Cyber Security

The OSCE Mission to Bosnia and Herzegovina (the Mission) works to enhance the ability of Bosnia and Herzegovina (BiH) to prevent and respond effectively to security threats emanating from cyberspace in accordance with its commitments as an OSCE participating State.

The Mission's comprehensive approach entails a spectrum of support, ranging from strategic to operational. These efforts involve support to development of a harmonized strategic cybersecurity framework, establishment of Computer Security Incident Response Teams (CSIRTs), and cybersecurity co-operation.

International commitments

BiH is politically dedicated to implementing OSCE commitments deriving from the OSCE Ministerial Council Decisions on Enhancing Efforts to Reduce the Risks of Conflict Stemming from the Use of ICT as well as the agreed set of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the use of Information and Communication Technologies (CBMs). The realization of these commitments and measures helps enhance related predictability and transparency, thereby reducing the possibility of misperceptions and conflict in the cyber domain. In light of the EU accession process, BiH has also expressed its determination to align with the network and information systems' security standards being applied across the EU (NIS2 Directive) and to fulfil the EU's General Data Protection Regulation. BiH moreover aims to implement the Council of Europe (CoE) Budapest Convention on Cybercrime and its protocols, which guides the development of national legislation and co-operation in combating cybercrime.

Key challenges

BiH still lacks an official and agreed strategic approach for responding to cybersecurity threats. BiH remains the only country in South-Eastern Europe without a state-level cyber security strategy and CSIRT. Key challenges include subpar co-ordination, insufficient harmonization, inadequate capacities, and the absence of a strategic vision. Moreover, existing legislation remains to be fully aligned with the relevant EU acquis, and there is no BiH law on information security.

The 2017 Decision of the BiH Council of Ministers on Designation of a CSIRT for Institutions of BiH still requires institutional operationalization. Also, key national priorities contained in the 2017-2022 Information Security Management Policy for BiH Institutions are yet to be operationalized – namely, the establishment of mechanisms to adequately respond to the contemporary challenges of the digital age.

All this leaves the public and private sectors in BiH, as well as individual citizens, highly vulnerable to the evolving threats from cyberspace - including to cyber-attacks and terrorism targeting critical infrastructure. According to statistics provided by the newly established academic CSIRT in BiH, the country faces between 300,000 and 400,000 cyber-attacks per day, or 2-3 million per week. Cyber-attacks targeting the BiH Parliamentary Assembly and the BiH Central Election Commission in 2022 have illustrated both the vulnerability of key ICT systems and the urgency to address cybersecurity gaps in order to safeguard democratic processes and personal data.

The role of the Mission

Under Mission auspices, BiH stakeholders developed and adopted a cybersecurity strategic framework that is being gradually realized through strategies and action plans at different levels of authority. Mission assistance is also helping establish, capacitate and network CSIRTs - as key protection and response mechanisms for cyber security.

The Mission is supporting the work of the Neretva Group - BiH cybersecurity experts and policy makers from public and private sectors working on developing cyber initiatives and policy. Similarly, the Mission facilitates international co-operation on cybersecurity support to BiH – helping pool resources and ensure synergy of efforts.

Under Mission auspices, a diverse group of State and entity-level stakeholders developed and agreed the Guidelines for a Strategic Cybersecurity Framework in BiH. Based on EU national cyber security strategies good practices, this milestone document operationalizes the OSCE cyber/ICT CBMs and represents a basis for development of a cybersecurity strategy for BiH and the related action plans. Overarching and comprehensive in nature, the Guidelines address priority areas for enhancing cyber security in BiH in accordance with international standards.

Through a donation of cutting edge IT equipment, and in line with the BiH Strategy for the Establishment of CERT/CSIRT (2011), the Mission supported the technical establishment of an academic CSIRT in BiH. This specialized team of cybersecurity experts now works to prevent and detect cyber incidents and cyber-attacks targeting public- and private-sector institutions.

Looking ahead

Through supporting BiH to implement OSCE cyber/ ICT CBMs, the Mission will contribute to preserving and enhancing interstate co-operation, transparency and stability, and so to reducing the risk of conflict that stems from the use of ICT. The Guidelines for a Strategic Cybersecurity Framework in BiH will continue to represent the basis for development of strategies and action plans in BiH as well as for BiH.

In view of the sheer importance of CSIRTs for effective prevention and response to cyber-attacks, Mission support will prioritize their establishment, capacity building and networking in BiH.

Similarly, by facilitating and promoting greater and more meaningful inclusion of women and youth experts in cyber affairs, the Mission will help to diversify the much-needed cybersecurity pool of expertise.

For more information,
scan the QR code.

osce Organization for Security and
Co-operation in Europe
Mission to Bosnia and Herzegovina

OSCE Mission to Bosnia and Herzegovina
Fra Anđela Zvizdovića 1, UNITIC Tower A
71000 Sarajevo
Bosnia and Herzegovina

Tel: +387 33 952 100
Fax: +387 33 442 479
press.ba@osce.org
www.osce.org/bih

Follow OSCE Mission to BiH