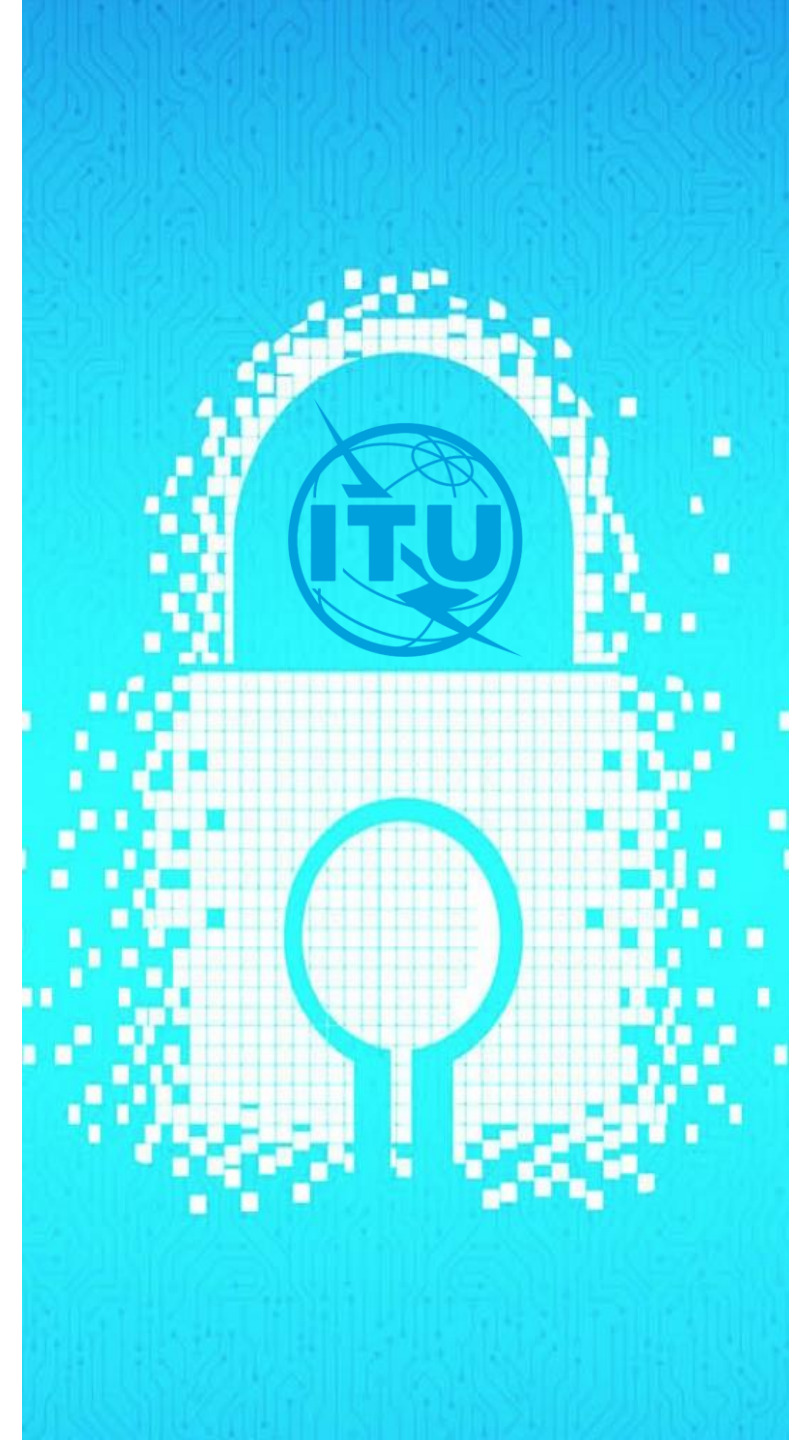


The Role of ITU in Cybersecurity Development

Orhan Osmani

International Telecommunication Union





ITU at a glance

What ITU does?



'Committed to Connecting the World'

193 + 700+ 150

MEMBER STATES

INDUSTRY & INTERNATIONAL ORGANIZATIONS

ACADEMIA MEMBERS



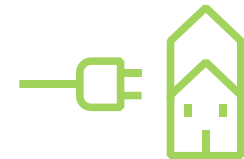
MEMBERSHIP



ITU-R Radiocommunication
Coordinating radio-frequency spectrum and assigning orbital slots for satellites



ITU-T Standardization
Development global standards



ITU-D Development
Bridging the digital divide

46 Countries:

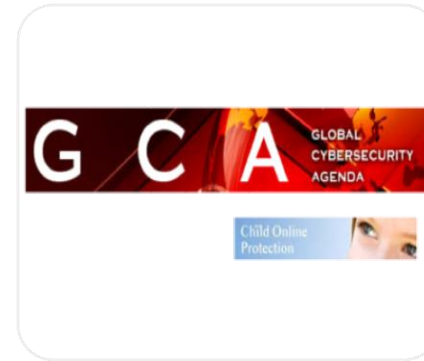
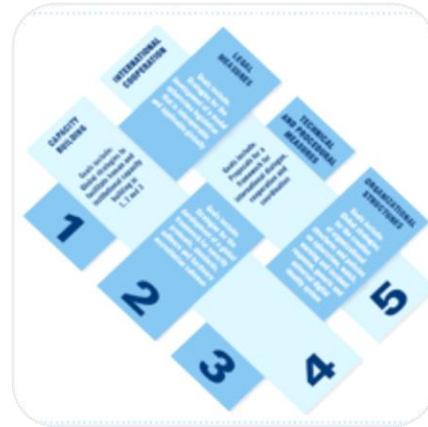
Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Republic of North Macedonia, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Vatican, Ukraine, United Kingdom.

REGIONAL INITIATIVES on CYBERSECURITY FOR EUROPE 2018-2021



EUR4: Enhancing trust and confidence in the use of information and communication technologies

Cybersecurity in ITU – A brief timeline



Geneva 2003 – Tunis
2005

WSIS entrusted ITU as
sole facilitator for WSIS
Action Line C5 -
“Building Confidence
and Security in the use
of ICTs”

In 2007 **Global
Cybersecurity Agenda
(GCA)** was **launched** by
the Secretary General of
ITU. GCA is a **framework
for development and
international
cooperation in
cybersecurity**

In 2008 ITU
Membership **endorsed**
the **GCA** as the ITU-wide
strategy on international
cooperation & initiative
on COP started.

Building confidence and
security in the use of
ICTs is widely embedded
in ITU Governing
Conferences’
resolutions.

The Role of ITU in Cybersecurity Development



To build confidence and security in the use of telecommunications/ICTs, develop and implement standards in cybersecurity on International Level



Assist Member States to strengthen cybersecurity capacity to effectively share information, find solutions, and respond to cyber threats, and to develop and implement national strategies and capabilities, including capacity building, encouraging national, regional and international cooperation towards enhanced engagement among Member States and relevant players



Develop products and services for building confidence and security in the use of telecommunications/ICTs, such as reports and publications, and for contributing to the implementation of national and global initiatives


How?: Our Approach - Implementation Mechanisms



Project
Implementatio
ns



Technical
Assistance



Information
Sharing



Capacity
Development

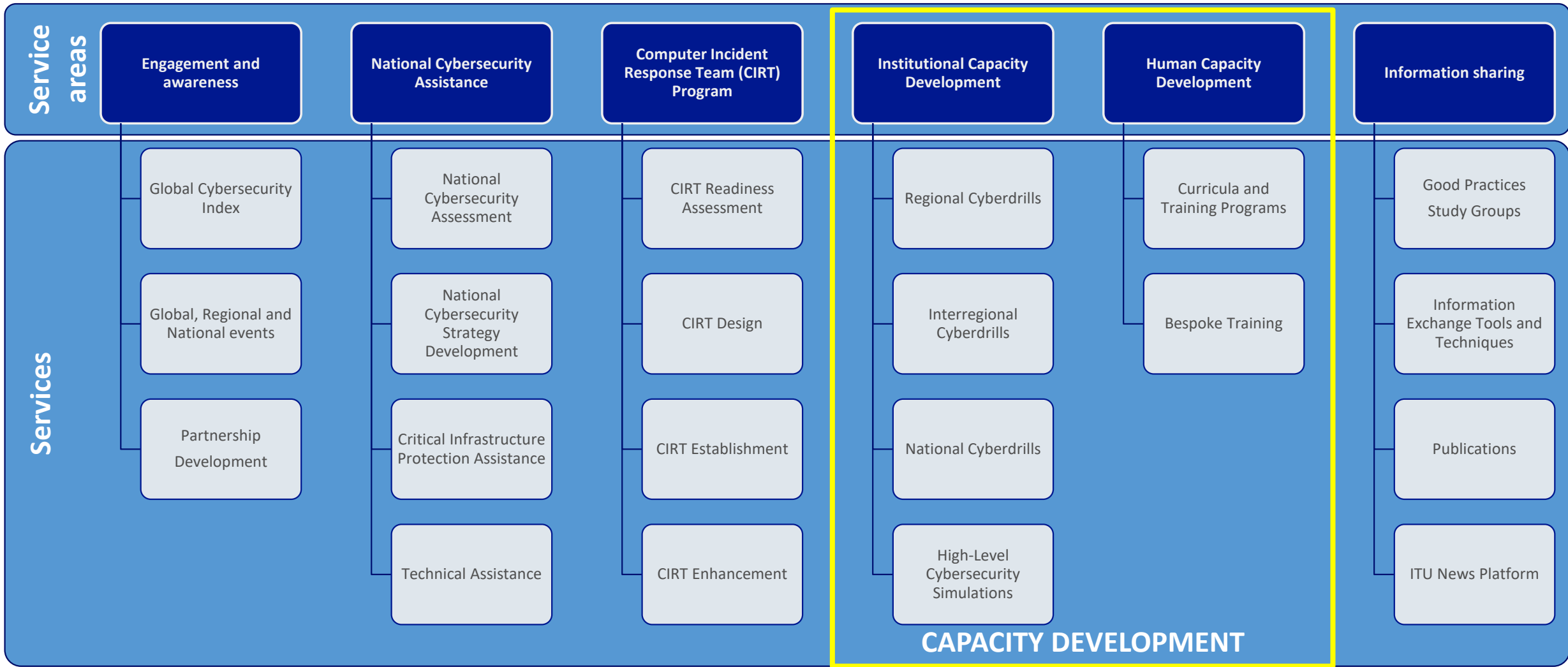


Partnership
Development



Product
Development

What?: Cybersecurity Services Offerings

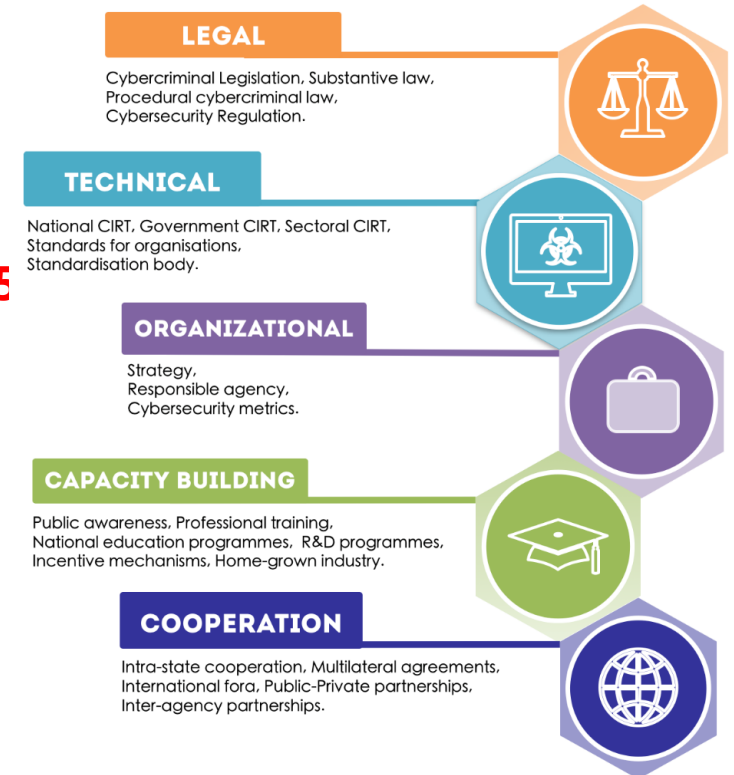


Global Cybersecurity Index [GCI]

GCI is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States *cybersecurity commitment* with regard to the **five pillars** identified by the High-Level Experts and endorsed by the GCA.

“GCI is a capacity building tool, to support countries to improve their national cybersecurity posture”

- GCIv1 : 2013-2014 period with **105** country responses
- GCIv2 : 2016-2017 period with **134** country responses
- **GCIv3 : 2018 period with 155 country responses**



Some important observations globally



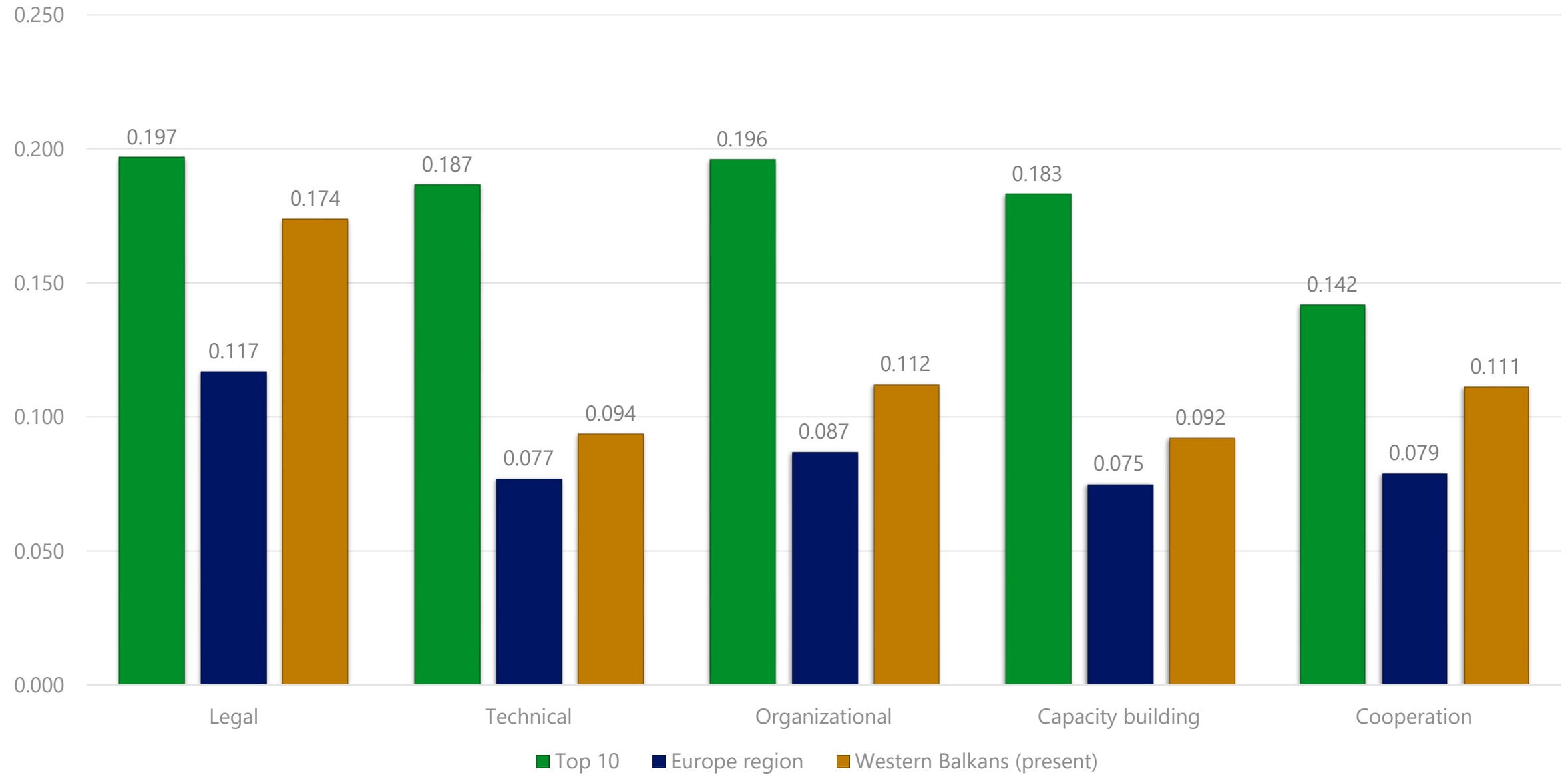
- ❖ **The survey shows 92 (53%) Member States carry out cybersecurity risk assessments.**
- ❖ **Countries are becoming more responsive to the aims of the GCI project. Many Member States provided data capturing the real situation of their countries, as well as providing their own on-ground best practices. There is some increase in the level of awareness and competition in the overall commitment worldwide.**
- ❖ **In the Legal pillar, Benin, Estonia and Poland have implemented new laws on cybercrime; Zimbabwe, Zambia, Egypt, South Africa, and Eswatini (formerly known as Swaziland) have new drafts on cybercrime law and Uganda is drafting its data/privacy protection.**
- ❖ **In the Organizational pillar, some Member States including Australia, Botswana, Canada, Czech Republic, Denmark, Japan, Jordan, Netherlands, Spain, Samoa, Singapore and Luxembourg have also updated their National Cybersecurity Strategy while Cameroon, Malawi, Tanzania and Zimbabwe are in the process of drafting their strategy.**
- ❖ **Most countries have improved their GCI values, overall GCI rankings have had large changes. Many countries moved to different places in the GCI rankings due to the cybersecurity improvements in the Europe region.**

Some important observations in the region



- ❖ **Albania** –approved law No.2/2017 on Cyber Security in 2017 to achieve a high level of cybersecurity by defining security measures, rights, obligations, and mutual co-operation between entities of critical, important infrastructures and the national authority for electronic certification and cyber security (NAECCS) in the role of a national CIRT.
- ❖ **Bosnia and Herzegovina** in the process to develop its network of CIRTs.
 - ❖ While the framework for the NCS for the country is being drafted.
- ❖ **Montenegro** has a standalone National Cybersecurity strategy including metrics to measure cybersecurity development on national level.
- ❖ **Serbia** - established relevant institutions such as the competent authority (Ministry of Trade, Tourism and Telecommunication), the national CERT, the Government CERT, Independent ICT Operators, Special CERTs following the adoption of Law on Information Security Serbia
 - ❖ **Serbia** also recognized critical infrastructure (CNI – ICT Operators of essential services) by adoption of bylaws which regulate critical infrastructure, protection measures against cyber security risks in ICT systems, and incident response procedure. Through the adoption of laws and bylaws in this field of cyber security, Serbia has mostly harmonized with the NIS directive.
- ❖ **The Republic of North Macedonia** carries out awareness campaigns for all age groups – through Foundation Metamorphosis, For all groups, MKD-CIRT, Stop. Think. Connect for Youth & Children, and the government in cooperation with the private and non-governmental sector launched a campaign "Surf safe"

Average: Western Balkans vs Rest



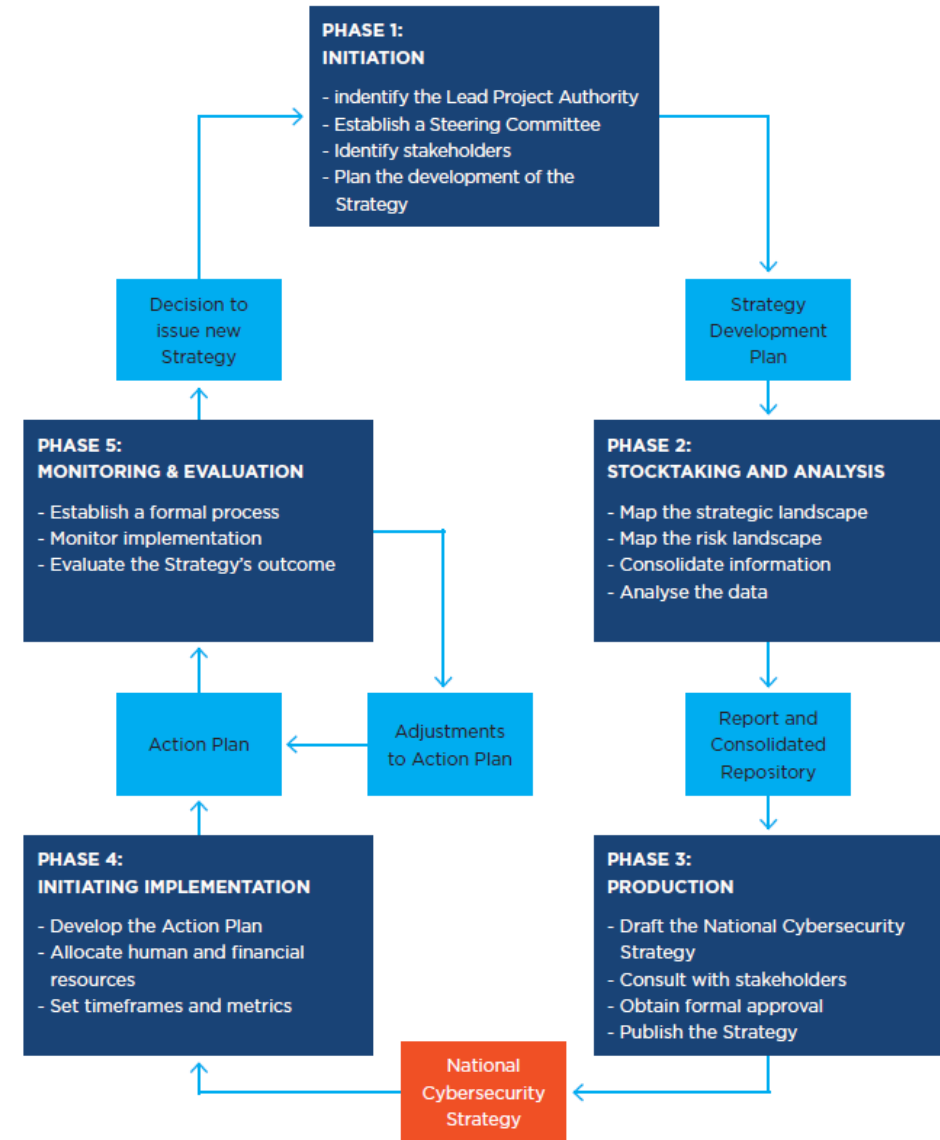
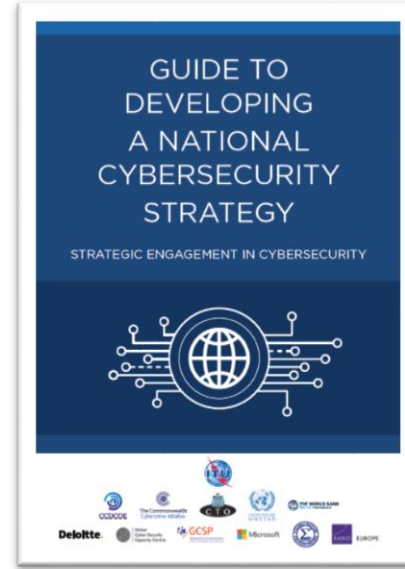
National Cybersecurity Strategy (NCS)

This Guide has primarily been structured as a resource to help government stakeholders in **preparing, drafting and managing** of the National Cybersecurity Strategy.

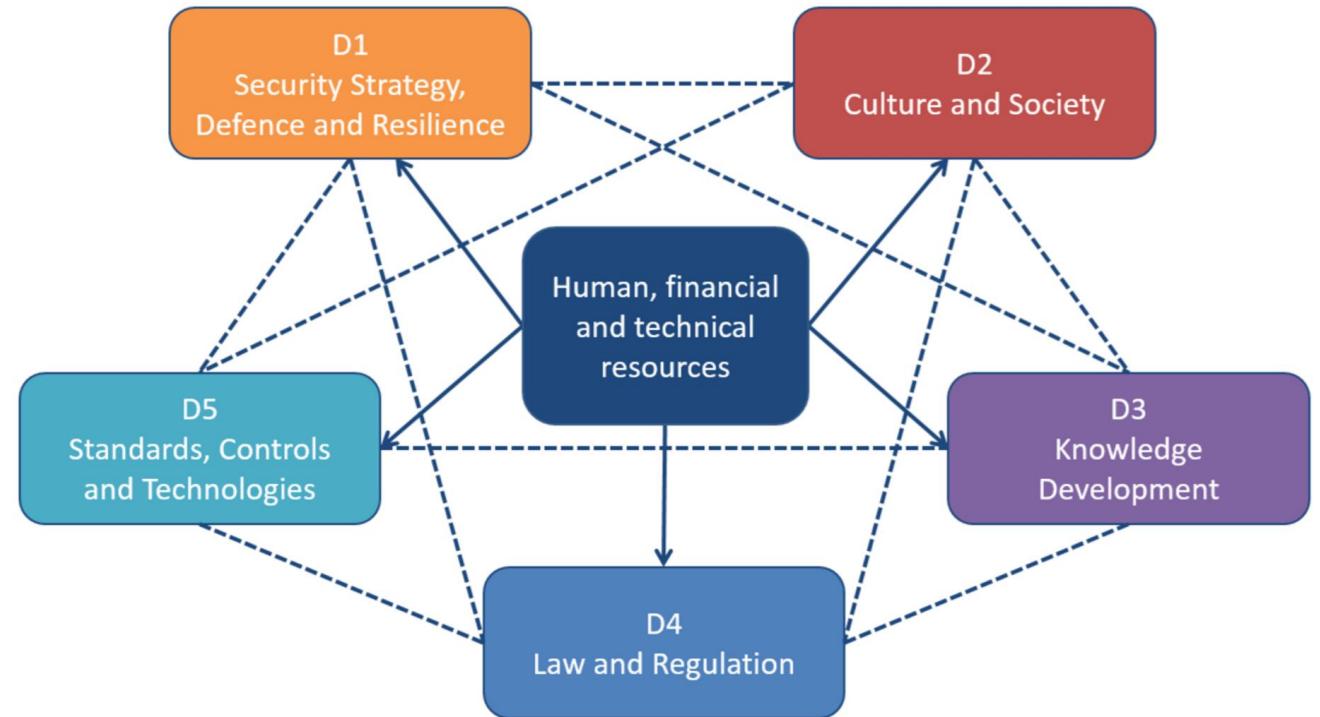
A joint effort of 12 partner organizations.

Released in September 2018 @ITU Telecom World

Available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf



Cybersecurity Capacity Maturity Model Assessments



Global
Cyber Security
Capacity Centre

OXFORD
MARTIN
SCHOOL



UNIVERSITY OF
OXFORD

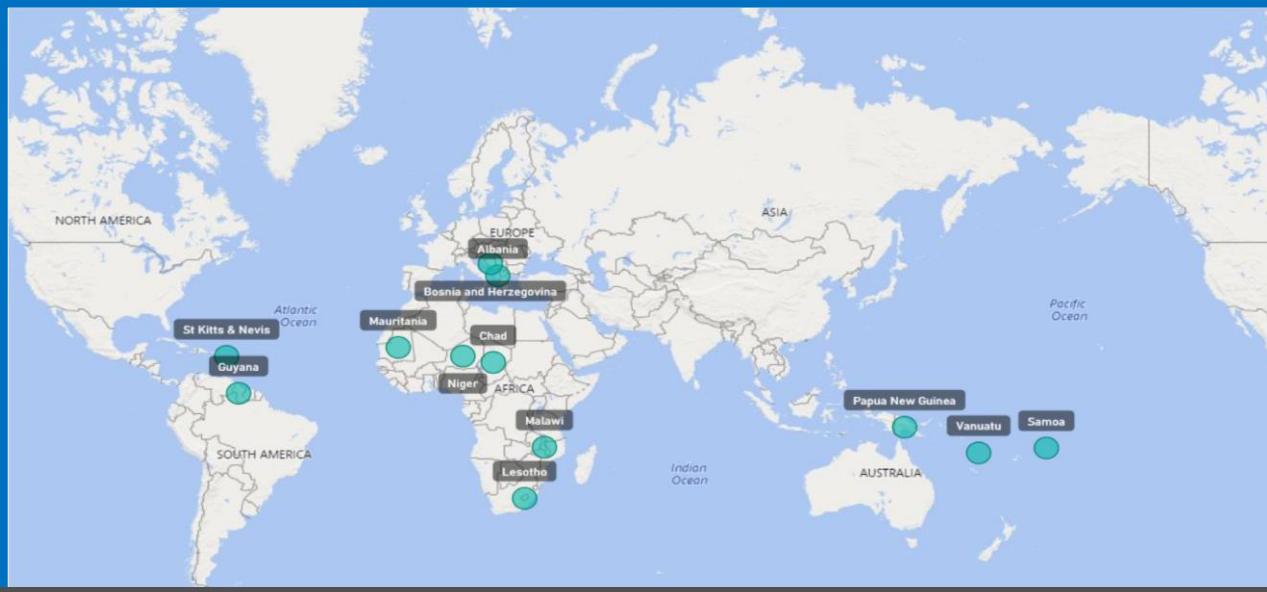
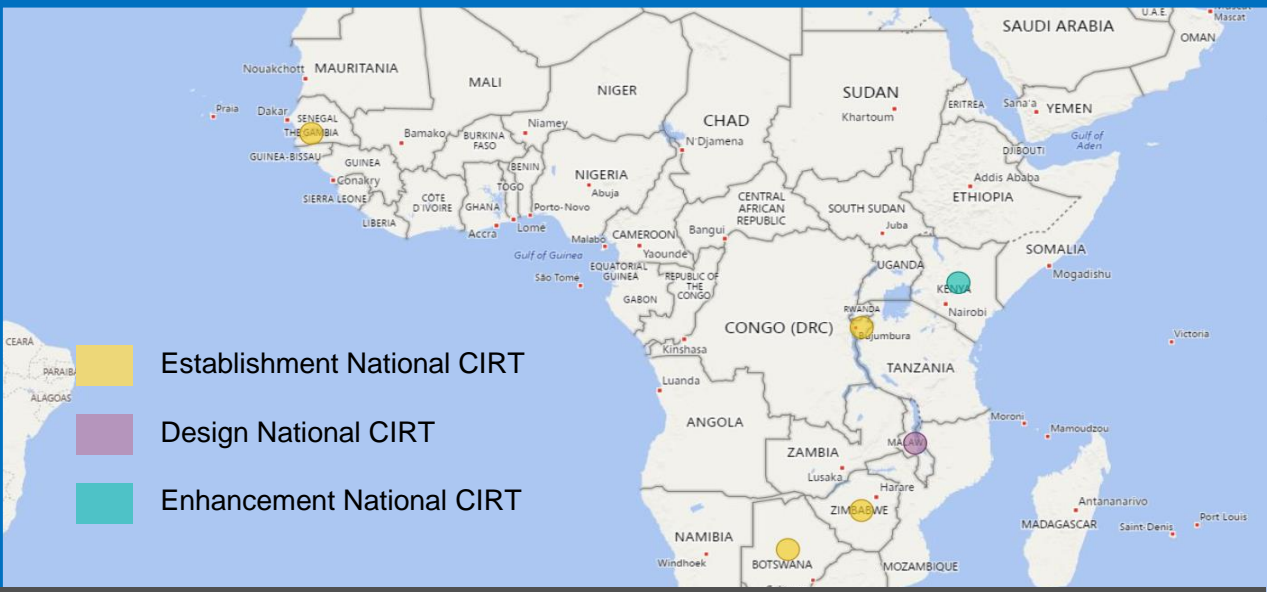
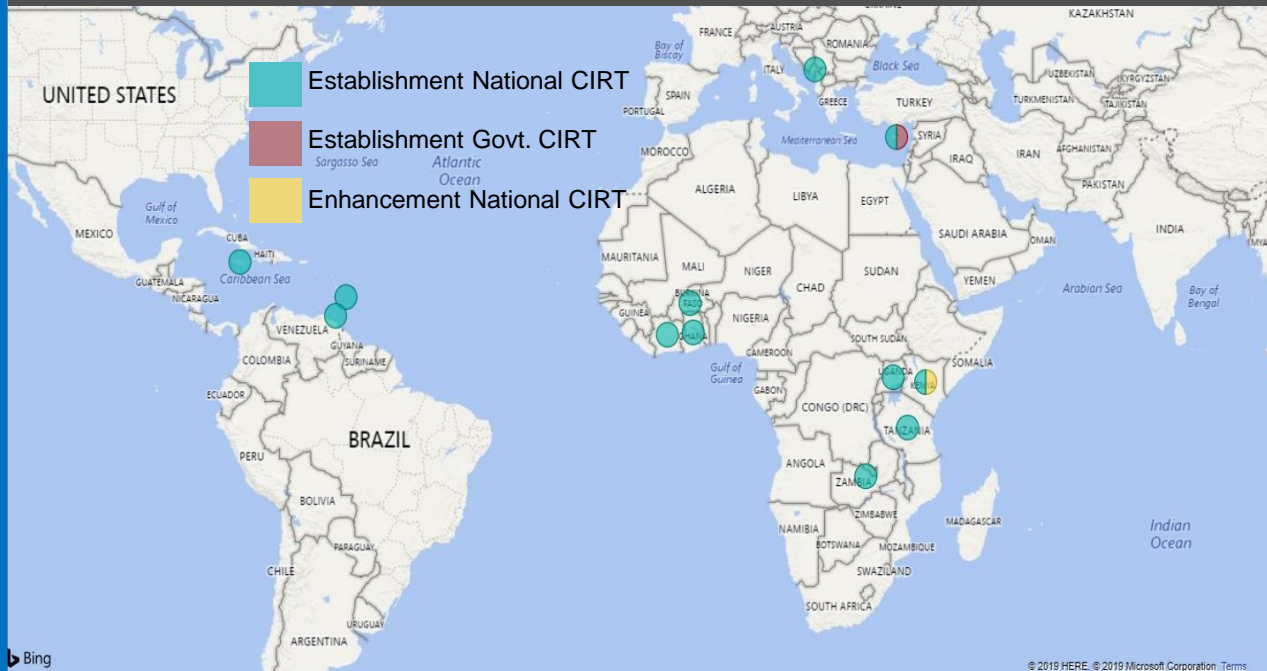
A decorative graphic consisting of two rows of three overlapping semi-circles. The top row is positioned above the text, and the bottom row is positioned below it. The semi-circles are in two shades of blue: a lighter, medium blue and a darker, royal blue. The overlapping areas create a gradient effect from light to dark blue.

CIRT Programme

77 CIRT READINESS ASSESSMENTS



13 CIRT ESTABLISHMENT + 1 ENHANCEMENT



CIRT ESTABLISHMENT IN 2019

CIRT ESTABLISHMENT- INTERESTS



Regional Cyberdrills -Objectives

1	Enhancing cybersecurity capacity and capabilities through regional collaborations and cooperation;
2	Enhancing the awareness and the capability of countries to participate and to contribute to the development and deployment of a strategy of defeating a cyber threat;
3	Strengthening international cooperation between Member States to ensure continued collective efforts against cyber threats;
4	Enhancing Member States' and incident response capabilities and communication;
5	Assisting Member States to develop and implement operational procedures to respond better to various cyber incidents, identify improvements for future planning CIRT processes and operational procedures

Regional Cyberdrills - Programme



1

Days 1 and 2 are dedicated to the organization of capacity building sessions, case studies or other themes-related training requirements, as well as COP-related issues, etc.

2

Day 3 is a conference day that includes presentations and panel discussions on current issues, latest assessment and current and emerging trends in cybersecurity threats and solutions.

3

Days 4 and 5 are structured around scenarios that consist of several incidents involving the most common types of attacks and possible resolutions.

CYBERDRILLS 2019



Europe - Romania
May 2019

Americas – Argentina
August 2019

Asia and Pacific + CIS
– Malaysia
September 2019

Arab States – Oman
October 2019

Africa – TBD
November 2019

ITUEvents

Europe Region
Cyberdrill

27-31 May 2019
Bucharest, Romania

Organised within the framework of the
ITU Regional Initiative for Europe on enhancing
trust and confidence in the use of ICTs



MINISTRY OF COMMUNICATIONS
AND
INFORMATION SOCIETY



CYBERDRILLS 2020



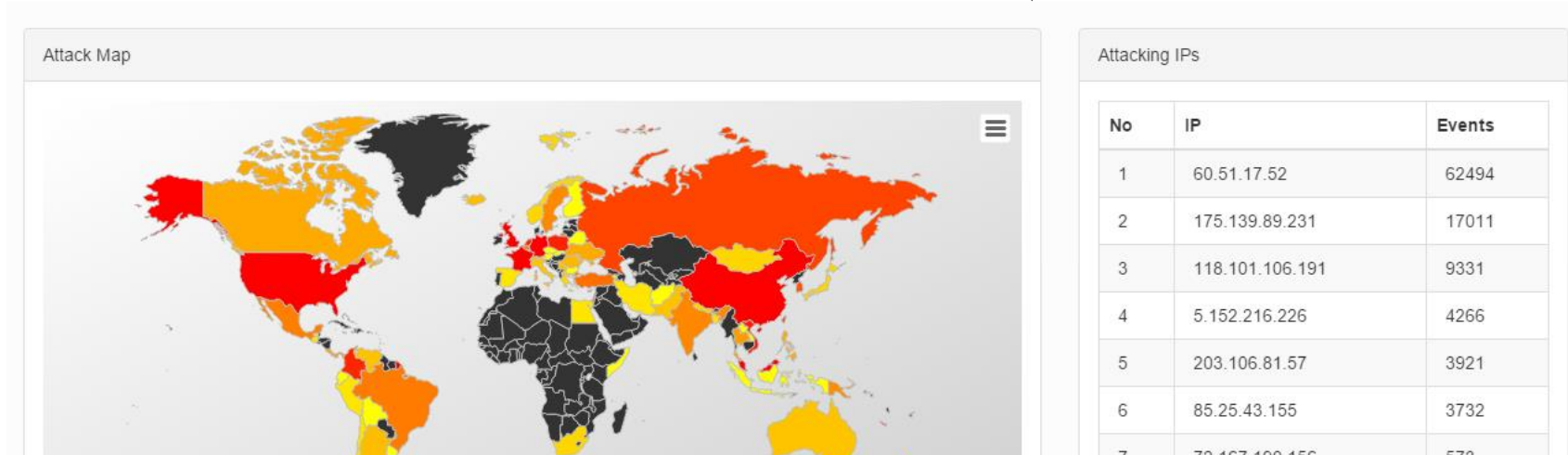
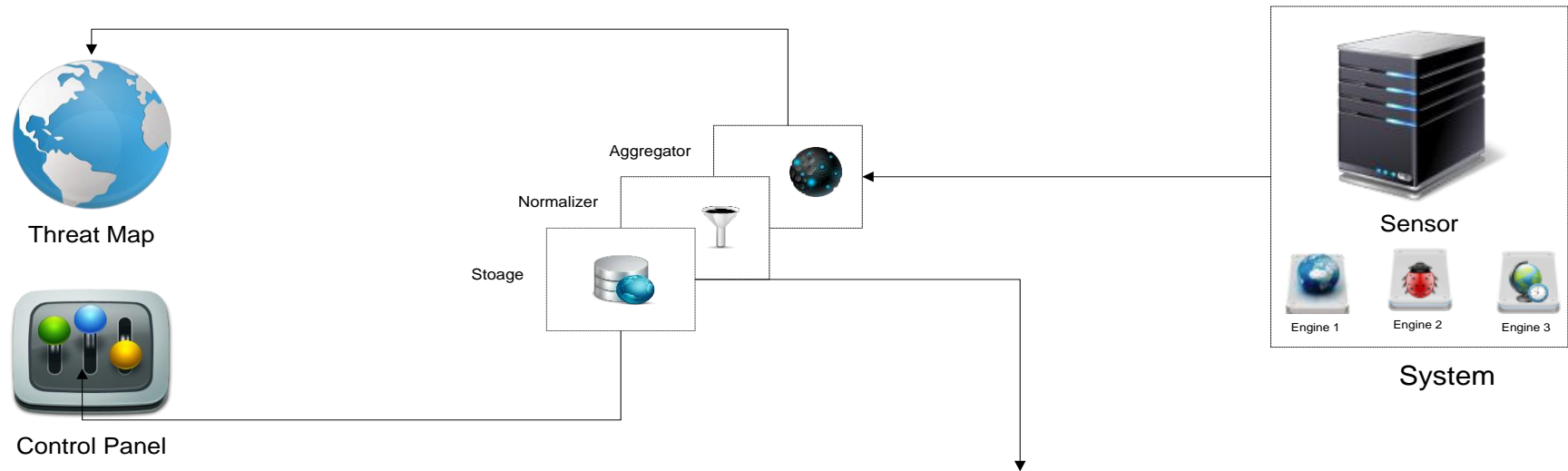
Europe - The Republic
of North Macedonia
June 2020

Arab States –
Kingdom of Saudi
Arabia
October 2020

A decorative graphic consisting of two rows of three overlapping semi-circles. The top row is above the text and the bottom row is below it. The semi-circles are in two shades of blue: a lighter blue and a darker blue. The overlapping areas create a pattern of varying blue tones.

The Honeyypot Research Network (HORNET)

Cyber Threat Intelligence – HORNET

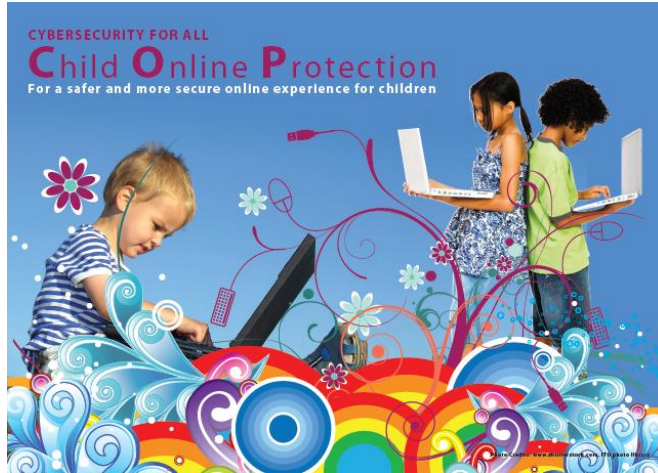


Dashboard

The main functions of the HORNET platform are:

- Enable countries to detect, recognize, and prevent attacks that target their cyberspace.
- Help the countries to strengthen the security monitoring of their cyberspace.
- Facilitate communication and improve collaboration between national CIRTs
- Play the role of a data sharing platform between National CIRTs

Child Online Protection [COP] Initiative



The COP Initiative aims at bringing together partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere.

Key Objectives:

- Identify risks and vulnerabilities to children in cyberspace
- Create awareness
- Develop practical tools to help minimize risk
- Share knowledge and experience

Cybersecurity Cooperation actions @ ITU

ITU STUDY GROUPS – Membership driven

ITU-D Study Group2 Question 3

- Securing information and communication networks: Best practices for developing a culture of cybersecurity

ITU-T Study Group 17 : Security

- Develop recommendations for future standards including in Cybersecurity

ITU-R Study Groups

- Securing radiocommunication networks

ITU Europe Events



ITUEvents

ITU Workshop for Europe on national cybersecurity strategies

26-28 June 2019
Skopje, North Macedonia

Follow us on Twitter @ITU_EUR
<http://itu.int/go/NCS-EUR-2019>

Organized within the framework of the ITU Regional Initiative for Europe on enhancing trust and confidence in the use of information and communication technologies.

Outcomes of this workshop will contribute to the Multiyear Digital Agenda 2018-2020 for the Western Balkans.



Hosted by



Republic of North Macedonia
**Ministry of Information
Society and Administration**

Co-organized by

DCAF Geneva Centre
for Security Sector
Governance



http://itu.int/go/EUR_EVENTS

Contact us



ITU Office for Europe

EURregion@itu.int

@ITU_EUR

<http://www.itu.int/go/EUROPE>

Cybersecurity Division

cybersecurity@itu.int

<https://www.itu.int/cyb>



SOME OF THE
ORGANIZATIONS WE WORK
WITH →



United Nations Office on Drugs and Crime