



OAS|CICTE

SECRETARIAT OF THE WORKING GROUP ON COOPERATION AND CONFIDENCE-BUILDING MEASURES IN CYBERSPACE

Inter-American Committee against Terrorism (CICTE)

Cybersecurity Program

Presentation Outline



Confidence Building Measures in Cyberspace:
CHS approval as a non-traditional confidence- and security-building measure (CSBM)

Establishment of the Working Group: Objective, Meetings, and Approved Cyber CBMs

Achievements (2022 -2023):

- Alignment of OAS/CICTE Cyber Diplomacy courses to the approved CBMs
- Prototype of the Improvement of the CBMs Portal Usage

2024 Workplan of the Technical Secretariat:

- Vision
- Key Focus Areas
- New Initiatives
- Cyber Diplomacy Trainings

Confidence Building Measures in Cyberspace

Cyberspace CBMs at the OAS

APPROVED CYBER MEASURES

The ultimate end-state desired of **CBMs for cyberspace** can be described as:

- I. A common understanding of acceptable State behavior in cyberspace;
- II. State of cyber stability in international relations.

2016 - CHS approval as a non-traditional confidence- and security-building measure (CSBM)

“Exchange information related to adopting and adapting provisions under domestic laws that govern processes for obtaining data and information, and exchange experiences involving government, service providers, end users and others, regarding prevention, management of, and protection against cyber threats, with a view to sustained mutual cooperation to prevent, address, and investigate criminal activities that threaten security and to ensure an open, interoperable, secure and reliable internet, while respecting obligations and commitments under international law and international human rights law, in particular.”



Working Group

Cooperation and Confidence-Building Measures in Cyberspace



APRIL 2017

Establishment of a Working Group on Cooperation and Confidence-Building Measures in Cyberspace through resolution **CICTE/RES.1.17**.



2017 – 2023

Working Group Meetings

February 2018
April 2019
July 2021
October 2022



2018 – 2023

11 CBMs

Currently the Working Group has incorporated **11 Cyber Confidence-Building Measures** "as non-traditional measures".

Points of Contact

Working Group on Cooperation and Confidence-building Measures in Cyberspace



82

**Cyber Policy
contacts**

19

**Ministry of Foreign
Affairs contacts**

Points of Contact

Working Group on Cooperation and Confidence-building Measures in Cyberspace

82

Cyber Policy
contacts

30

Countries

19

Ministry of Foreign
Affairs contacts



Achievements 2022 – 2023

CICTE's efforts as Technical Secretariat

1



Cyber Diplomacy Training Program

Alignment of trainings topics based on Approved CBMs

Supports the implementation of CBM:

CBM #4: Strengthen **capacity building** for public and private officials in **cyber diplomacy**

CBM #5: Incorporation of **cybersecurity and cyberspace issues** in **training courses** for diplomats and officials at the Ministries of Foreign Affairs and other government agencies

2



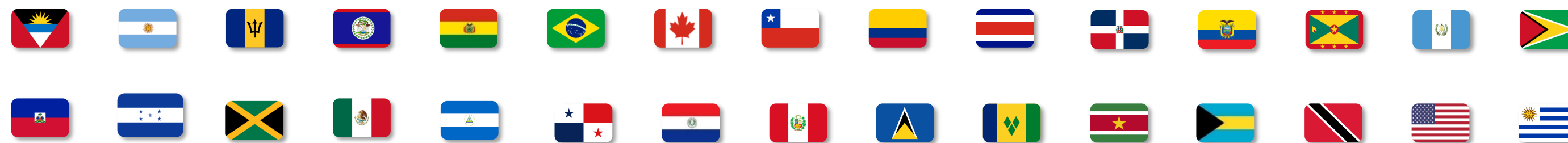
Improvement of the CBMs Web Portal

Supports the implementation of CBM:

CBM #1: Provide information on **cybersecurity policies**

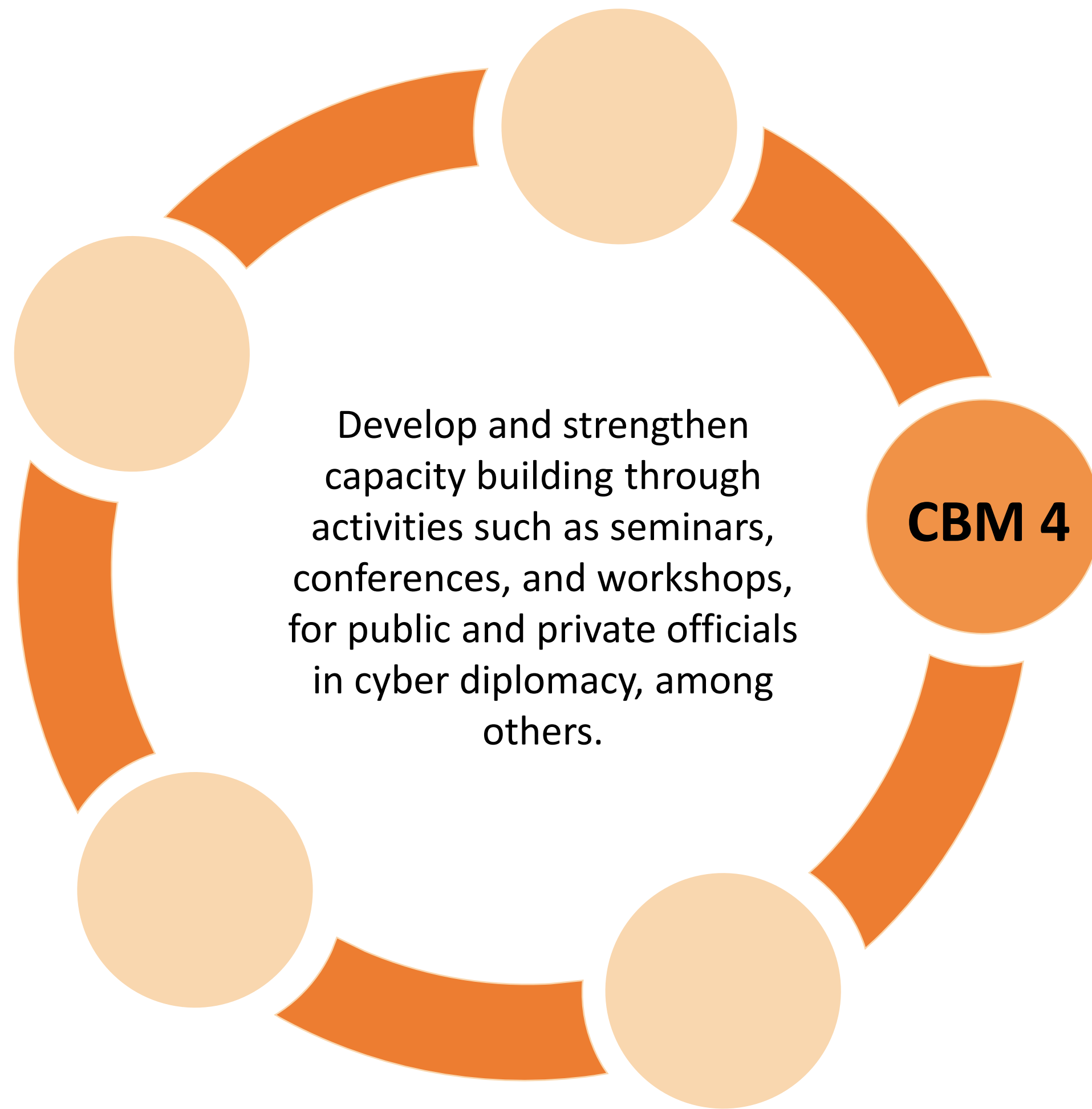
CBM #2: Designate a **national cyber point of contact** at the policy level.

CBM #3: Designate **points of contact** in the Ministries of Foreign Affairs



Achievements 2022 – 2023

CICTE's efforts as Technical Secretariat



February 2022

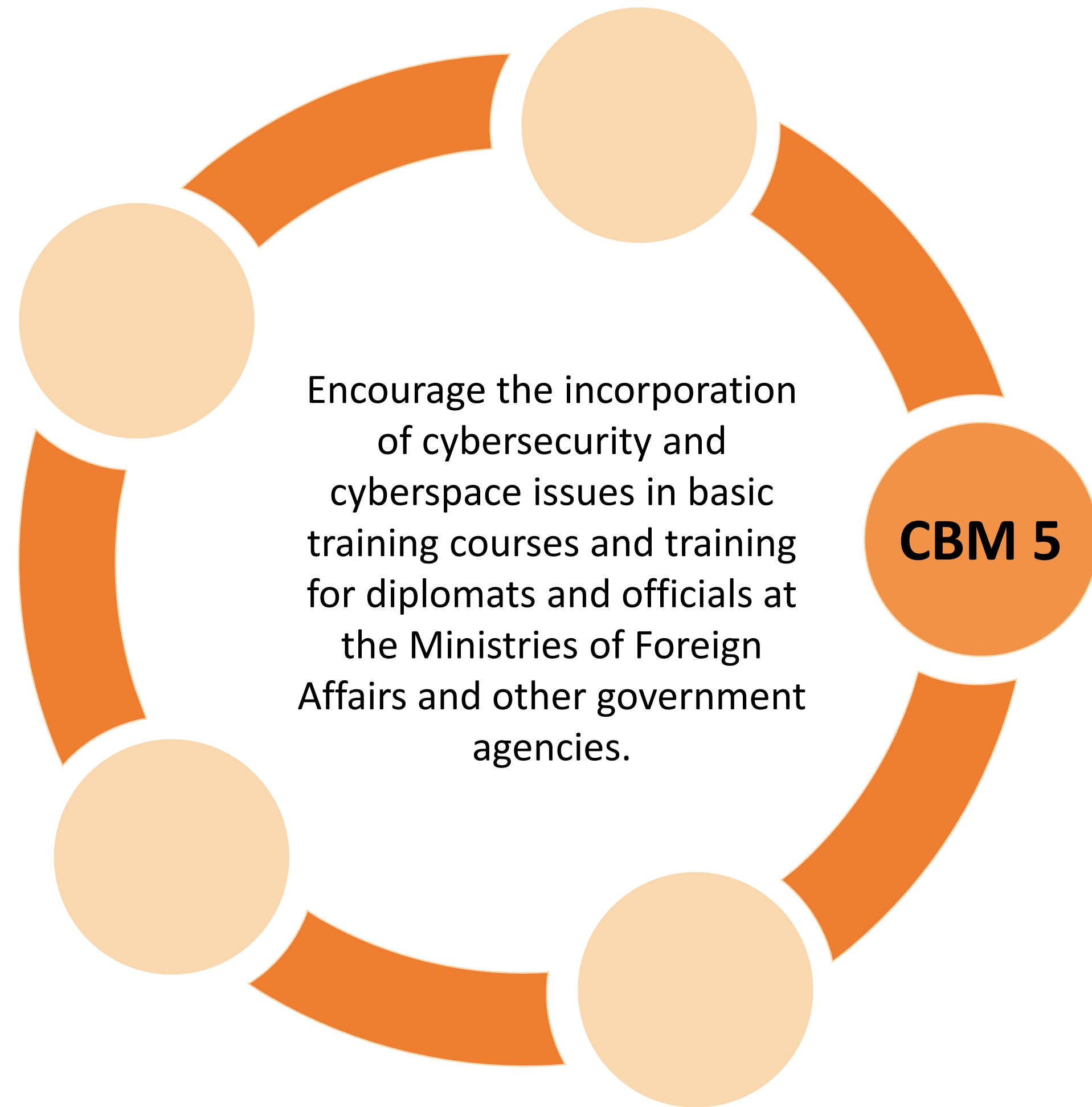
- International Cyber Diplomacy, Law and Norms

February 2023

- International Cyber Diplomacy, Law and Norms

Achievements 2022 – 2023

CICTE's efforts as Technical Secretariat



May 2022

- Cyber Diplomacy

November 2023

- Programme of Action for Advancing Responsible State Behaviour in Cyberspace



Achievements 2022 – 2023

CICTE's efforts as Technical Secretariat



October 2022

- Alumni Workshop: International Law of Cyber Operations
- Executive Course: International Law of Cyber Operations

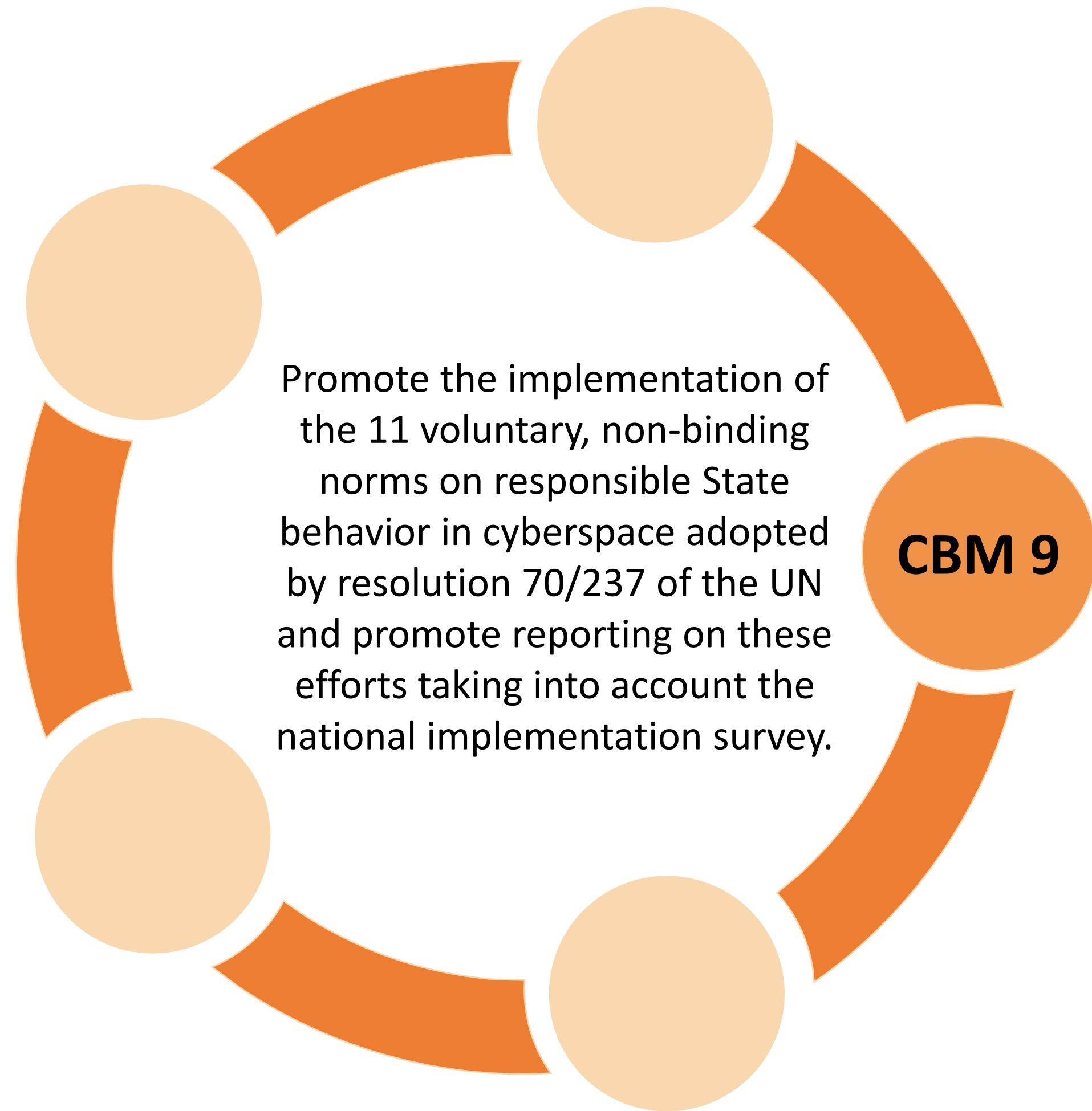
April 2023

- Application of International Humanitarian Law to Cyber Operations



Achievements 2022 – 2023

CICTE's efforts as Technical Secretariat



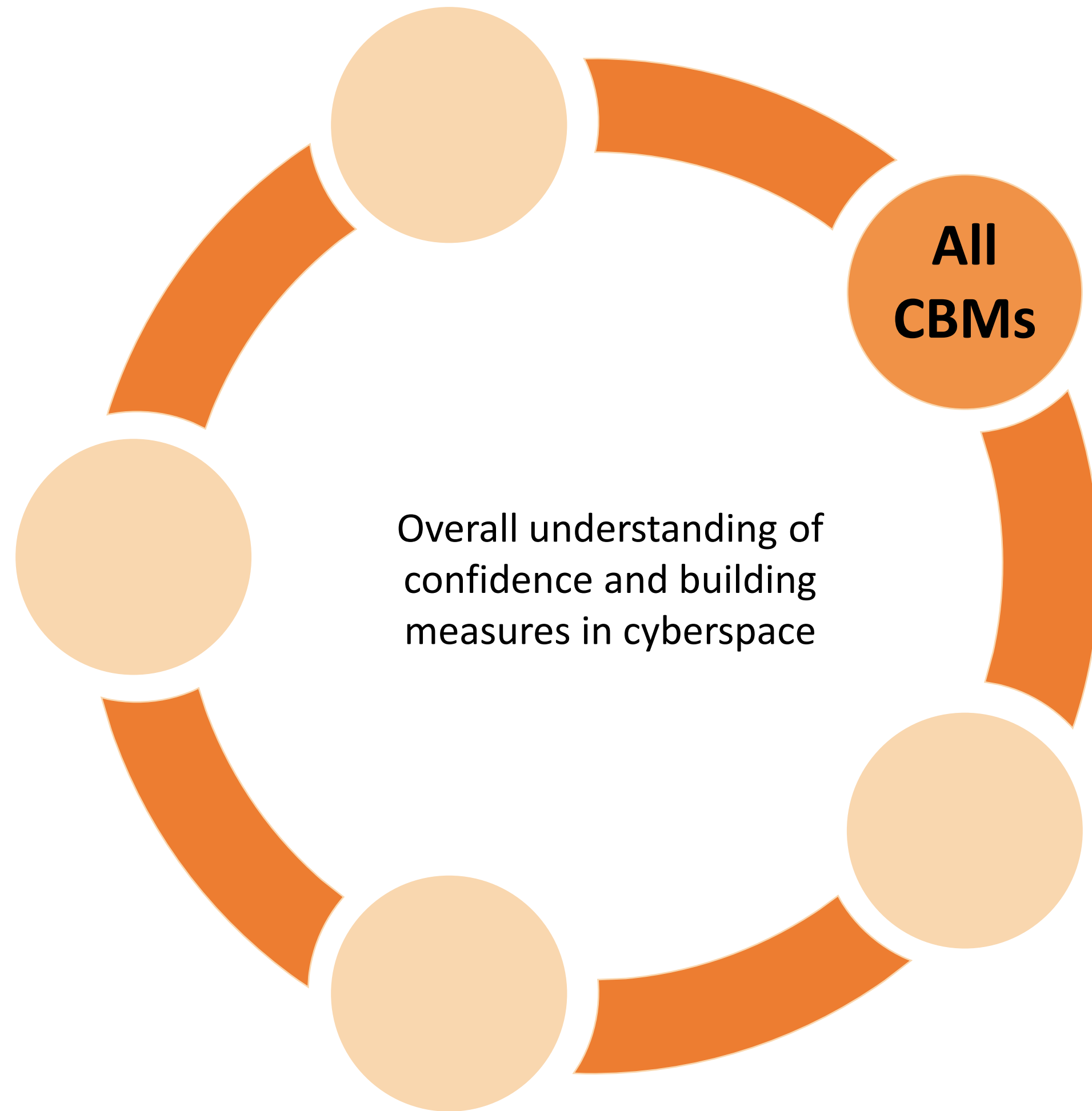
March 2023

- State Responsibility and Response Options



Achievements 2022 – 2023

CICTE's efforts as Technical Secretariat



November 2022

- Cooperation and Confidence-Building Measures in Cyberspace (CCBMS)

+500

Officials from the region trained in Cyber Diplomacy and Internal Law in the last 5 years

9

Cyber Diplomacy and Internal Law courses held from 2022 – 2023

22

Member States participating in OAS Cyber Diplomacy and Internal Law trainings

2024 VISION



“To strengthen and consolidate the Cyber CBMs Working Group by promoting active engagement among Points of Contact through a hands-on portal usage and establish synergies between cyber diplomacy and international law initiatives to support the implementation of approved CBMs”

Working Group on Cooperation and Confidence-Building Measures in Cyberspace

The Group focuses on non-traditional Confidence Building Measures (CBMs), specifically those related to cyberspace.

Key Focus Areas – 2024

Technical Secretariat Proposed Workplan



IMPROVEMENT OF
PORTAL SERVICES



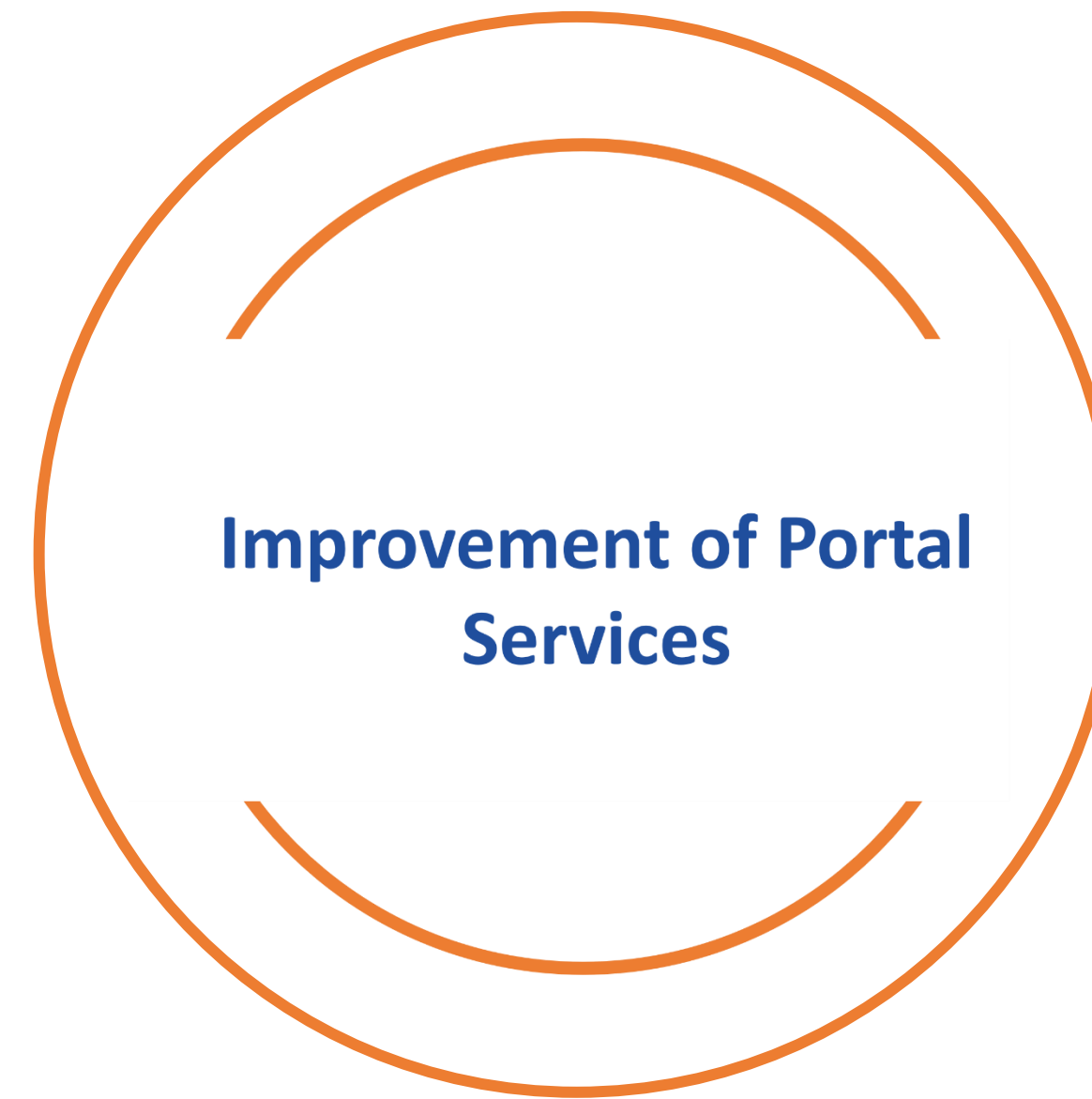
WEBINAR SERIES
INFORMATIVE
SESSIONS



ALIGNMENT OF
EXISTING AND
NEW CAPACITY
BUILDING
INITIATIVES WITH
APPROVED CBMS

New Initiatives

Technical Secretariat Proposed Workplan 2024



OAS | CICTE

New Initiatives

Technical Secretariat Proposed Workplan 2024



Information Session based on the agreed Cyber CBMs

- **Webinar 1 (CBMs 1, 2 y 3):** Points of Contact – *June 2024*
- **Webinar 2 (CBMs 4 y 5):** Capacity Building – *September 2024*
- **Webinar 3 (CBM 6):** Cyber diplomacy – *November 2024*

New Initiatives

Technical Secretariat Proposed Workplan 2024



**Improvement of Portal
Services**



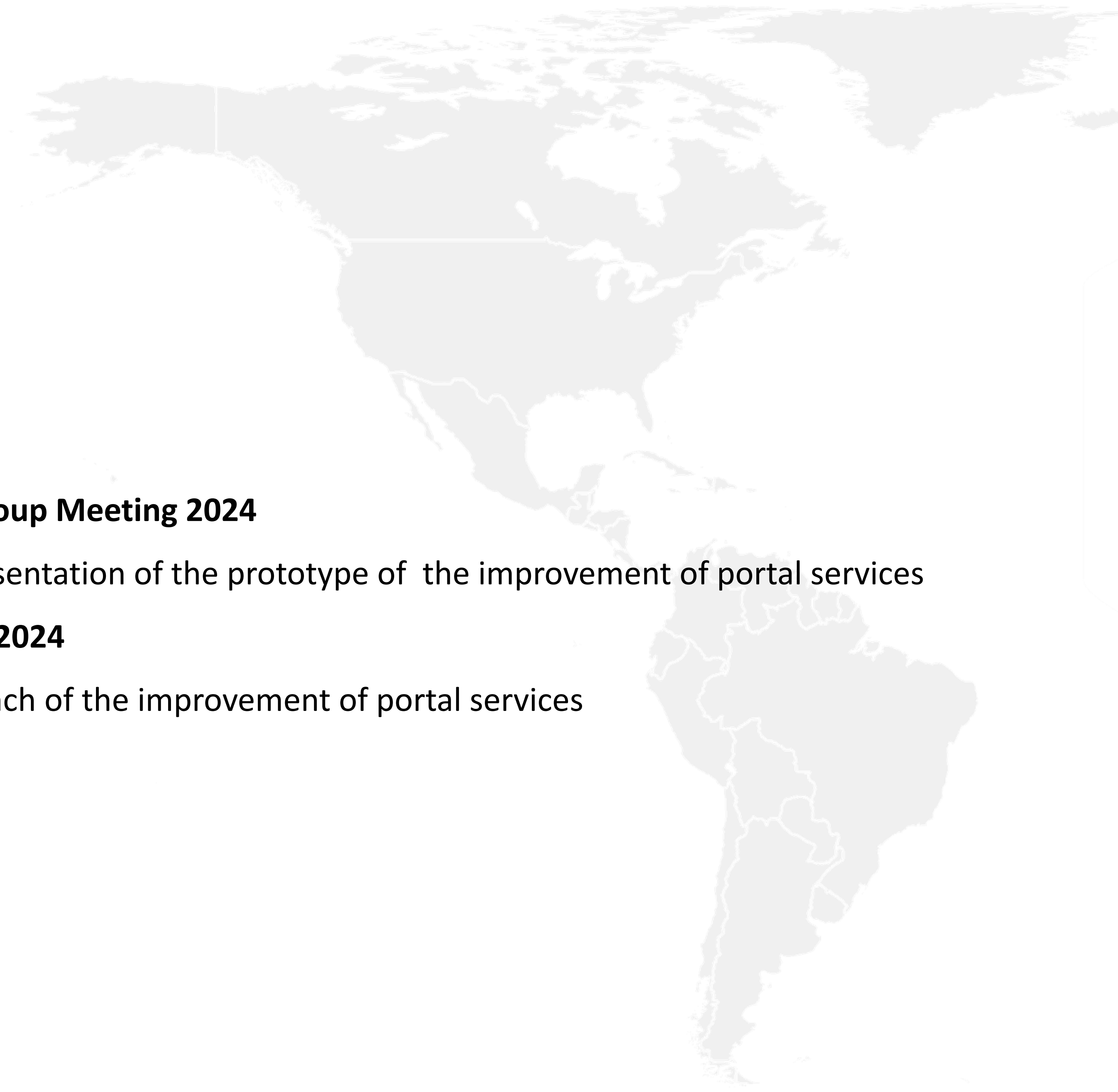
OAS | CICTE

Working Group Meeting 2024

- Presentation of the prototype of the improvement of portal services

September 2024

- Launch of the improvement of portal services



New Initiatives

Technical Secretariat Proposed Workplan 2024



National Dialogue on International Law in Cyberspace

A two-day capacity building series composed of a conference style on *Day 1* and interactive workshops on *Day 2*. The Dialogue aims to **foster discussion and a shared understanding of the application of international law in cyberspace, as well as enhance legal capacity at the national level.** Discussions will be tailored to **support the host country's needs in considering the development of a national position on international law in cyberspace.**

Security and Technology Fall School

Training program that addresses the capacity development gap in normative frameworks within the realm of emerging technologies and international security, particularly focusing on the ***intersection of international law, voluntary state behavior, information technologies, and artificial intelligence.*** The capacity building training is tailored for diplomats and policy-makers, all CBMs Points of Contact can benefit from this initiative.



Cyber Diplomacy Training Program

Technical Secretariat Proposed Workplan 2024



Scheduled Cyber Diplomacy Courses



Subregional Course – First Edition

“Securing the Digital Frontier: Cybersecurity and Critical National Infrastructure”

Date: May 2024



Virtual Masterclass – Based on CBM #7

“Cybersecurity and Human Rights: Gender-Inclusive Approach to Digital Freedom and Security”

Date: April 2024



Short Intensive Courses – 4-week training program

- Week 1: *Artificial Intelligence Policy*
- Week 2: *Cybersecurity Diplomacy*
- Week 3: *Digital Diplomacy*
- Week 4: *Interactive discussions*

Date: August 2024

Since 2017

+850
officials trained

+26
courses held

28
Member States' participation



CBMs Implementation Survey

Circulated by the Chair



| | |
|--|---|
| | |
| <p>Does your government have a full understanding of the CBMs and how to implement them?</p> | <p><i>There is a need to deepen the understanding of promotion measures, as well as the 11 non-binding voluntary standards adopted in resolution 70/237 of the United Nations General Assembly.</i></p> |
| <p>What type of challenges is your Government facing in implementing any of the eleven cyber CBMs?</p> | <p><i>Human resource capacity in the different relevant sectors and lack of policy instruments are the top challenges for CBM implementation.</i></p> |
| <p>Are there measures of engagement or assistance that would help your Government implement the cyber CBMs?</p> | <p><i>Continuous training and workshop. Adapting to best practices and making our legislation more current.</i></p> |
| <p>What additional regional initiatives do you consider can be executed to help your Government in the implementation of CBMs?</p> | <p><i>For our country, the idea of a repository of cyber incidents that can function as a didactic platform and as a transparency mechanism is still attractive.</i></p> |



OAS|CICTE

**Thank you!
Merci
Gracias
Obrigado**

**Kerry-Ann Barrett
Mariana Jaramillo
Nelson Guanilo**

Cybersecurity Program
Inter-American Committee against Terrorism
Organization of American States
cybersecurity@oas.org
www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

Twitter
@OEA_Cyber