans.

ADVISORY AND LEADERSHIP FOCUS

CAPACITY DEVELOPMENT

Improving cybersecurity capacity in the Least Developed and Developing Countries.

TECHNICAL ASSISTANCE FOCUS



CREATING TRUSTED CYBERSPACE FOR ALL

ENHANCING ORGANIZATIONAL STRUCTURES

Establishing prepared organizational structures to support national commitments in cybersecurity.

PROJECT FOCUS

COOPERATION AND COORDINATION

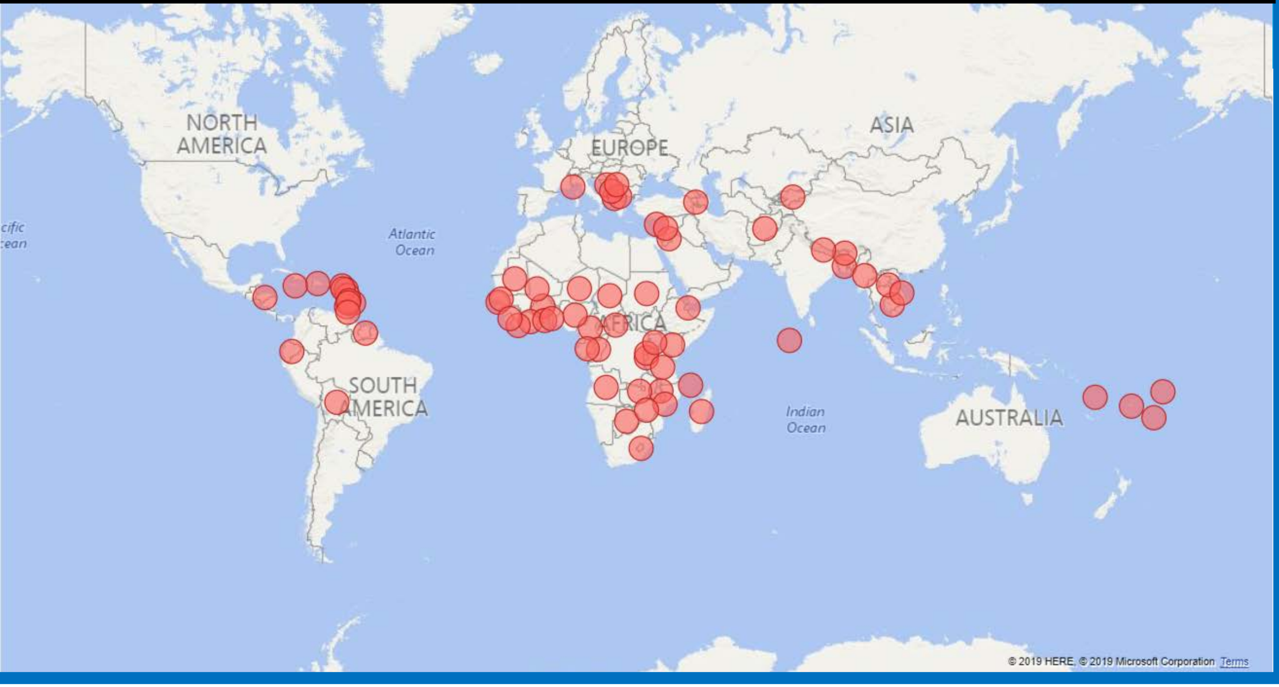
Promoting cybersecurity coordination and collaboration, enabling national digital transformation journey and trust building.

AWARENESS & ENGAGEMENT FOCUS

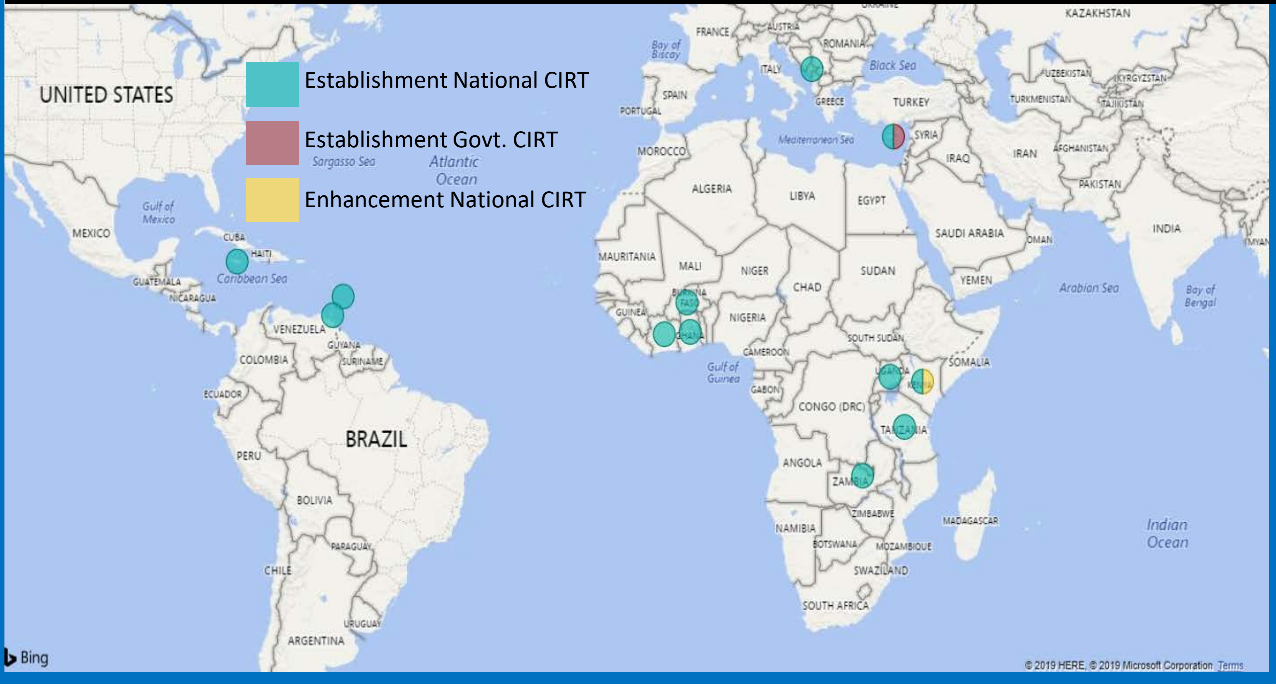
CYBERSECURITY PRIORITY AREAS

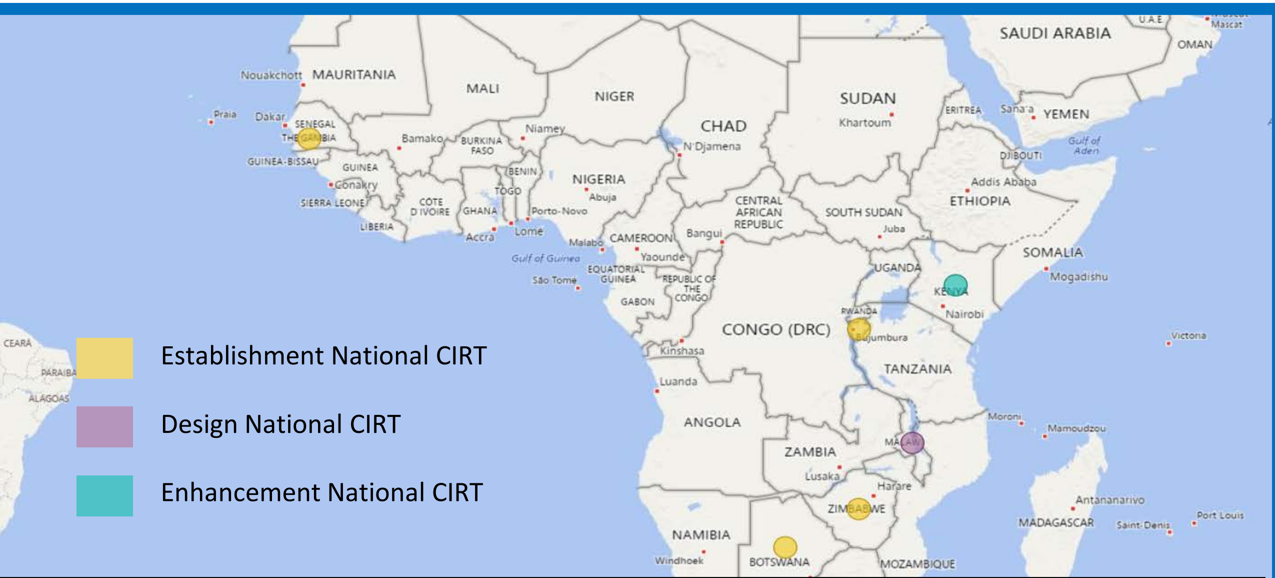
	Incident Response Capabilities	Cybersecurity Engagement and Awareness	Cybersecurity Capacity Development	National Cybersecurity Posture	Online Safety for Children and Youth
OUTPUTS DELIVERABLES	**CIRT** Assessment, Design, Implementation and Enhancement **CIRT Products and Services**	**Awareness and Information Sharing**: GCI Report, Awareness and Info-Sharing Workshops **Facilitate support and cooperation** between ITU Membership **Partner Engagement** in CSR activities and initiatives	Cyberdrill - Cybersecurity **Exercises** and Technical Hands-on Trainings Technical, process and Technological Trainings and Information Sharing Workshops	Cybersecurity **Strategy**, **Policy** and Planning: Transfer of Knowledge, Tools and Direct Assistance **Advisory** and consultancy role. **Development** of NCS	**COP** Guidelines: Transfer of Knowledge, Tools and Direct Assistance
WS	Enhancing Organizational Structures	Cooperation and Coordination	Capacity Development	Technical and Policy Measures	

77 + CIRT READINESS ASSESSMENTS

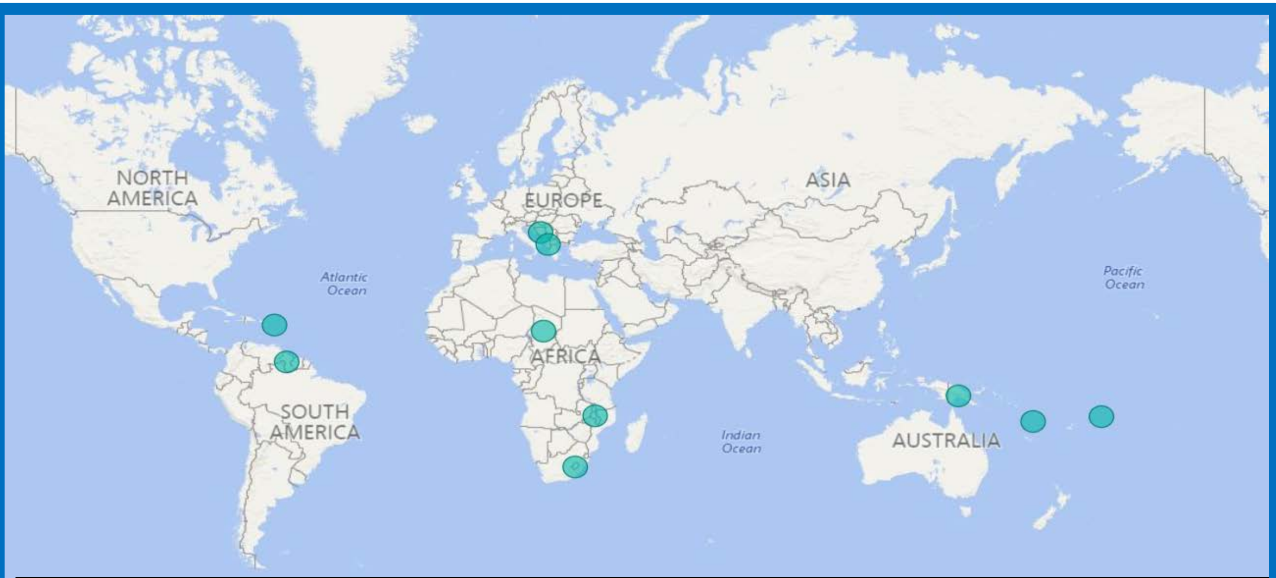


14 CIRT ESTABLISHMENTS


Establishment National CIRT
Establishment Govt. CIRT
Enhancement National CIRT
UNITED STATES
BRAZIL
Atlantic Ocean
Indian Ocean
Bing
© 2019 HERE, © 2019 Microsoft Corporation Terms



6 ONGOING CIRT ESTBLISHMENTS



CIRT ESTABLISHMENT– INTERESTS FOR 2020

The role of National CIRTs in Developing Countries

- Facilitate the development of a national CIIP strategy (CIIP)
- Assisting owners & operators of CII to mitigate their information risk
- Establish a trusted communication channel between all the stakeholders
- Provide early warning
- Coordination of incidents response at the National level
- Help CII to develop their own incident management capabilities.
- Testing and measuring CIIP maturity over time and guiding strategy based on measurement
- Promote National Culture of Cybersecurity

CyberDrills

The cyberdrills are designed with a dual purpose: as a platform for cooperation, information sharing, and discussions on current cybersecurity issues, as well as to provide hands-on exercise for national Computer Incident Response Teams (CIRTs) / Computer Security Incident Response Teams (CSIRTs).

Global Cybersecurity Index (GCI)

National Cybersecurity teams are getting better resource support – financial and human.

The developing countries are learning from other ITU Member States through shared good practices

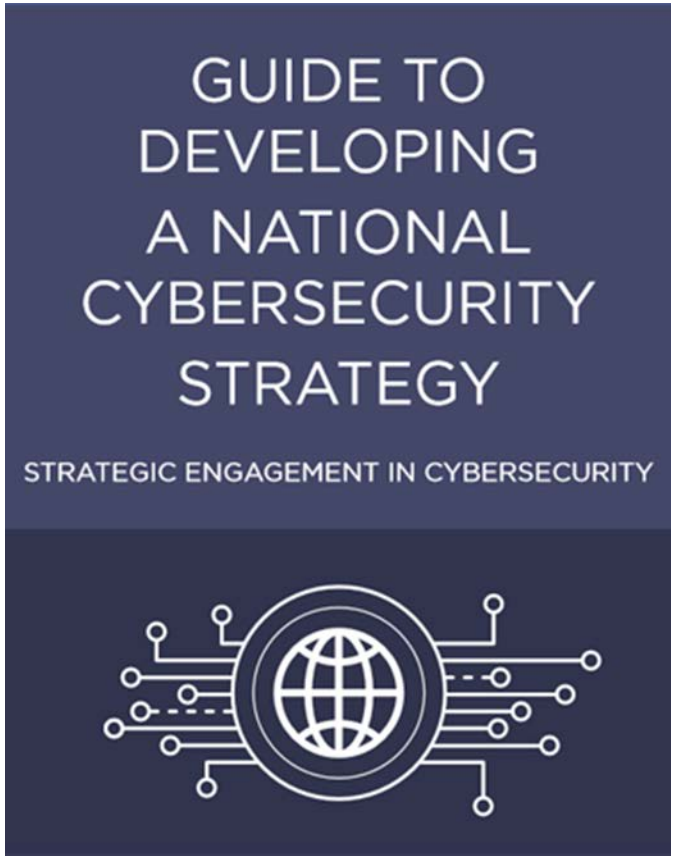
GCI is becoming a capacity development tool, developing countries use GCI as a decision-making tool to improve their national cybersecurity, hence enhancing global cybersecurity awareness level.

The Least Developed and Developing Countries better identify cybersecurity areas to improve.

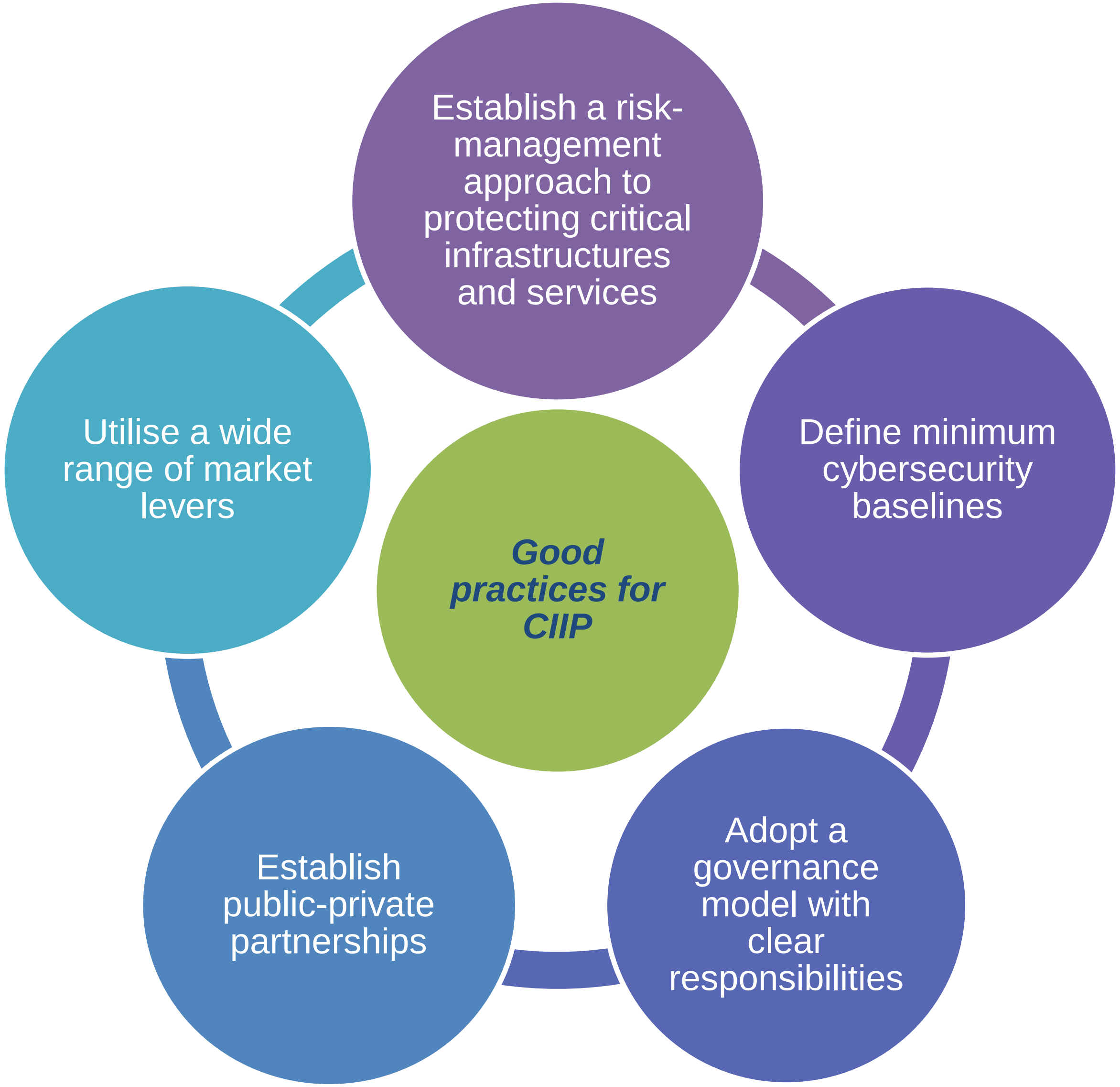
GCI contributes to awareness creation and improvement in national cybersecurity postures

Critical Information Infrastructure Protection ITU Perspective

National Cybersecurity Strategy


GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY
STRATEGIC ENGAGEMENT IN CYBERSECURITY

Focus Area 4– Critical infrastructure services and essential services


Good practices for CIIP
Establish a risk-management approach to protecting critical infrastructures and services
Define minimum cybersecurity baselines
Adopt a governance model with clear responsibilities
Establish public-private partnerships
Utilise a wide range of market levers

Partnerships

THE WORLD BANK

GFCE

OCSC
Oceania Cyber Security Centre

UNODC
United Nations Office on Drugs and Crime

OIPC ICPO INTERPOL
INTERPOL

And many more organizations including academia, private sector organizations that are ITU Sector Members

THANK YOU

cybersecurity(at)itu.int
gci(at)itu.int