Incidents related to ICTs rose to record new heights in 2016, such as:

- High profile hacks and espionage
- Websites knocked out by attacks and malware infections
- Attacks on Critical Infrastructure
- Big data breaches and personal information theft

The trend is clear - Effective international cyber/ICT security will grow in importance.

Cyber/ICT security policy makers have not been idle.

- More than a dozen bilateral and multilateral agreements on cyber/ICT security
- Additional cyber/ICT Confidence Building Measures (CBMs) adopted by the OSCE
- New UN Group of Governmental Experts (UNGGE) starts work
- The EU Directive on security of network and information systems (NIS) adopted

*Information taken from the Symantec Internet Security Threat Reports. WEB THREATS BLOCKED refers to web threats blocked over the measured period of time by Symantec services alone.
OSCE Milestones in Cyber/ICT

Confidence Building Measures (CBMs) - aimed at reducing the risks of conflict stemming from the use of ICTs.

Increase in the share of 57 OSCE participating States implementing one or more cyber/ICT security CBMs.

61% (2015) 90% (2016)

In 2016, OSCE participating States adopted new cyber/ICT security CBMs focused on:

- Greater regional collaboration
- Critical Infrastructure Protection
- Crisis Communication Channels
- Public-Private Partnerships

OSCE conducted the first crisis communication readiness check for participating States.

48 States Responded

- Median Response Time: 14 Hours, 11 Minutes
- Best Response Time: 6 Minutes

At the Hamburg Ministerial Council, OSCE Foreign Ministers endorsed the implementation of existing CBMs.

2017 Click here to follow the OSCE's continued efforts in cyber/ICT security.