osce.org

TNT Department • Ben Hiller • Cybersecurity Officer

OSCE Confidence Building Measures to reduce the Risks of Conflict Stemming from the Use of ICTs

Organization for Security and Co-operation in Europe

Who are we?


With 57 participating States in North America, Europe and Asia, the OSCE is the world's largest regional security organization. The OSCE works for stability, peace and democracy for more than a billion people, through political dialogue and practical work.

What's our history?

The OSCE traces its origins to the early 1970s where it started as an important **multilateral forum for dialogue and negotiation** between East and West during the Cold War

What do we do?

The OSCE approaches any security related issue in a cross-dimensional way, taking into account politico-military, economic and environmental, and human aspects.

- This is particularly beneficial in relation to enhancing cyber/ICT security as it is a shared domain!

A key objective in our security related efforts is to create greater openness, transparency and co-operation between States.

- To date the OSCE has developed the world's most advanced regime of **arms control and confidence building measures**

Translating OSCE core expertise to the 21st century

Following the recommendations of the UN GGE which highlighted the great potential CBMs can have to enhance transparency, co-operation, and stability between States, **OSCE participating States put theory into practice!**

- PC.DEC/1106: Initial Set of OSCE CBMs to reduce the risks of conflict stemming from the use of ICTs

Drawing on the OSCE's comprehensive toolbox for effective risk reduction measures, **participating States applied the organization's core expertise to the 21st century**

Regional Organizations vs. global challenge?

Regional organizations such as the OSCE are ideal platforms for this type of work:

- They **bring together those States that often have difficult relations**. It is far more likely that two neighbors share a dispute over a border area or the use of natural resources than two far-away countries.

- Since the perpetrators of hostile cyber actions are difficult to identify, a State that is victim to such action has to guess who is responsible. **Chances are that suspicions will fall on a neighbour with whom relations are already strained!**

OSCE cyber/ICT security CBMs

Objective: To enhance transparency between States by promoting exchanges of information and communication between **policy makers and diplomats**.

The CBMs can be broadly categorised in three clusters:

- CBMs which allow States to "read" another State's posturing in cyberspace (CBMs 1, 4, 7 and 10) making cyberspace that little bit more predictable!
- CBMs which offer opportunities for timely communication and co-operation including to defuse potential tensions (CBMs 3, 5 and 8).
- CBMs which promote national preparedness and due diligence to address cyber/ICT challenges (CBMs 3, 6 and 8)

OSCE CBMs

Posturing

- On national and transnational threats to ICTs (CBM 1)
- On measures taken to ensure open, interoperable, secure and reliable Internet (CBM 4)
- On national organizations, strategies, policies and programmes – including cooperation between public and private sector (CBM7)
- List on national terminology (CBM 9)

Communication

- Hold consultations to prevent political or military tension (CBM 3)
- Use of OSCE as platform for dialogue, exchange of best practices, awareness raising, and info on capacity building (CBM 5)
- IWG to meet at least three times a year/development of additional CBMs (CBM 11)
- Nomination of focal points (CBM 8)

Preparedness

- Facilitate cooperation among relevant national bodies (CBM2)
- Put in place modern and effective legislation to facilitate effective cross border cooperation between authorities to counter terrorist/criminal use of ICTs (CBM 6)
- Rapid communication lines between authorities on the policy levels (CBM 8)

Why are the CBMs significant?

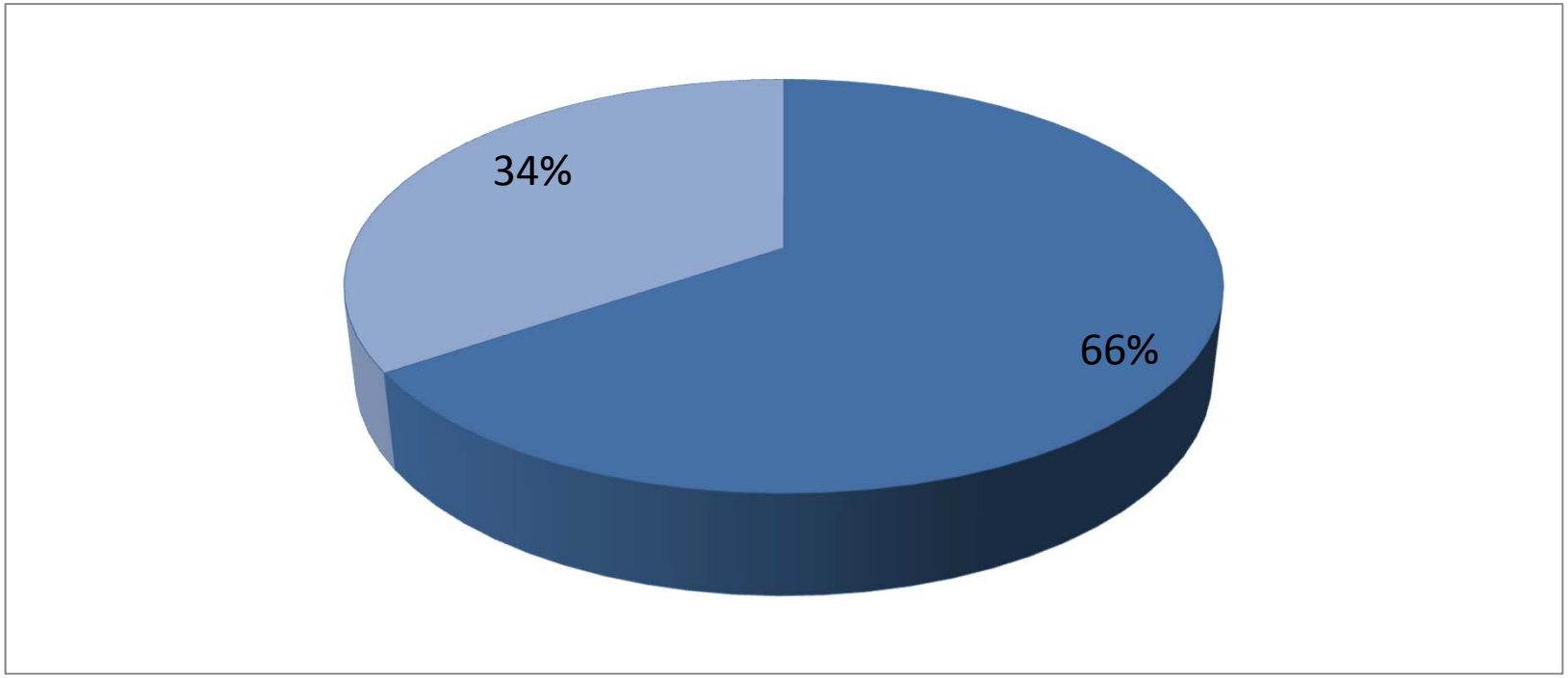
- **The CBMs can create the conditions that can give States the confidence to put down their guard in favour of searching for common solutions.**

- **This is just the start!** OSCE States adopted an incremental approach to confidence. It focuses on the implementation of the first set, and the development of additional and more ambitious CBMs building on increased levels of confidence

- **The CBMs will not stop an intentional conflict but they can stop an unintentional conflict** by stopping or slowing down the spiral of escalation!

- **Non-implementation does not shine good light on a State**.

Overall implementation so far



This is an outstanding result given the legal status of the OSCE and the non-binding nature of the CBMs!

Challenge 1: Overcoming internal constraints

- Sustain momentum in difficult political environment accompanied with erosion of trust and confidence.
- Sustain interest by all States in process ➔ Depends on success of developing cyber as a foreign policy/diplomacy topic throughout OSCE region.
- It is often the simple things creating the biggest challenge: nominating focal points, posting information, using systems provided (POLIS)

Challenge 2: Overcoming regional fragmentation

The OSCE does not operate in a vacuum! How can we enhance inter-regional co-ordination as part of a coherent global approach?

There needs to be a thread that binds regional efforts together, both, on the strategic and practical level.

- S**trategic level:** UN GGE reports serve as a universal reference/guidance on how to achieve cyber stability between States. All regional efforts should strive towards these recommendations!

- **Practical level:** "Co-ordinated Fragmentation": Institutionalized inter-regional information exchange and regular review of regional efforts at the global/UN level (UNIDIR?/academia role?)

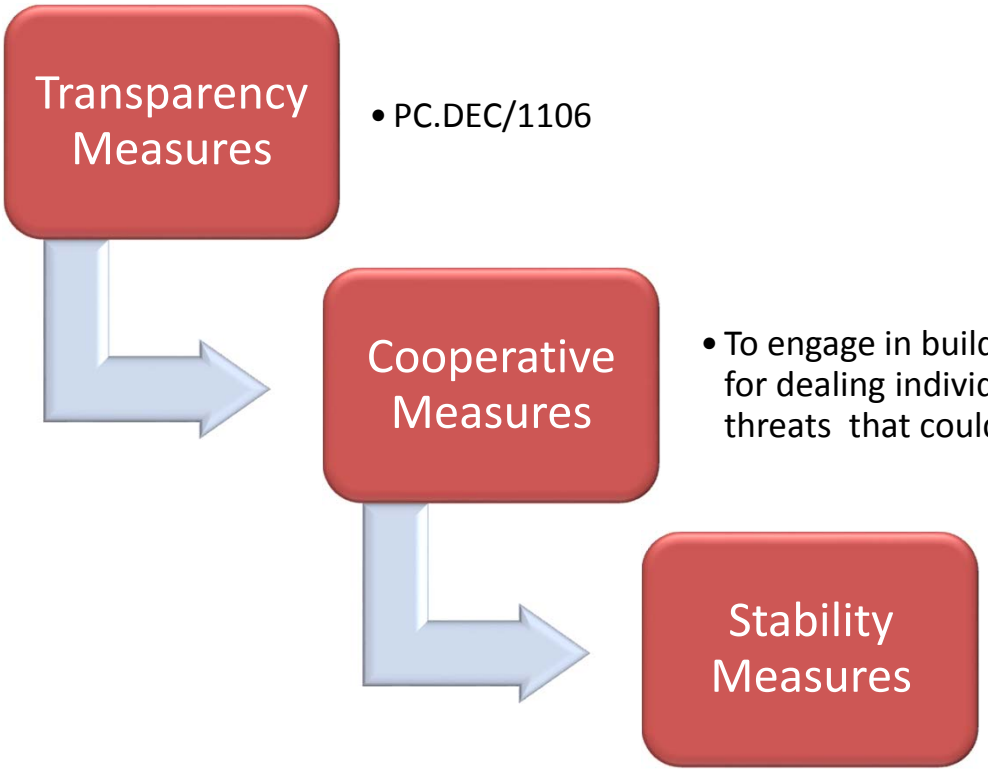
Challenge 3: Overcoming capacity constraints

How can you enhance transparency if some States do not have the right tools to engage in the process?

- For instance, CBM 7 of PC.DEC/1106 promotes exchange of national cyber/ICT security strategies and policies to enhance transparency between States. This requires States to have relevant strategies, polices and legal frameworks in the first place!

  ➔ **CBMs need to be actionable! This is why the proposed second OSCE set also focuses on practical aspect and on operationalizing/testing some of the CBMs in the first set such as crisis communication lines!**

OSCE CBMs: Next steps



- PC.DEC/1106
- To engage in building processes and capabilities for dealing individually and collectively with cyber threats that could impact on peace and stability
- To engage in stabilizing behaviors and refrain from destabilizing activities in cyberspace.