Making the Fourth Industrial Revolution
Work for All

4IR Cybersecurity ITU Perspective

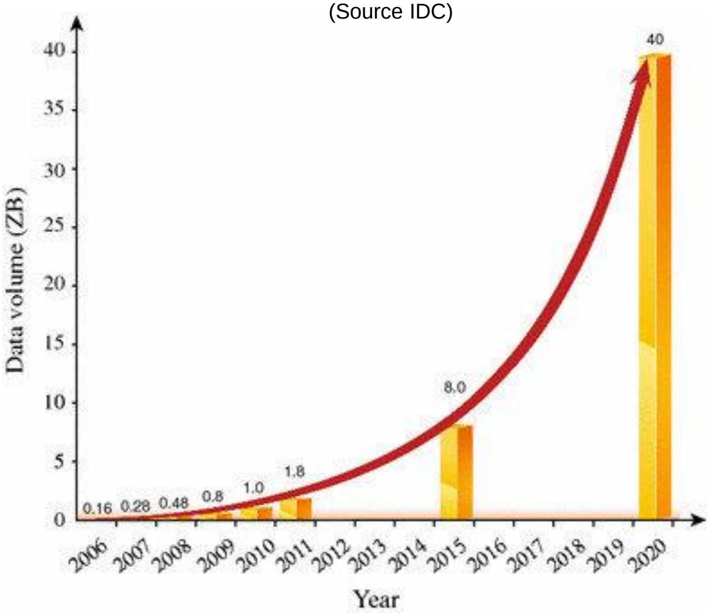
Pablo Palacios
14/10/2020

4IR Cybersecurity: ITU Perspective

More Data and More Exposed

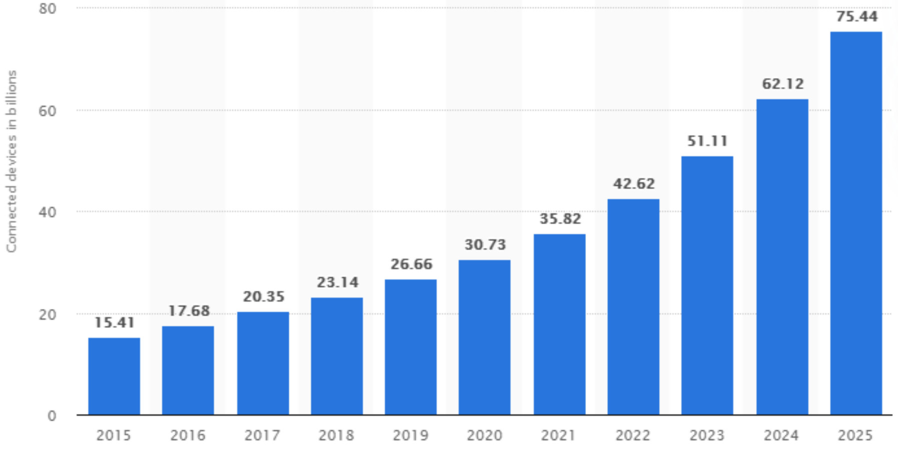
Annual Data Generation per Year

(Source IDC)



IoT connected devices installed base worldwide from 2015 to 2025

(Source Ericsson)



4IR impact on cybersecurity

- Capacity of collecting data
- Capacity of storing and sharing data
- Capacity of analyse and infer

- More Vulnerabilities
- Broader attack surface

4IR Cybersecurity: ITU Perspective

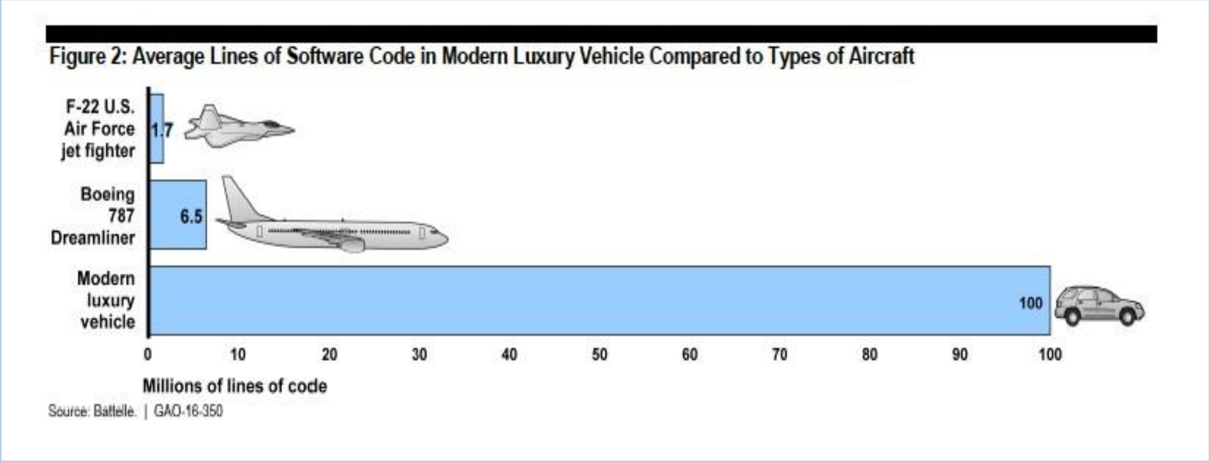


Figure 2: Average Lines of Software Code in Modern Luxury Vehicle Compared to Types of Aircraft

Source: Battelle. | GAO-16-350

Average of 15 – 50 errors per 1000 lines of delivered code

(Code Complete)

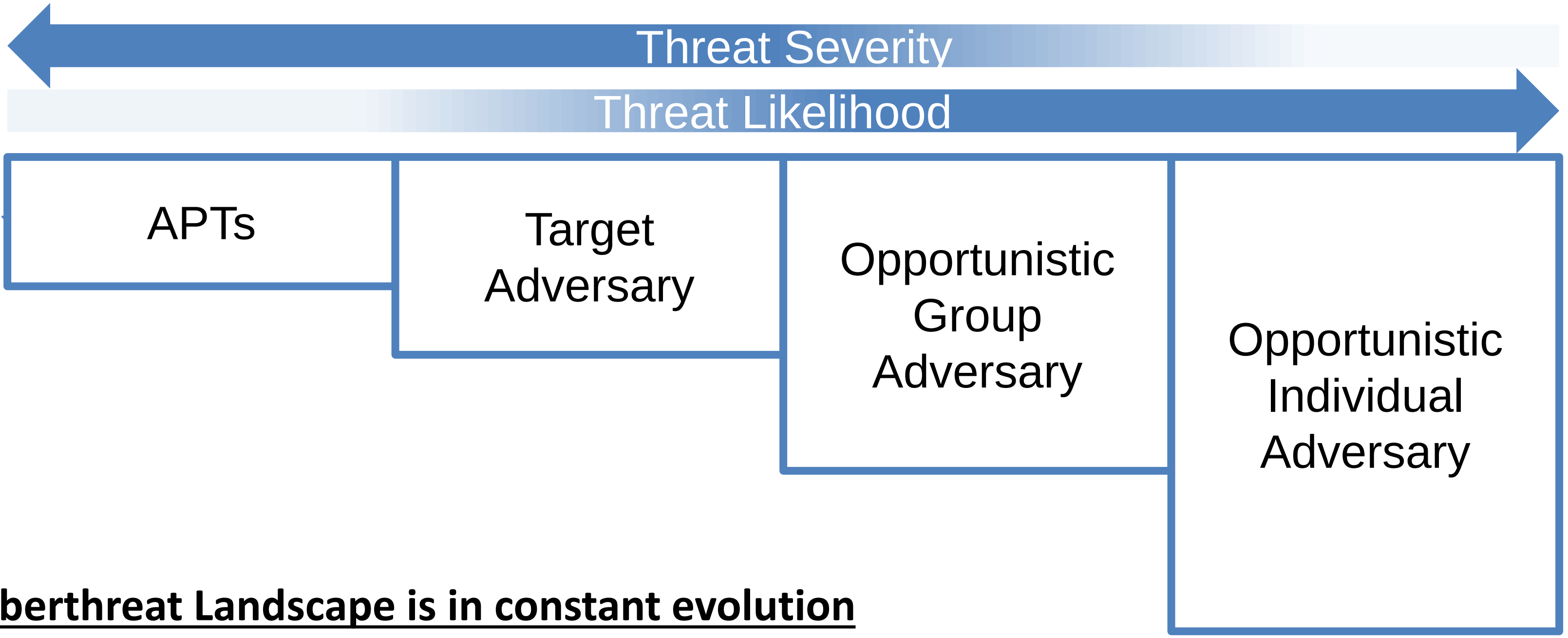
<u>4IR Paradigm is all-encompassing</u>

- Production
- Domotics
- Smart cities
- eHealth
- Energy

- Critical Infrastructure
- eCommerce
- IoT
- Banking
- Finance

4IR Cybersecurity: ITU Perspective

APTs adapt to victims' defences by using multiple attack vectors and are able to pursue their objective in a **stealthy way** for a **prolonged period of time.** These adversaries are often sponsored by states to pursue their geopolitical interests (NIST).



Threat Severity
Threat Likelihood
APTs
Target Adversary
Opportunistic Group Adversary
Opportunistic Individual Adversary

Cyberthreat Landscape is in constant evolution

Insiders

Criminals

Hacktivists

State Proxies

Script Kiddies

Organised Crime

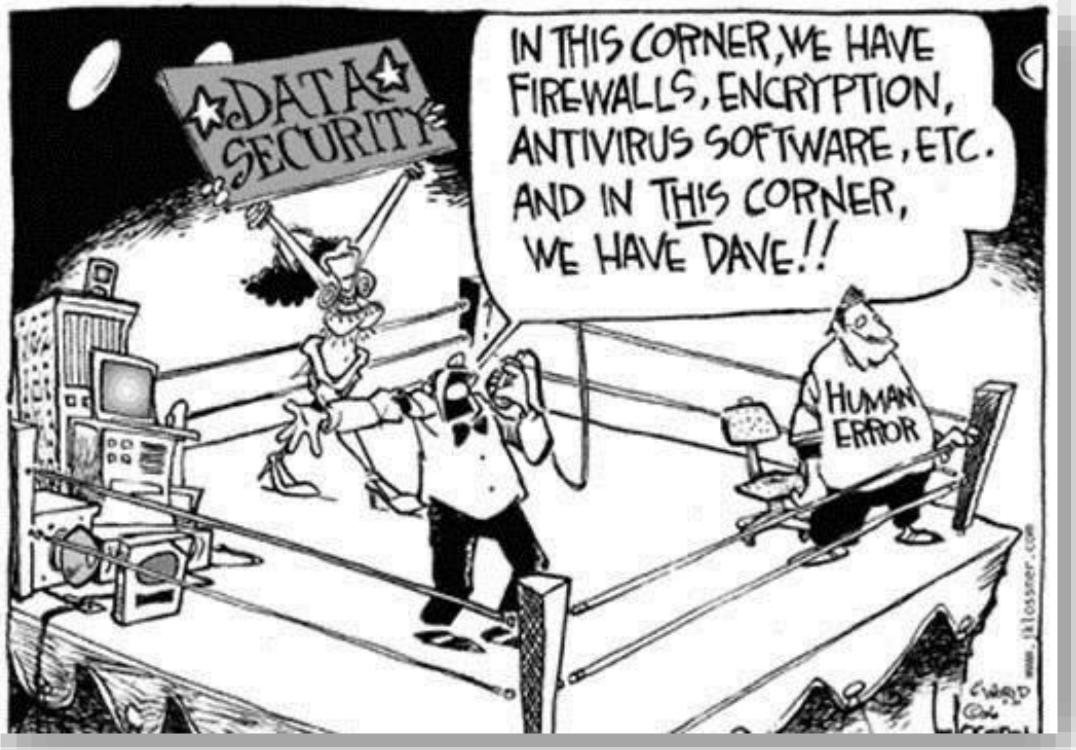
Terrorism

4IR Cybersecurity: 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
www.jklossner.com

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)

Cybersecurity is a key enabler of digital transformation

A rapidly increasing number of new cybersecurity risks emerge stressing the need to strengthen cyber resilience:

- Compromising physical security
- Services disruptions
- Personal data
- Production downtimes
- Damaging equipment
- Financial losses
- Reputational losses

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: “*Offensive cyber capabilities are developing more rapidly than our ability to deal with hostile incidents*”

Spectrum of offensive actions

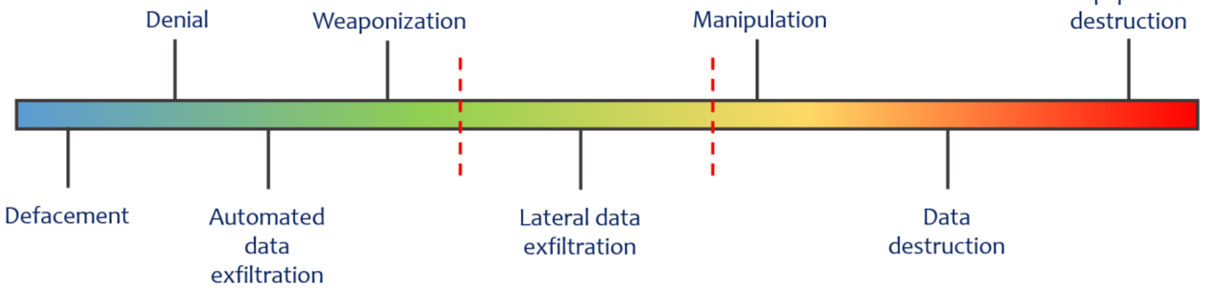
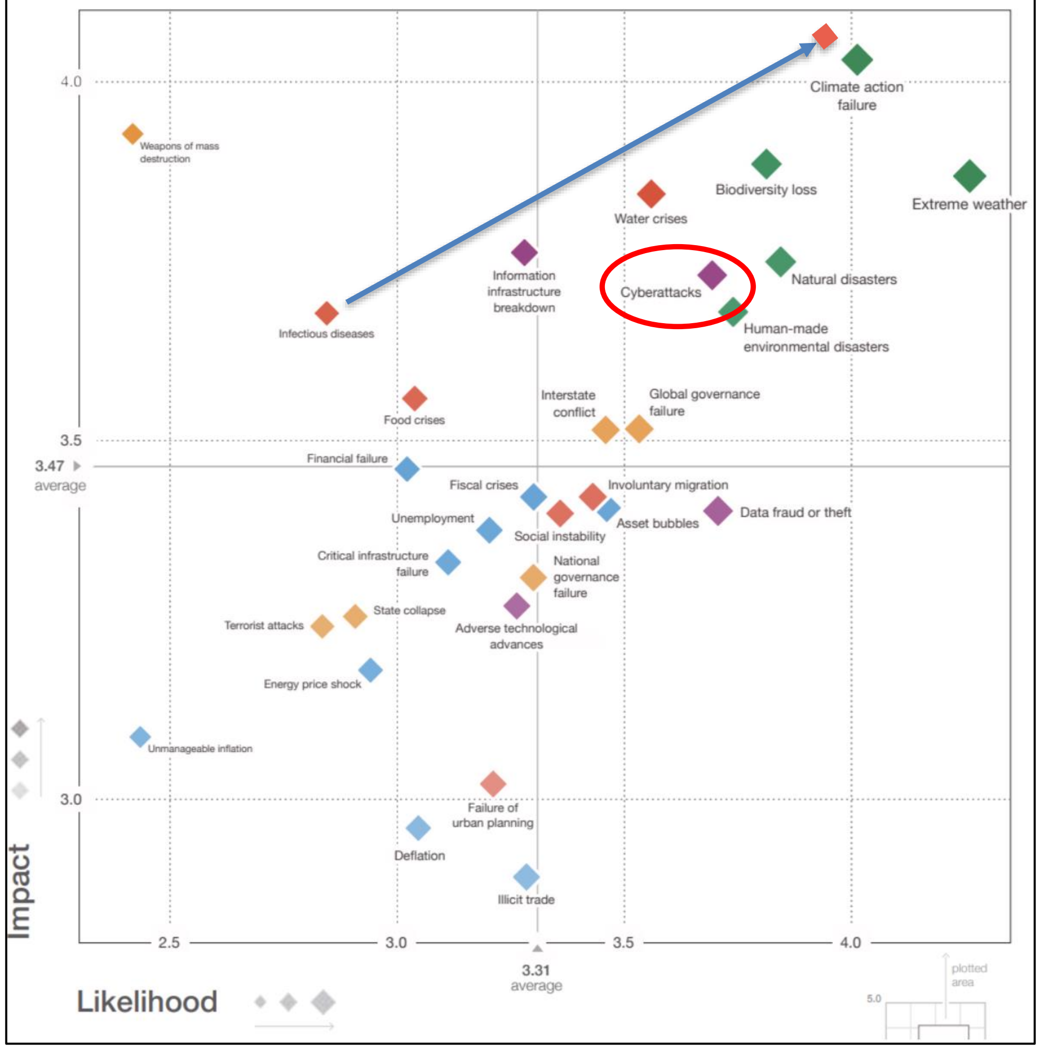
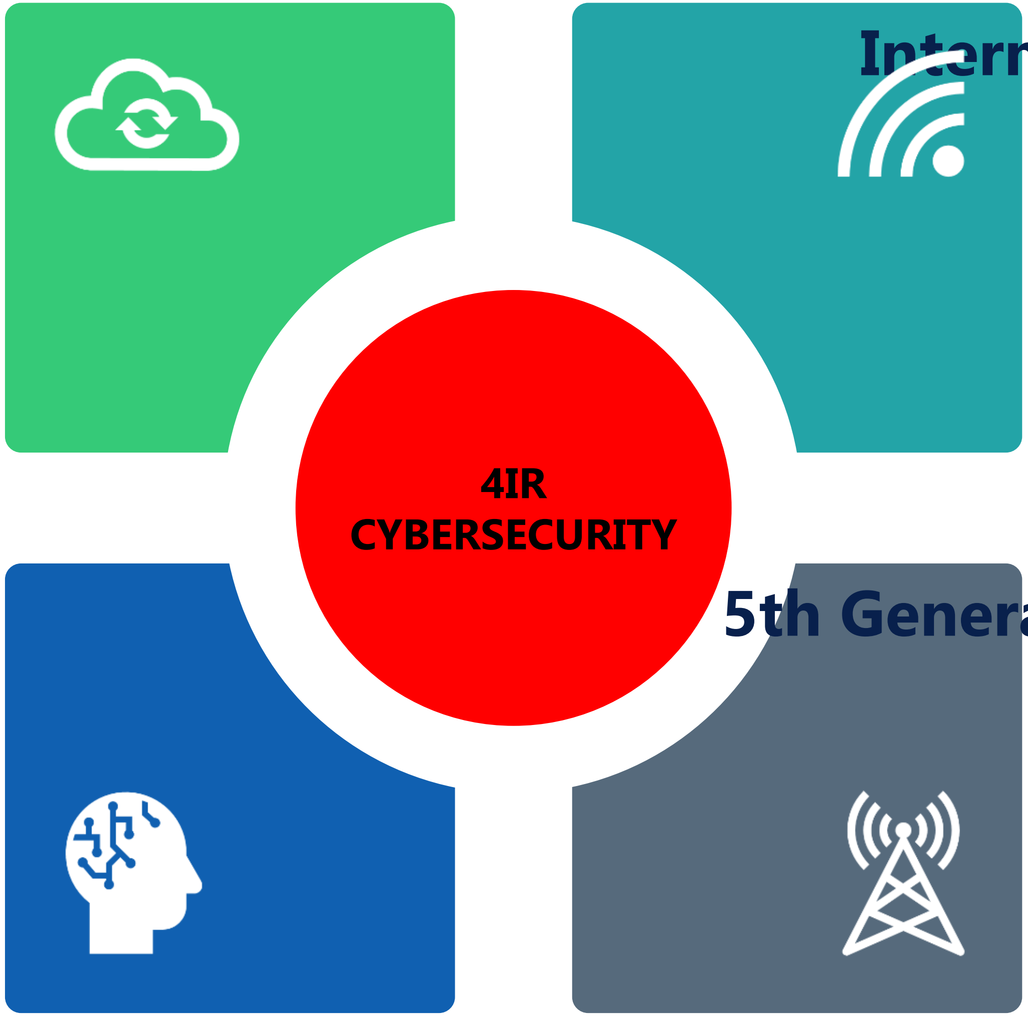


Figure II: The Global Risks Landscape 2020



4IR Cybersecurity: ITU Perspective



Cloud Computing

- Software vulnerabilities
- Network attacks
- Lateral movement
- Isolation failure
- Control over data stored abroad

Internet of Things

- Privacy risks
- Data security risks
- Ransomware
- DoS and DDoS
- Physical attacks

Artificial Intelligence

- Alteration of automated decisions
- AI employed in offensive tools
- AI as a defensive resource

5th Generation communication

- Supply chain security
- Previous generation vulnerabilities
- Weaknesses of the different verticals

4IR Cybersecurity: ITU Perspective

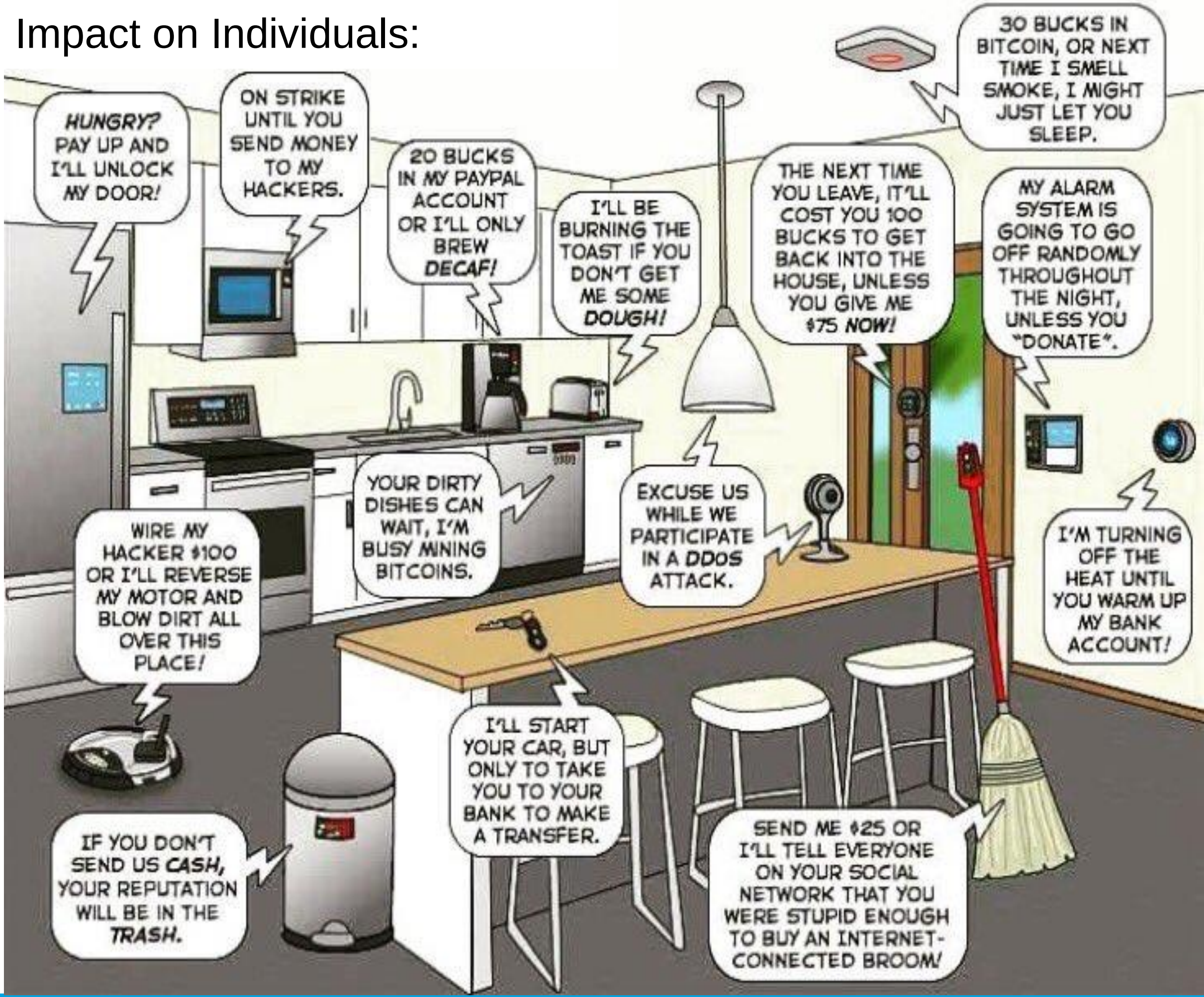
Potential impacts

- Disruption of operations
- Disruption of essential services
- Economic impact
- Public safety
- Theft of data
- Intellectual Property theft, etc.

Cyber risks for all 4IR verticals

Smart grids
Smart roads
Smart building
Supply of essential services
Industry
Communication
Healthcare
Wearable devices
Bank and Finance
Smart everything

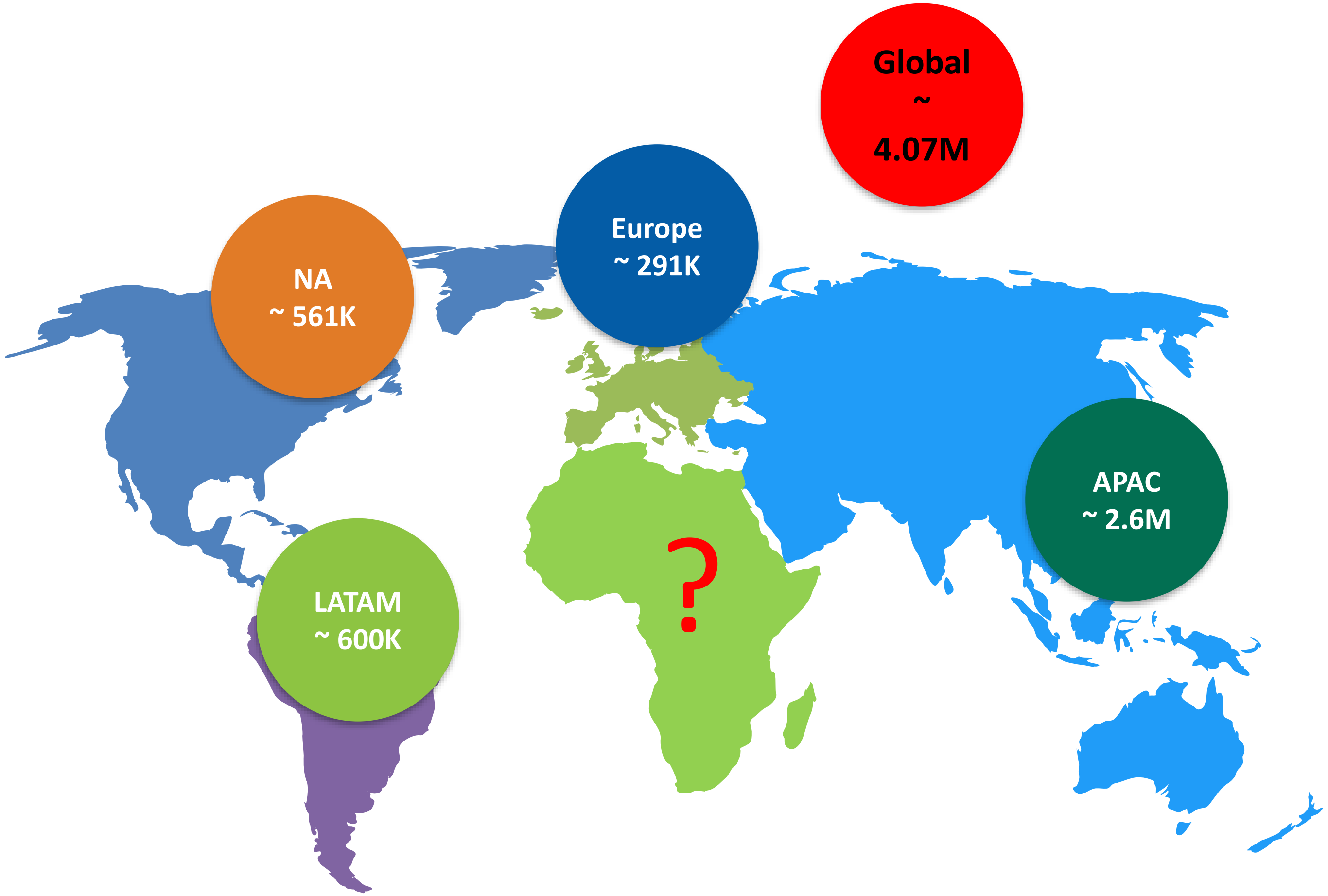
Impact on Individuals:


HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

4IR Cybersecurity: ITU Perspective

The Cybersecurity Workforce Gap by Region

Source: ISC2



3.5 Million

The number of unfilled cybersecurity positions globally by 2021

- Cybersecurity Ventures

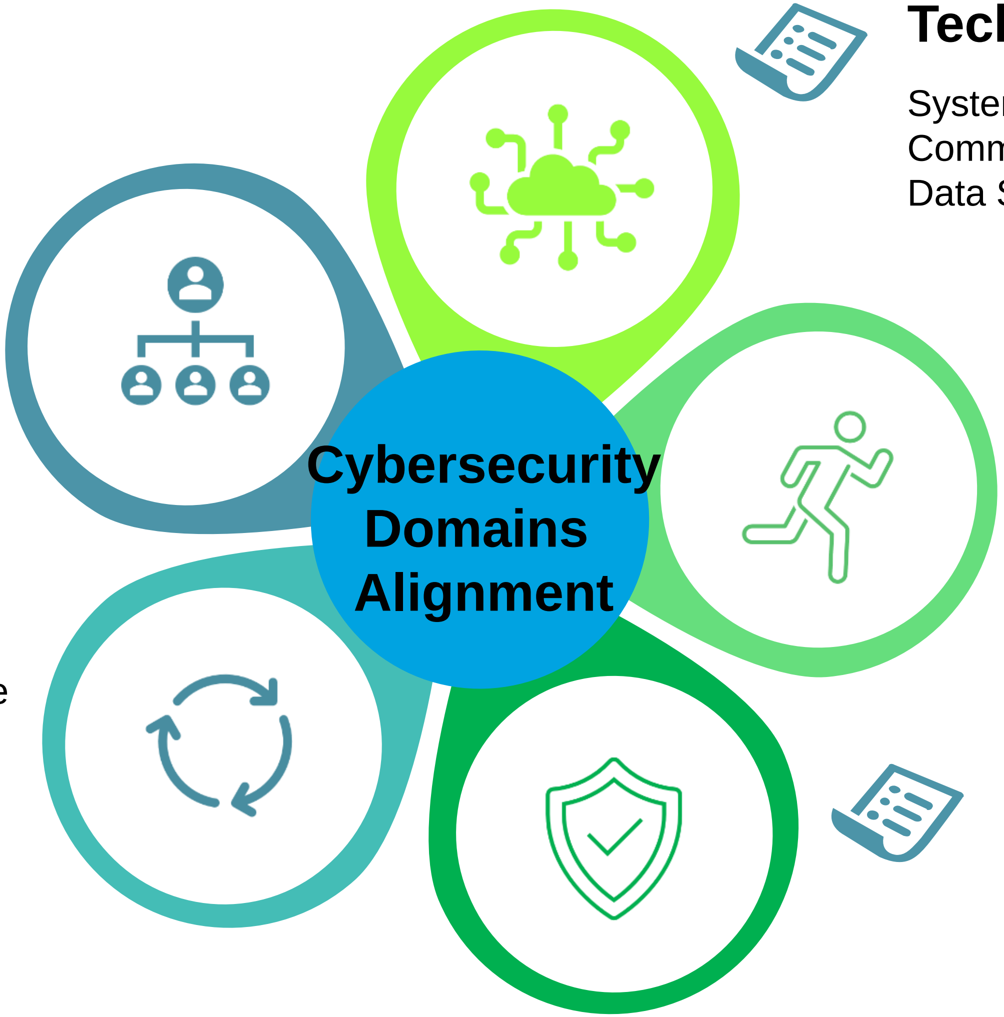
4IR Cybersecurity: ITU Perspective

Governance

Policy and Strategy
Risk Management
Compliance

Processes

CIRT & Incident Response
Information sharing
Threat Intelligence
Cybersecurity SOPs
Logical Access Control
Monitoring and Evaluation



Technology

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

People

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

Physical Security

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

ITU Role in Cybersecurity Development

PRIORITY AREAS

4IR Cybersecurity: ITU Perspective

FOCUS ON DELIVERING IMPACT

TECHNICAL AND POLICY MEASURES

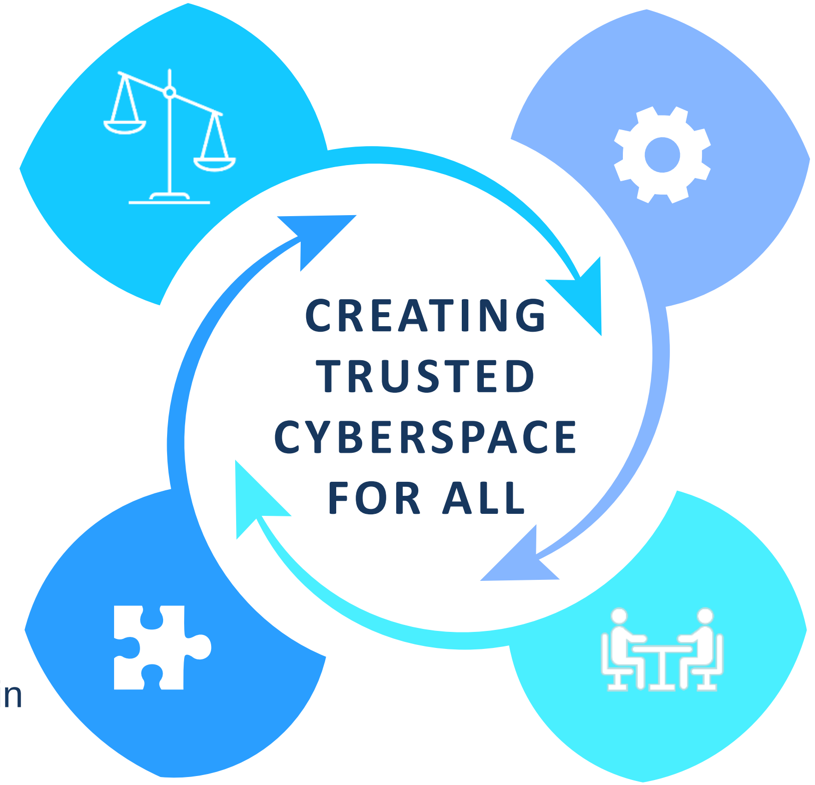
Accelerating the development and adoption of sound national cybersecurity strategies and comprehensive action plans.

ADVISORY AND LEADERSHIP FOCUS

ENHANCING ORGANIZATIONAL STRUCTURES

Establishing prepared organizational structures to support national commitments in cybersecurity.

PROJECT FOCUS



CAPACITY DEVELOPMENT

Improving cybersecurity capacity in the Least Developed and Developing Countries.

TECHNICAL ASSISTANCE FOCUS

COOPERATION AND COORDINATION

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

AWARENESS & ENGAGEMENT FOCUS

4IR Cybersecurity: ITU Perspective

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**	

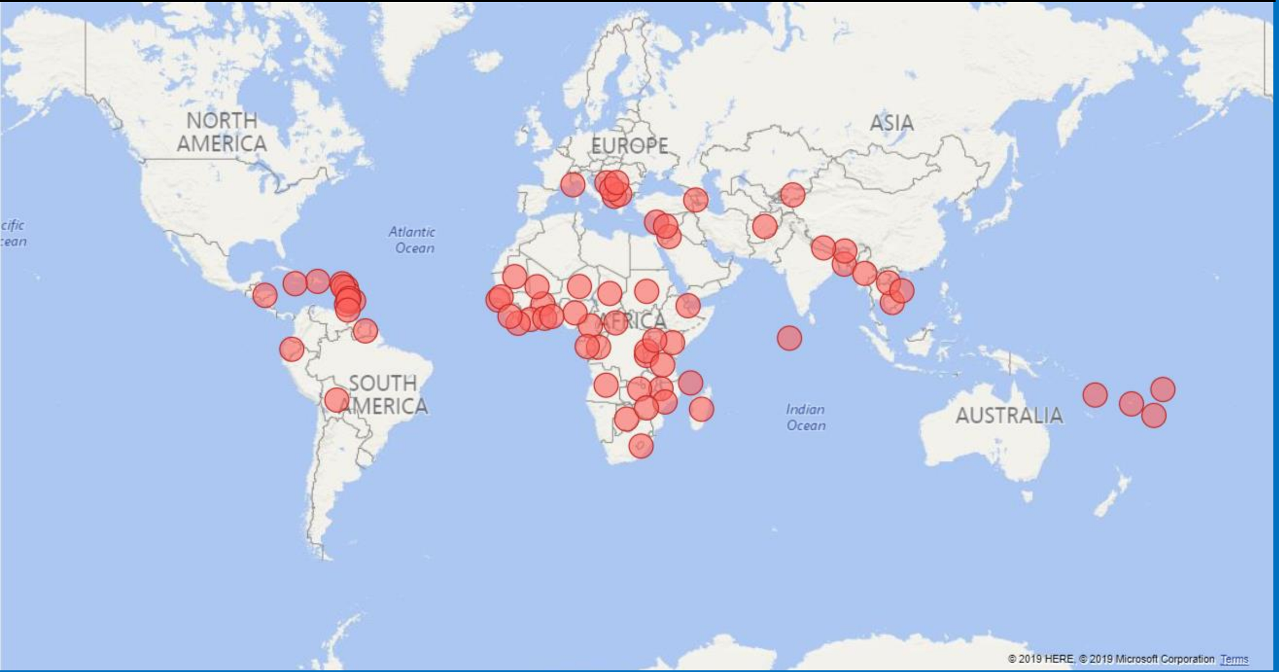
The role of National CIRTs in Developing Countries

- Facilitate the development of a national cybersecurity posture
- Assisting operators 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 operators develop their own incident management capabilities.
- Testing and measuring maturity over time and guiding strategy based on measurement
- Promote National Culture of Cybersecurity

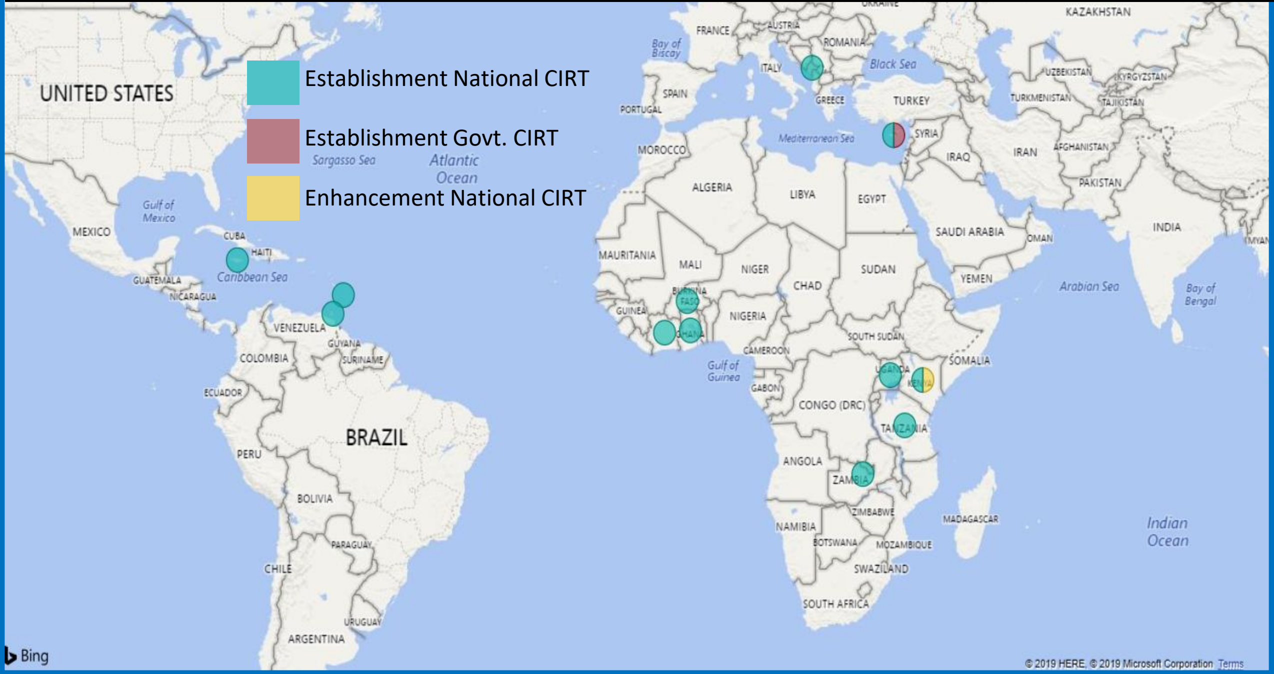
CyberDrills

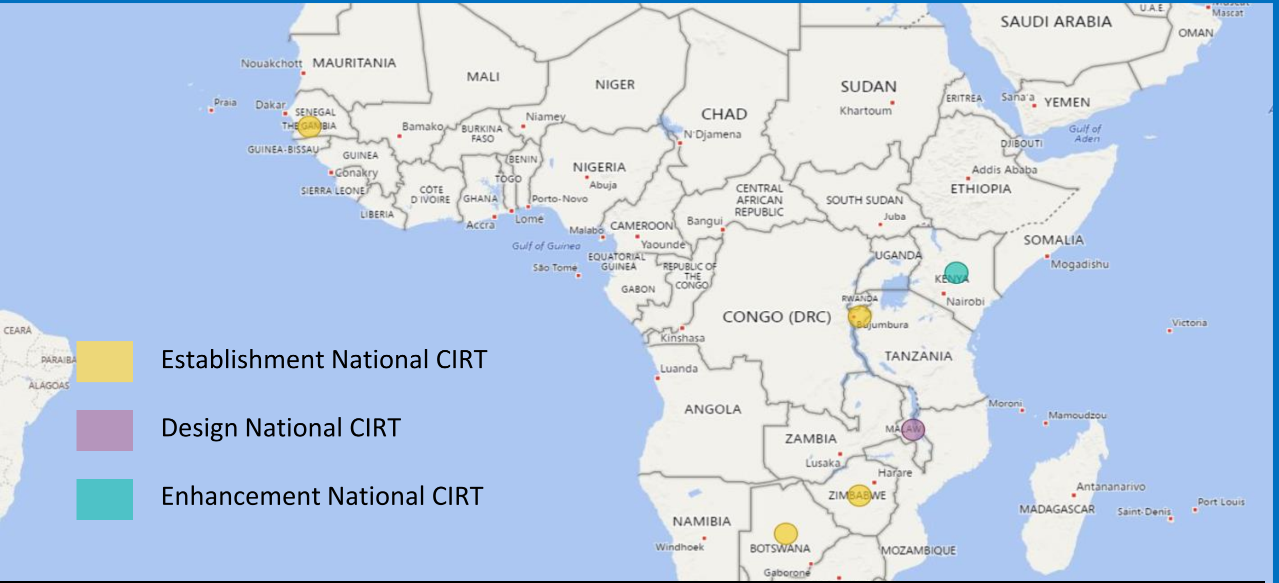
The cyberdrills are designed with a dual purpose: as a platform for cooperation, information sharing, and discussions on current cybersecurity issues, as well as to provide hands-on exercise for national Computer Incident Response Teams (CIRTs) / Computer Security Incident Response Teams (CSIRTs).

77 + CIRT READINESS ASSESSMENTS

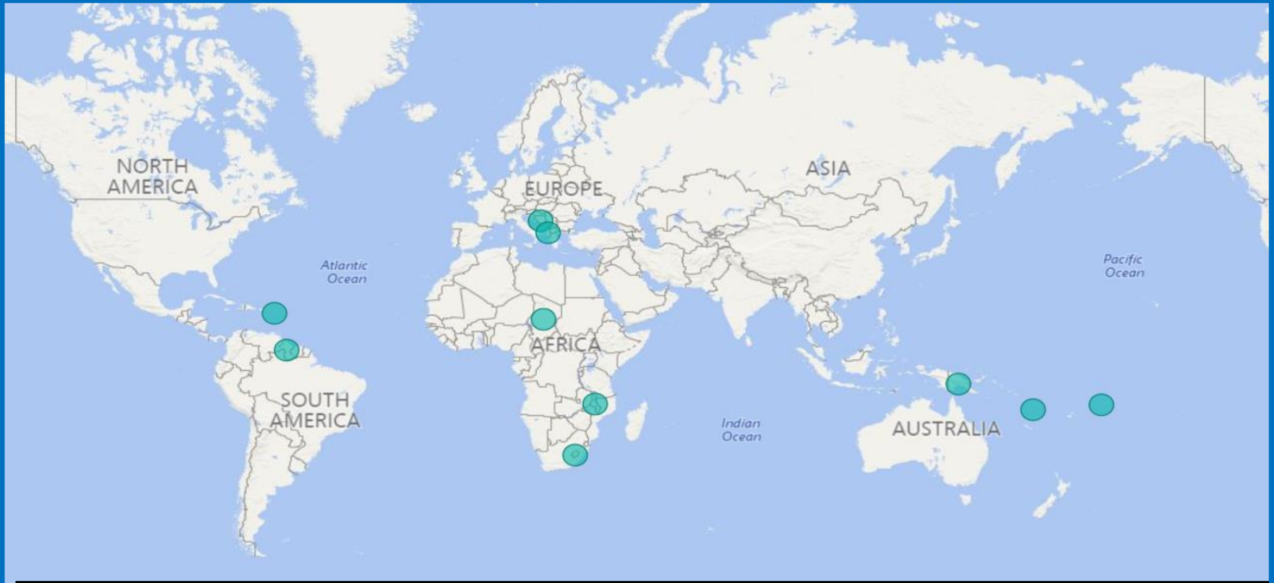


14 CIRT ESTABLISHMENTS





6 ONGOING CIRT ESTBLISHMENTS



CIRT ESTABLISHMENT– INTERESTS FOR 2020-2021

Global Cybersecurity Index (GCI)

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

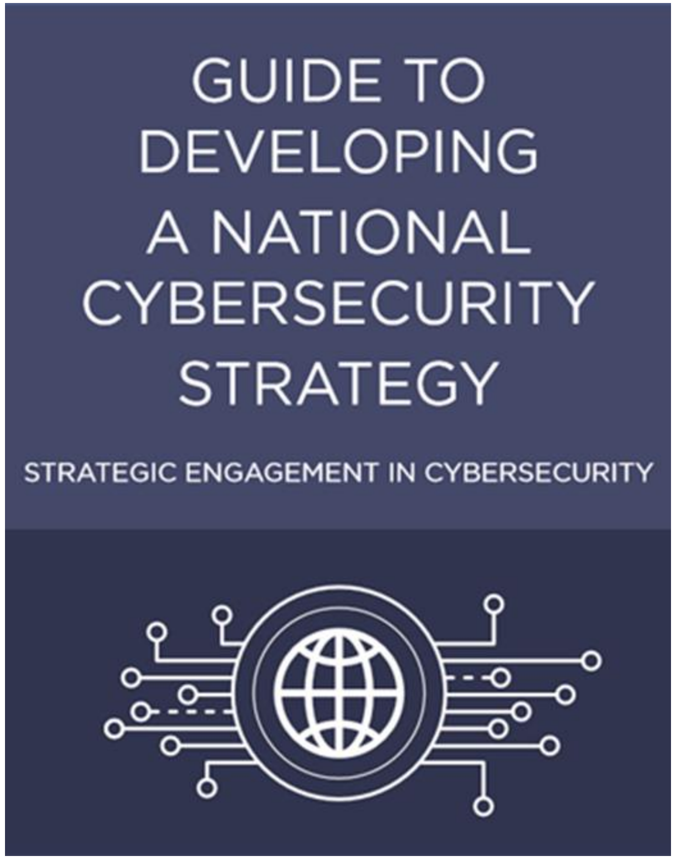
Developing countries are learning from other ITU Member States through shared good practices.

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.

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

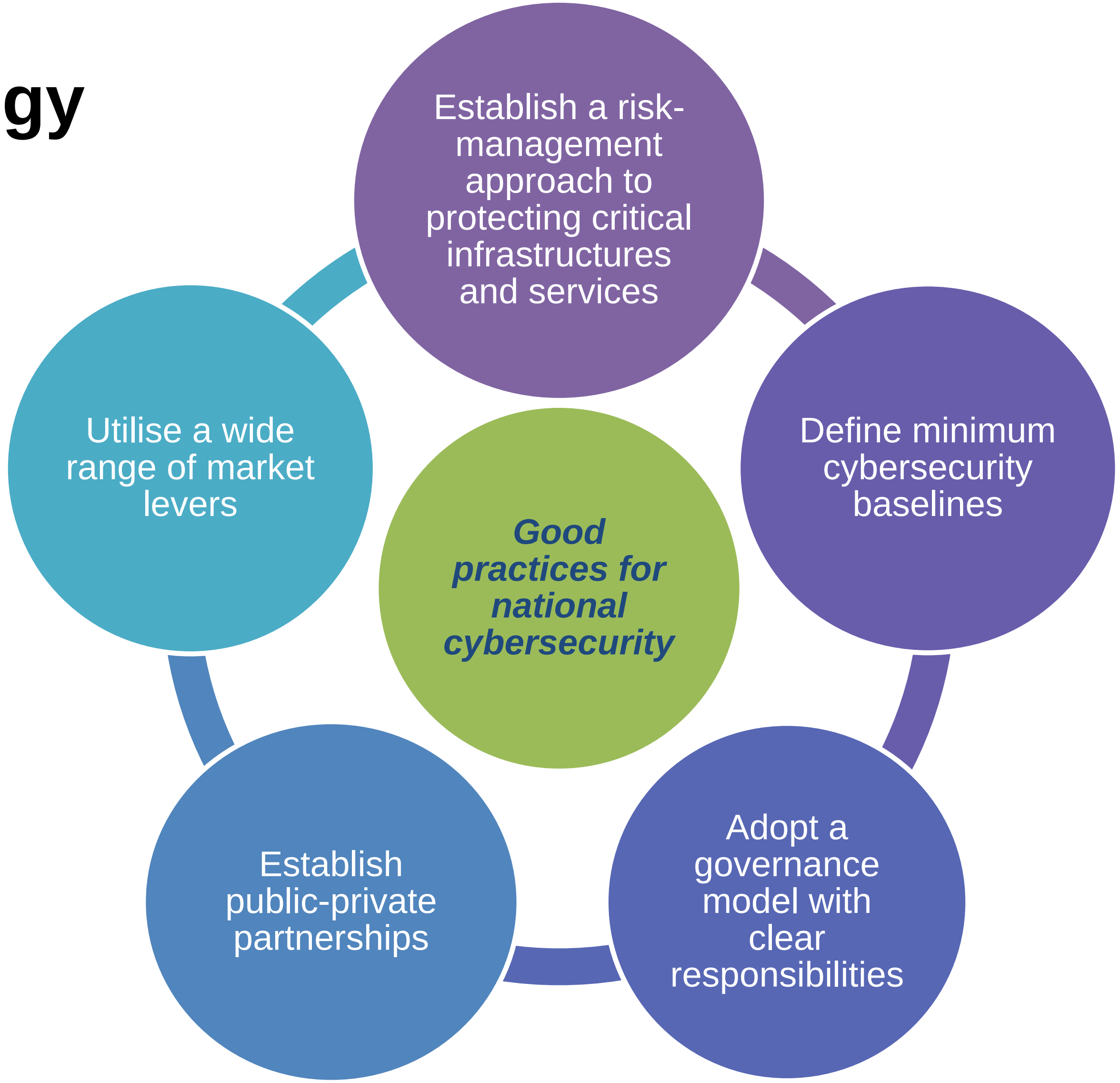
GCI contributes to awareness creation and improvement in national cybersecurity postures.

National Cybersecurity Strategy



GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY

STRATEGIC ENGAGEMENT IN CYBERSECURITY



Good practices for national cybersecurity

- 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

THANK YOU

cybersecurity@itu.int
gci@itu.int