
10 YEARS
of OSCE Cyber/ICT Security
Confidence-Building Measures
OSCE

TIMELINE OF MAJOR EVENTS

2012

Open-ended **Informal Working Group (IWG) established** under the auspices of the Security Committee *(Permanent Council Decision No. 1039).*

2013

Eleven transparency measures adopted *(Permanent Council Decision No. 1106).*

2016

MARCH

Five co-operative measures adopted *(Permanent Council Decision No. 1202).*

NOVEMBER

OSCE Secretariat conducts **first Communications Check** for the CBM 8 Point of Contact network.

DECEMBER

Foreign Ministers of OSCE participating States **endorse the CBMs** at the Ministerial Council *(Decision No. 5/16).*

2017

Ministerial Council Decision *(No. 5/17)* agree to place a **specific focus on CBM implementation.**

2018

"Adopt-a-CBM" initiative introduced by IWG Chair.

IN THE PAST 10 YEARS

2019

First meeting of the **CBM 8 Points of Contact** in Vienna.

2020

OSCE Secretariat introduced **online expert sessions.**

2021

E-learning course on OSCE's cyber/ICT security **CBMs.**

2022

SEPTEMBER

E-learning course on CBM 16 Coordinated Vulnerability Disclosure.

NOVEMBER

CBM 15 report on ***"Cyber Incident Classification:*** *A Report on Emerging Practices within the OSCE region".*

2023

CBM 14 report on *"Emerging Practices in* ***Cybersecurity-Related Public-Private Partnerships*** *and Collaboration in OSCE participating States".*

Foreword by the OSCE Chairman-in-Office

In today's interconnected world, where Information and Communication Technologies (ICTs) have become the backbone of communication, commerce, and diplomacy, the need for a secure and co-operative cyberspace cannot be understated. The Organization for Security and Co-operation in Europe (OSCE) has emerged as a pioneer in enhancing cyber/ICT security. OSCE, the largest regional security organization that has a rich history in traditional arms control, in addition has successfully adapted its expertise to the digital age, focusing on building confidence with the aim to reduce the risks of conflict arising from the use of ICTs by its participating States.

At the heart of these efforts are confidence-building measures (CBMs), practical and non-binding measures aimed at enhancing transparency, co-operation, and stability in cyberspace. These measures have evolved to address emerging challenges, covering areas in the scope of sharing cybersecurity-related information and critical infrastructure protection, thus creating cyber resilience in the participating States.

In December 2013, when OSCE participating States adopted the first set of confidence-building measures which focus on increasing transparency through voluntary exchange of information between participating States, thus identifying common problems and seeking joint solutions.

These measures include sharing national perspectives on ICT threats, fostering co-operation among relevant national bodies, conducting consultations to reduce misperception and protect critical ICT infrastructure, and exchanging information on ensuring a secure internet. OSCE serves as a platform for dialogue, encourages modern national legislation for co-operation, and facilitates communication through contact points and terminology sharing, through the established Informal Working Group under the PC Decision 1039.

The 10th Anniversary of the first set of cyber/ICT security CBMs, as well as the current security circumstances in Europe remind us that we need to make more in meaningful implementation of CBMs for the benefit of people in the OSCE Region. As Chairman in Office of the OSCE, I once again reiterate that our firm commitment to consistent focus on cyber/ICT security will be added value in reaching the comprehensive security in Europe. These CBMs are probably one of the most effective means that exist in the OSCE toolbox.

This booklet explores collaborative efforts between CBM adopters and the OSCE Secretariat, resulting in the development of valuable cyber capacity-building tools, including also insightful reports.

In conclusion, this account of OSCE's journey in enhancing cyber/ICT security through CBMs reflects the organization's commitment to creating a safer and more stable cyberspace. As you explore these pages, you'll gain an understanding for the co-operation driving this vital endeavour. OSCE has not only adapted to the digital age but has also embraced it, showing the way forward for regional and international organizations in the pursuit of cyber stability.

OSCE functionality and relevance lie in its tools. CBMs on cyber/ICT security are important tools that have proved being one of the best in the list. Therefore, we better implement them. It's about people!

BUJAR OSMANI
Chairman-in-Office

Foreword by the OSCE Secretary General

2023 marks the 10th anniversary of the adoption of the first set of cyber/ICT security confidence-building measures (CBMs) at the Organization for Security and Co-operation in Europe (OSCE). The adoption of the CBMs in 2013 signaled a breakthrough in international cyber policy negotiations, with the OSCE being the first regional security organization to adopt concrete measures in support of discussions at the United Nations.

The OSCE pioneered these efforts with the aim to reduce the risks stemming from the use of ICTs, and to foster transparency and co-operation in the OSCE area. CBMs may be voluntary and non-binding, but participating States have made a political commitment to adhere to these measures and they are making a real difference. Over the past decade, the OSCE has become a global leader in the practical and meaningful implementation of cyber/ICT security CBMs, thanks to the active engagement of its participating States and with the support of the OSCE Secretariat.

These efforts have paved the way for new partnerships among states from various OSCE sub-regions and have fostered co-operation between neighbouring countries. The objective is to increase national cybersecurity resilience and thereby make the OSCE participating States more secure in cyberspace. The concrete results of these efforts include publicly available capacity-building tools that not only promote the OSCE's work in this field but also serve as inspiration for other regions when embarking on the path of confidence-building.

OSCE participating States have affirmed the continued relevance of cyber/ICT security CBMs and have intensified efforts towards their practical implementation. They have made the enhancement of national capacities and cybersecurity skills a top priority, signalling that international co-operation remains both possible and mutually beneficial.

This publication takes stock of the work the OSCE has done over the past decade and marks the significant achievements along the way. It serves as a reminder of the importance of working together towards common goals and shared values, and as an inspiration to all of us to continue discussions on cyber/ICT security in the OSCE, as well as in other international fora. We have come a long way and look forward to continued progress.

HELGA MARIA SCHMID
OSCE Secretary General

Introduction to CBMs

The Organization for Security and Co-operation in Europe (OSCE) is the largest regional security organization with a comprehensive approach to security and vast experience in traditional arms control. It is a pioneer in enhancing cyber/ICT (Information and Communication Technologies) security, in particular by **reducing the risks of conflict stemming from the use of ICTs by its participating States.** With States increasingly using ICTs to pursue their foreign policy objectives, these technologies add a complex dimension to inter-state relations. To address this, participating States have **developed and adopted a set of confidence-building measures (CBMs)** to reduce the risks of conflict stemming from the use of ICTs.

In 2012, an open-ended **Informal Working Group** (IWG) was established under the auspices of the Security Committee *(Permanent Council Decision No. 1039)* with the mandate to elaborate a set of CBMs to **enhance interstate co-operation, transparency, predictability and stability,** and to reduce the risks of misperception, escalation and conflict that may stem from the use of ICTs.

Since then, participating States have adopted two sets of CBMs:

- **Eleven transparency measures adopted in 2013** *(Permanent Council Decision No. 1106),* which promote cyber resilience and preparedness, encourage communication and increase transparency.
- **Five co-operative measures adopted in 2016** *(Permanent Council Decision No. 1202),* which further address effective communication channels, public-private partnerships (PPPs), critical infrastructure protection and the sharing of vulnerability information.

The 16 CBMs aim to build multi-layered relationships based on openness and co-operation and lay a foundation for the peaceful resolution of disputes in cyberspace. Whilst **the measures are non-binding, all 57 participating States made a political commitment to adhere to them.**

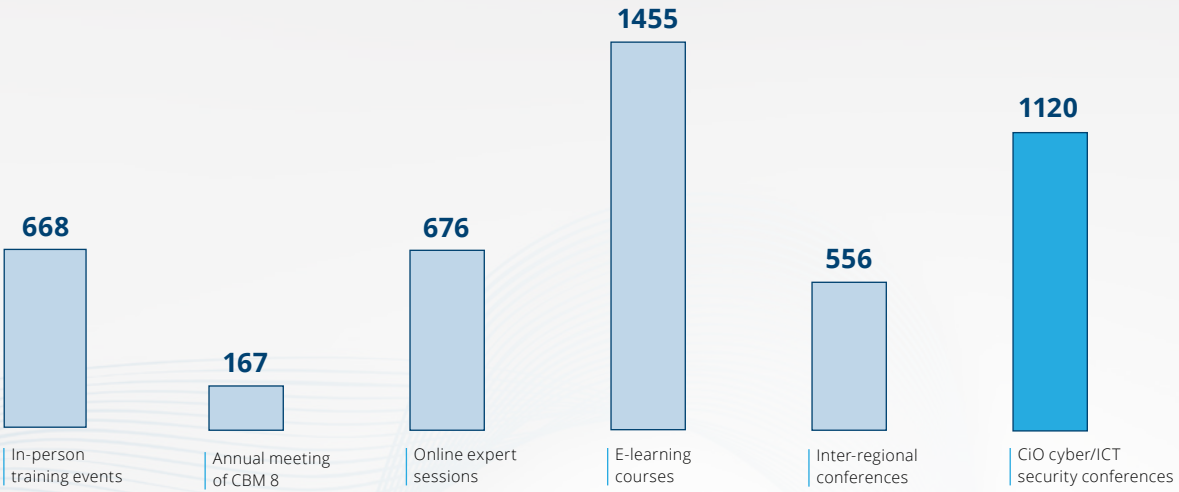
In 2016 and 2017, **the foreign ministers of the OSCE participating States reaffirmed their commitment to the CBMs and agreed to place a specific focus on implementation,** drawing attention to using the CBMs in practice *(Ministerial Council Decision No. 5/16 and Ministerial Council Decision No. 5/17).*

The role of the OSCE Secretariat

The OSCE Secretariat's Transnational Threats Department assists participating States in their efforts to implement cyber/ICT security CBMs both at national and regional levels. For example, the Department organizes a range of activities designed to enhance states' capacities to tackle cybersecurity-related threats, with a key focus on regional co-operation. These include **training events** on topics such as sub-regional co-operation, the applicability of international law in cyberspace, cyber diplomacy and other specialized topics.

To complement these in-person activities, the OSCE also organizes **a series of online events,** which include dedicated expert sessions for the CBM 8 PoC network or the OSCE Cybersecurity Awareness Month.

NUMBER OF PARTICIPANTS IN OSCE EVENTS ON CYBER/ICT SECURITY



In recent years, the exchanges and co-operation with other regional organizations that have already developed, or are in the process of negotiating, their own regional cybersecurity confidence-building measures, have also increased. The OSCE regularly contributes to inter-regional co-operation activities and shares lessons learned, while publications about OSCE's good practices on implementing specific CBMs are publicly available to serve as an inspiration to other regions.

In order to highlight the practical applicability of the cyber/ICT security CBMs, the OSCE Secretariat developed a general e-learning course featuring the diverse and extensive work in the OSCE region on operationalizing these measures.

Expected learning effort:
2 hours (self-paced)

Certificated offered:
Certificate of completion

Language:
English, French, Russian

OSCE e-learning platform:
https://elearning.osce.org/

As at 1 October 2023, there are **more than 1240 learners** enrolled in this course.

Chairpersonships-in-office

Since the adoption of the first set of CBMs, OSCE Chairpersonships-in-Office (CiO) began organizing **workshops and conferences** dedicated to **cyber/ICT security** as one of their key priority areas:

Serbia 2015 — Workshop on global, regional and sub-regional co-operation to support the implementations of CBMs

Germany 2016 — Workshop on reducing the risks of conflict stemming from the use of ICTs

Austria 2017 — Annual conference on the protection of critical infrastructure

Italy 2018 — Annual conference on cyber/ICT security CBM implementation

Slovakia 2019 — Annual conference on multilateralism in cyber diplomacy

Albania 2020 — Annual conference on multi-stakeholder co-operation in cyberspace

Sweden 2021 — Annual conference on a comprehensive approach to cyber/ICT security

Poland 2022 — Annual conference on raising social awareness, promoting cyber in education and building cyber resilience

North Macedonia 2023 — Annual conference on comprehensively addressing cyber security challenges and improving resilience across different sectors

Implementation of cyber/ICT security CBMs

Since 2015, the **rate of CBM implementation has risen from 61% to 98%,** measured as participating States implementing at least one of the 16 CBMs at national level. Regular reporting of national developments in the field of cyber/ICT security related to the CBMs is encouraged in the IWG, but also in various activities during the training events and workshops organized by the OSCE Secretariat. On a voluntary basis, States can also share information related to the implementation of CBMs on an online platform, thus making the information available to the other participating States.

THE OSCE DEVELOPED A SERIES OF CONFIDENCE-BUILDING MEASURES (CBMs) TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF ICTs IN THE OSCE REGION:

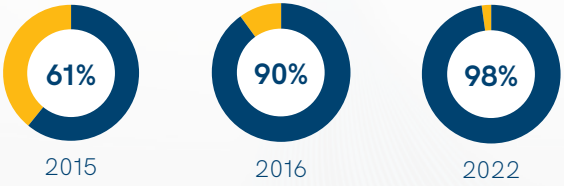
Crisis Communications Channels

Greater Co-operation

Understanding States' postures on the use of ICTs

Critical infrastructure Protection

Use of CBMs by participating States



Points of Contact Network

56/57

Participating States
Ready to Communicate

CBM 8 POINT OF CONTACT NETWORK

The **most implemented CBM** to this day is No. 8, with **56 participating States having nominated at least one Point of Contact (PoC)** and made that information available to other States. The OSCE maintains an up-to-date directory of CBM 8 PoCs on an online platform and supports the network's further development into a community of cyber policy and technical experts on the basis of common experiences and practical interactions.

For a number of years, the OSCE Secretariat has worked with participating States to build a strong network of technical and political PoCs, with the aim of fostering trust and co-operation. By organizing regular meetings and facilitating bilateral exchanges between them, **the OSCE has transformed a list of names into a community of policymakers that work together to promote cyber stability.**

To ensure that the CBM 8 PoC Network is up to date and functioning properly, the OSCE organizes regular communication checks—short exercises designed to check the relevance of the contact information as well as practice communication between PoCs in the event of a real incident. These checks include tasks ranging from responding to simple questions to complex scenarios that require collaboration between PoCs from different participating States.

The "Adopt-a-CBM" initiative

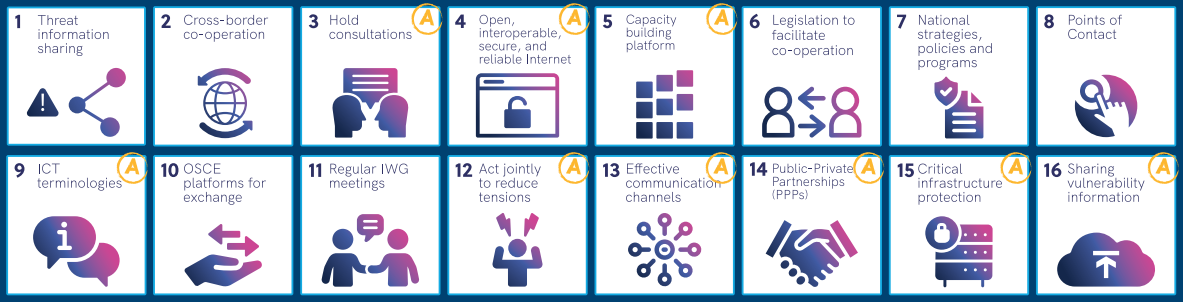
The national implementation of the CBMs is a voluntary commitment by each participating State, however the **measures adopted at the political level need to be put into practice to be meaningful.** With the aim of encouraging the OSCE-wide implementation of CBMs and co-operation between participating States, the 2018 **Chair of the IWG inaugurated the "Adopt-a-CBM" initiative,** which encourages participating States to **champion the implementation of specific CBMs.** It invites them to explore concrete modalities for achieving national- and regional-level CBM implementation. Over the years, it has proved fruitful and has substantially contributed to an increase in the practical implementation efforts, with a substantial number of participating States joining the initiative. So far, nine CBMs have been adopted by 23 participating States.

"For over a decade, the OSCE Informal Working Group on cyber/ICT security has been working on confidence-building measures to increase interstate co-operation, transparency, predictability, and stability. The sixteen measures are not only relevant for the OSCE, but further support the United Nations framework for responsible state behavior in cyberspace. As key tools for strengthening international peace and security, we must continue working on their implementation. One such effort is the "Adopt-a-CBM" initiative, which has already gathered almost half of the OSCE participating States to share good practice examples. I am heartened by the active engagement of participating States and our shared commitment to continuing the practical focus of our work."

Ambassador Christophe Kamp
Permanent Representative of the Kingdom of the Netherlands
in the OSCE and Chair of the Informal Working Group

CBM 8 and CBM 11 are not part of the "Adopt-a-CBM" initiative and can be considered as continuously implemented: CBM 8 through the OSCE Secretariat's activities related to the PoC Network and CBM 11 by ensuring that the meetings of the Informal Working Group are convened at least three times a year.
CBMs 3, 4, 5, 9, 12, 13, 14, 15 and 16 are championed through the "Adopt-a-CBM" initiative.

OSCE CYBER/ICT SECURITY CBMs



A * *championed through the "Adopt-a-CBM" initiative*

Some of the CBMs have only been **adopted by one participating State,** while other measures are championed **by a group of countries,** requiring additional co-operation and co-ordination. As a result of these efforts, a variety of activities have taken place, benefitting all participating States. Every group has issued **discussion papers,** which lay down the vision for the OSCE-wide implementation of the specific CBM, while other adopter groups have reached out to participating States through **questionnaires,** to map the national state of play and positions related to the specific CBMs. Organizing **events with expert speakers** on specific topics has also become a popular approach to explore the modalities for implementing a CBM. The concrete results of such CBM adopter co-operation are **publicly available capacity-building tools,** like a database of ICT-related terminology, an e-learning course and good practice reports.

CBM 9 – A GLOSSARY OF ICT-RELATED TERMINOLOGY IN THE OSCE REGION

Serbia decided to be an adopter of CBM 9, which refers to national terminologies and definitions of terms in the field of information security. A publicly available website (cbm9.gov.rs) was set up to provide **a glossary of cyber/ICT security-related terminology derived from official documents of the OSCE participating States** and translated into the official languages of the OSCE. There is currently no intention to develop a consensus terminology, however Serbia plans to undertake an analysis of the used terminology, as well as the similarities and differences in definitions. **As at October 2023, the glossary comprises more than 2000 terms.**

Joint activities for CBM implementation

Over the years, the OSCE Secretariat's Transnational Threats Department has developed **projects to support the implementation of CBMs** and the activities of the adopter groups. Such support included the development of an e-learning course, conducting research and publishing good practice reports. These resulted in publicly available cyber capacity-building tools.

E-LEARNING COURSE ON COORDINATED VULNERABILITY DISCLOSURE, CBM 16

To support the implementation of CBM 16, the OSCE Secretariat has developed a specialized e-learning course on the topic of coordinated vulnerability disclosure — a process on managing ICT vulnerabilities in a way that minimizes their harm. **The e-learning course provides an overview of coordinated vulnerability disclosure as a tool to strengthen national, regional and international cybersecurity.**

Expected learning effort:
2 hours (self-paced)

Certificated offered:
Certificate of completion

Language:
English

OSCE e-learning platform:
https://elearning.osce.org/

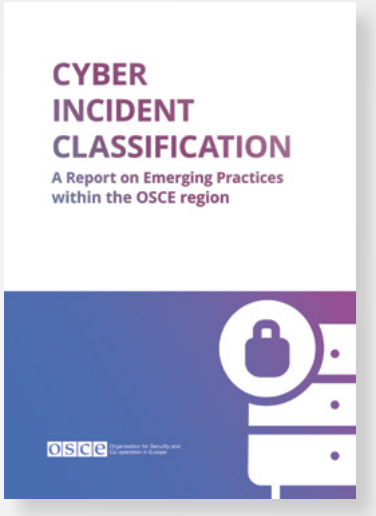
As at 1 October 2023, there are **more than 260 learners** enrolled in this course.

REPORT RELATED TO CBM 14 – EMERGING PRACTICES IN CYBERSECURITY-RELATED PUBLIC-PRIVATE PARTNERSHIPS AND COLLABORATION IN OSCE PARTICIPATING STATES, MARCH 2023

The report builds upon previous studies carried out by participating States, which gathered examples of public-private partnerships (PPPs) in cyber/ICT security. It is based on a series of interviews the OSCE Secretariat conducted with public sector representatives actively involved in co-operation with the private sector. **The report highlights examples of existing practice from OSCE participating States and provides baseline recommendations to promote public-private collaboration** as an important element in strengthening national cyber resilience and international cyber stability.

REPORT RELATED TO CBM 15 – CYBER INCIDENT CLASSIFICATION: A REPORT ON EMERGING PRACTICES WITHIN THE OSCE REGION, NOVEMBER 2022

The report highlights emerging practices in national classification of cyber incidents by underlining commonalities in existing approaches among OSCE participating States and identifying the limitations of this process. Experiences in developing cyber incident classification systems might be diverse across participating States, however, exchanges about these experiences build trust and understanding on a regional and international level. **The report contains recommendations for setting up national incident classification systems** and serves as a capacity-building tool within the OSCE area and beyond.



OSCE Communities

In order to promote greater transparency and explore possible avenues of inter-state co-operation, **CBM 1 and CBM 7 encourage OSCE participating States to share information** on their national structures, strategies, policies and programmes responsible for cyber/ICT security, as well as their national views on various aspects of national and transnational threats to and in the use of ICTs. To facilitate such exchanges, **the OSCE provides a dedicated workspace on its website, the OSCE Communities.** There, participating States can edit their country profiles, add essential information, like the names and contacts of their national Points of Contact, and share documents, including national legislation, cybersecurity strategies and cyber threat assessments. This information is accessible to other participating States, allowing them to better understand each other's policies and positions, and avoid misunderstandings. Furthermore, **OSCE Communities serves as a platform for the PoC network through which States can voluntarily share further information.**

Published by the Organization for Security and Co-operation in Europe
Vienna, October 2023

Layout and design by Rita Papp

This publication is published in line with the mandate of the OSCE Transnational Threats Department. The views expressed in this publication are those of the authors and do not necessarily reflect the official position of the OSCE and its participating States.

ISBN 978-92-9271-249-5

Transnational Threats Department

OSCE Secretariat
Wallnerstrasse 6, A-1010 Vienna, Austria
https://www.osce.org/secretariat/cyber-ict-security