Transnational Threats Department

Cyber/ICT Security

The OSCE is playing a unique and pioneering role in enhancing cyber/ICT (Information Communication Technologies) security, in particular by reducing the risks of conflict stemming from the use of ICTs between its participating States.

In recent years ICTs have added a complex dimension to inter-state relations. Events in cyberspace often leave room for ambiguity, speculation and misunderstanding. The worry is that miscalculations and misperceptions between states arising from activities in cyberspace could escalate, leading to serious consequences for citizens as well as for the economy and administration, and potentially fuelling political tensions.

A key challenge is that ICTs have made offence easy and defence difficult. While states are heavily investing in offensive and defensive cyber capabilities, currently there are no technical means to attribute cyber activities beyond reasonable doubt.

Building confidence

Under the auspices of the OSCE, the Organization's 57 participating States have developed and continue to work on a ground-breaking set of confidence-building measures (CBMs) to reduce the risks of conflict stemming from the use of ICTs. They are designed to make cyberspace more predictable and offer concrete tools and mechanisms to avoid and address potential misunderstandings, including:

- A mechanism to bring together States for consultations over potential cyber/ICT security incidents to de-escalate rising tensions;
- A platform for exchanging views, national cyber/ICT security policies and approaches to allow States to better "read" each other's intentions in cyberspace;
- Co-operation items including protecting ICT-enabled critical infrastructure as part of enhancing cyber resilience in the OSCE region for the benefit of all.

Confidence-building measures (CBMs)

OSCE States have adopted two sets of confidence-building measures.

The first set of transparency measures (2013) established, among other things, official contact points and communication lines to prevent possible tensions resulting from cyber activities (see: www.osce.org/pc/109168).

The second set (2016), focused on further enhancing co-operation between participating States — including, for example, to effectively mitigate cyber-attacks on critical infrastructure that could affect more than one participating State (see: www.osce.org/pc/227281).

OSCE Organization for Security and Co-operation in Europe

Regional organizations such as the OSCE are ideal platforms for building confidence in cyberspace: They have often been conceived for conflict prevention, and offer practical expertise with CBMs and associated mechanisms that can be applied to this new domain. The OSCE is the first regional security organization with such a diverse constituency that has managed to reach agreement on CBMs focusing on cyber so far.

The role of the OSCE Secretariat

The OSCE Secretariat's Transnational Threats Department assists participating States in their endeavours to enhance cyber/ICT security. Specifically, its Cyber Security Officer assists with implementing and developing new cyber/ICT security CBMs, offering guidance and policy advice as well as co-ordinating organizational output in this field.

The Transnational Threats Department also offers concrete activities designed to enhance participating States' capacities with tackling cyber/ICT security related threats, individually and co-operatively. Such activities range from exercises promoting adequate national responses to potential cyber-attacks on critical infrastructures, to workshops on countering the use of the Internet for terrorist purposes, and training on investigating and prosecuting cybercrimes.

OSCE efforts related to cyber/ICT security complement UN guidance by Groups of Governmental Experts on enhancing cyber stability between States recommending a four-pronged approach to global cyber stability between States:

1. Enhance transparency, co-operation, and stability between States in cyberspace through confidence-building measures (CBMs);
2. Develop acceptable norms of state behavior in cyberspace and clarify how international law applies in this domain;
3. Enhance international co-operation;
4. Build national/international capacities to deal with cyber challenges.

More information at www.un.org/disarmament/topics/informationsecurity

Learn more

Promoting peace in cyberspace: the OSCE experience

Cyberspace is an emerging theatre for tensions and conflicts between States. Learn about the OSCE's landmark efforts to mitigate the threat in our video: www.osce.org/secretariat/226046

Follow OSCE

OSCE Secretariat
Transnational Threats Department
Wallnerstrasse 6
1010 Vienna, Austria

E-mail: Ben.Hiller@osce.org
www.osce.org/secretariat/cyber-security

Organization for Security and Co-operation in Europe