Transnational Threats Department

Cyber/ICT Security

OSCE Organization for Security and
Co-operation in Europe

What is cyber/ICT security?

The Organization for Security and Co-operation in Europe (OSCE) plays a pioneering role in enhancing cyber/ICT security, in particular by reducing the risks of conflict stemming from the use of Information Communication Technologies (ICTs) by its participating States.

The use of ICTs by states has had a profound impact on foreign relations, shaping how states interact, influence and engage with each other in cyberspace. This added complexity has increased the likelihood of misperception, escalation and tension.

To address this issue, OSCE participating States have **developed and adopted two sets of cyber/ICT security confidence-building measures (CBMs)** to reduce the risks of conflict stemming from the use of ICTs by states.

Building confidence in cyberspace

In 2012, an open-ended **Informal Working Group** (IWG) was established under the auspices of the Security Committee (*Permanent Council Decision No. 1039*). The IWG has the **mandate to elaborate CBMs to enhance inter-State co-operation, transparency, predictability and stability**.

The work of the IWG has led to the adoption of two sets of CBMs for cyberspace:

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

The 16 cyber/ICT security CBMs aim to build multilayered 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 have made a political commitment to adhere to them**.

Cyber/ICT security Points of Contact network meeting. Vienna, Austria (OSCE/Ruzica Stojicic Bencun)

OSCE gathers experts to discuss minimizing vulnerabilities in cyber/ICT security. Istanbul, Türkiye (OSCE/Seher Ciplak)

The role of the OSCE Secretariat

The OSCE Secretariat’s Transnational Threats Department (TNTD) assists participating States in their implementation of cyber/ICT security CBMs.

TNTD organizes a range of activities to develop national capacities to address cyber-security threats, as well as promote regional co-operation and resilience. These activities include sub-regional training events on the importance of CBMs, training courses on international cyber diplomacy, workshops on the applicability of international law in cyberspace and technical briefings on the protection of critical infrastructure.

A particular focus of TNTD’s cyber/ICT security activities is the operationalization of the CBM 8 points of contact network, which connects designated national points of contact into a community of cyber experts. Such tools enable rapid communication in case of emergencies as well as offer opportunities for closer co-operation and joint action.

In addition to its in-person activities, TNTD has also developed a series of online products accessible to the general public, such as reports and e-learning courses. **One such course has been specifically developed to raise awareness of OSCE efforts in cyberspace and provide a detailed overview of each of the Organization’s 16 CBMs.**

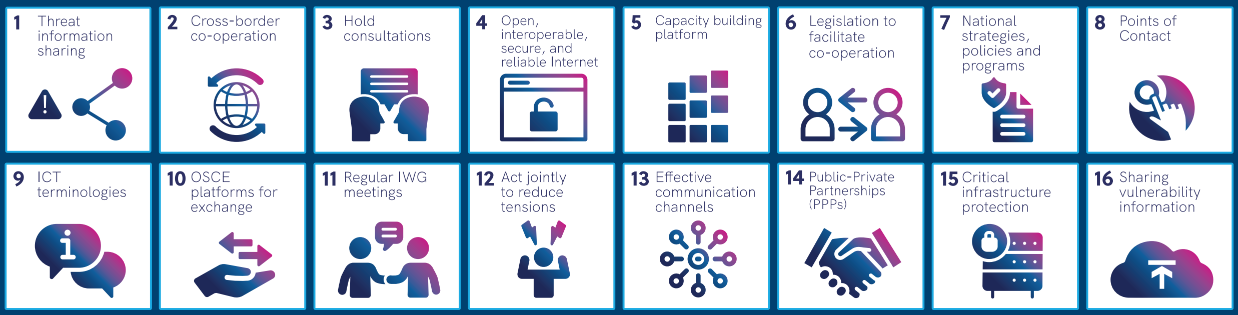
Expected learning effort: 2 hours (self-paced)

Certificated offer: Certificate of completition

Language: English, French, Russian

OSCE e-learning platform: elearning.osce.org

OSCE CYBER/ICT SECURITY CBMs



1 Threat information sharing

2 Cross-border co-operation

3 Hold consultations

4 Open, interoperable, secure, and reliable Internet

5 Capacity building platform

6 Legislation to facilitate co-operation

7 National strategies, policies and programs

8 Points of Contact

9 ICT terminologies

10 OSCE platforms for exchange

11 Regular IWG meetings

12 Act jointly to reduce tensions

13 Effective communication channels

14 Public-Private Partnerships (PPPs)

15 Critical infrastructure protection

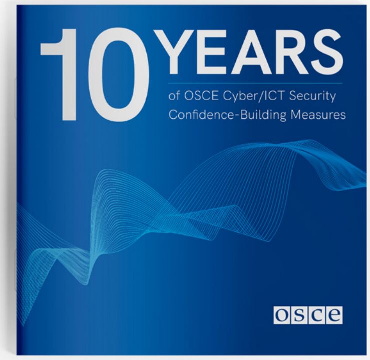
16 Sharing vulnerability information

Supporting United Nations efforts

CBMs are an important element of the international framework of responsible state behaviour in cyberspace, which was developed at the United Nations (UN). As such, OSCE efforts in cyberspace are closely interlinked with the work of the UN in this area. As a regional organization, the OSCE acts as an implementer of UN-level agreements through practical and action-oriented work.

Through a network of national offices and national capacity-building efforts, the OSCE has extensive insight into the specific needs and concerns of its participating States. As such, it plays an important role in informing the UN processes by providing feedback on the practical implementation of UN recommendations.

2023 marked the tenth anniversary of the adoption of the first set of OSCE cyber/ICT security CBMs. The *OSCE launched a publication* which serves as a collection of OSCE experience in the development and implementation of such measures, presenting examples of best practices and key results. It describes efforts across the OSCE area and highlights key examples of the OSCE Secretariat's work in the field.



Selected reading and courses:

OSCE reports:

Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States

Cyber Incident Classification: A Report on Emerging Practices within the OSCE region

E-learning courses:

OSCE Cyber/ICT security Confidence-Building Measures

OSCE Cyber/ICT security CBM 16: Coordinated Vulnerability Disclosure

Follow OSCE

OSCE Secretariat
Transnational Threats Department
Wallnerstrasse 6
1010 Vienna, Austria

osce Organization for Security and Co-operation in Europe

cybersec@osce.org
https://www.osce.org/secretariat/cyber-ict-security