Organization for Security and Co-operation in Europe

The Role of OSCE Confidence -Building Measures in addressing cyber/ICT security challenges to critical infrastructure

osce.org

Transnational Threats Department – Velimir Radicevic – 09.10.2018

Cyber security dimension of critical infrastructure

Importance of critical infrastructure and the implications of attacks

- Lifeline of states, essential assets – regardless of the level of development of the state in question;
- This makes them prime targets –and also objects of intense tensions following a cyber-attacks;
- It is difficult to form an international front on critical infrastructure – every state has different definitions and perceives different threats. Some have sector-specific strategies, others do not.

The political dimension of cyber operations

- Cyber-attacks against critical infrastructure are not just limited to "lone wolves" or criminal groups – many experts connect the scope and sophistication of cyber-attacks to actions by states;
- States are developing cyber capabilities for use in peace-time, previously deployed in or during conflicts;
- More than 50 States have active cyber programmes that give militaries an active role. 10 out of 15 biggest military spenders possess or are developing offensive cyber capabilities;
- The Council on Foreign Relations' (CfR) Cyber Operations Tracker counts 22 States suspected of sponsoring cyber operations.

What has been happening on the international level?

The United Nations as a critical stakeholder

- The need to tackle threats to critical infrastructure is not just a national exercise, but is also a prerequisite to international peace and security;
- A dedicated group for addressing cyber/ICT security issues was established in December 2003 through A/RES/58/32;
- The Group would have varying membership numbers – from 10 to 25, tasked with producing reports to the Secretary General;
- The first consensus report was presented in 2010, the last one in 2015, covering aspects from the applicability of international law to CBMs;
- The 2016/2017 Group failed to produce a consensus report, but the work is expected to continue.

UN GGE as a vehicle for critical infrastructure -protection norms

- The 2015 report stresses that a State should not conduct or knowingly support ICT activities that intentionally damage or impair the use and operation of critical infrastructure;
- The territory of States should also not be used (knowingly or otherwise) to conduct malicious cyber operations by non-governmental groups;
- In addition, States should take appropriate measures to protect their critical infrastructure from ICT threats.

Intertwined thematic pillars within UN GGE reports

UN GGE reports identified a four -pronged approach to global cyber stability:

1. Develop acceptable norms of state behavior, and clarify how exactly international law applies;

2. Enhance transparency, co-operation, and stability between States in cyberspace through **confidence-building measures**;

3. Enhance international co-operation;

4. Build national/international capacities to deal with cyber challenges

Introduction to the OSCE Cyber/ICT security CBMs

OSCE cyber/ICT security CBMs and their clusters

- **Objective:** To enhance transparency between States by promoting exchanges of information and communication between **policy and decision makers** .
- **The CBMs will not stop an intentional conflict but they can stop an unintentional conflict** by stopping or slowing down the spiral of escalation .
- The 16 voluntary CBMs can be broadly categorised in three clusters :
  - **Posturing** - CBMs which allow States to "read" another State's posturing in cyberspace (CBMs 1, 4, 7 and 10) making cyberspace more predictable.
  - **Communication** - CBMs which offer opportunities for timely communication and co-operation including to defuse potential tensions (CBMs 3, 5 and 8).
  - **Preparedness** - CBMs which promote national preparedness and due diligence to address cyber/ICT challenges (CBMs 3, 6 and 8).

OSCE cyber/ICT security CBMs – three clusters

Posturing

- Info exchange on national and transnational threats to ICTs (CBM 1)
- Info exchange on measures taken to ensure open, interoperable, secure and reliable Internet (CBM 4)
- Info exchange on national organizations, strategies, policies and programmes (CBM7)
- List on national terminology related to ICTs (CBM 9)
- pS voluntarily use OSCE platforms to conduct CBM - relevant communication (CBM 10)

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 national focal points (CBM 8) to raise concerns and communicate through
- Identify and exercise effectiveness of communication lines (CBM 13)

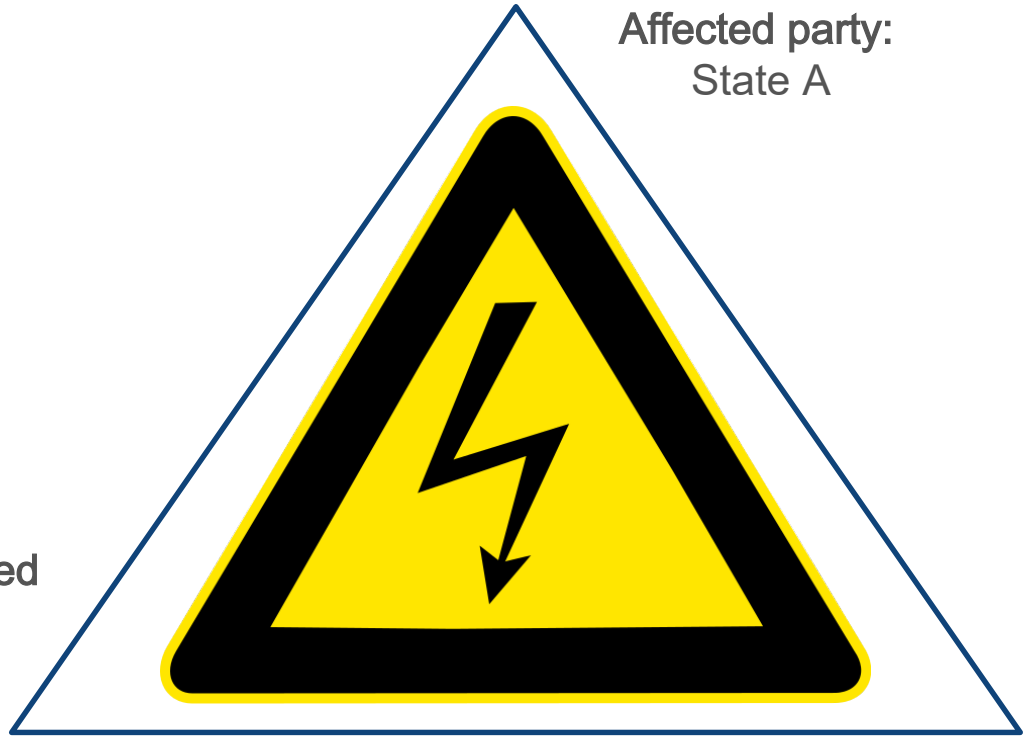
Preparedness

- Facilitate cooperation among relevant national bodies (CBM2)
- Effective legislation to facilitate cross border cooperation between authorities to counter terrorist/criminal use of ICTs (CBM 6)
- Activities to identify co-operative activities (CBM 12) to reduce risks
- **Activities to enhance protection of ICT enabled critical infrastructure (CBM 15)**
- Reporting of vulnerabilities of ICTs including with private sector (CBM 16)
- Promote PPPs and exchange best practices/responses to common challenges (CBM 14)

Confidence Building Measure 15 – Critical Infrastructure Protection

- Develop shared responses, including crisis management procedures;
- Adopt voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident;
- Share national views of categories of ICT -enabled infrastructure that OSCE participating States consider critical ;
- Improve the security of national and transnational ICT -enabled critical infrastructure including their integrity ;
- Raise awareness about protecting industrial control systems.

Implementation example: Cyber incident involving two or more states



Implementation example: Key components of effective crisis communication mechanisms for addressing a cyber incident

People: CBM 8 Points of Contacts

Procedures: Clearly defined steps and procedures for consultations (CBM3)

Channels: Crisis Communications Network (requires information exchange templates - CBMs 13 and 10)

Translating OSCE core expertise into the 21st Century

We are CBMs! ➔ OSCE participating States put theory into practice. Key decisions are:

- PC.DEC/1039 (2012): Development of CBMs to reduce the risks of conflict stemming from the use of ICTs .
- PC.DEC/1106 (2013): Initial Set of OSCE CBMs to reduce the risks of conflict stemming from the use of ICTs .
- PC.DEC/1202 (2016): Second Set of OSCE CBMs to reduce the risks of conflict stemming from the use of ICTs .
- MC.DEC/5/16 (2016) and MC.DEC/5/17 (2017) : Ministerial endorsement and commitment to implement.
- FSC.DEC/5/17 (2017): Approval to use the OSCE Communications Network for crisis cyber/ICT security communication.

What can the OSCE do to enhance critical infrastructure protection?

Implementation of CBM 15 by interested participating States (France, Romania, Slovakia, Spain)

CBM 15 was “adopted” – round tables/ discussions will be held on:

1. Crisis management in the protection of industrial control systems ;

2. Information sharing best practices ;

3. Modalities for co-operation and crisis management in the event of an attack against CI;

4. Building coherence of incident classification criteria .

Sub-regional trainings, scenario -based discussions, tailored support…

1. TNTD supports States – organizing sub-regional trainings, where hypothetical attacks on critical infrastructure are discussed ;

2. The attacks all have significant chances for political escalation – and give opportunities to think what regional/int. mechanisms can prevent them;

3. They are also inter-sectoral – policy makers, technical appointees and critical infrastructure operators are invited;

4. Chances high that similar trainings will be held in the near future – last one held in Rome for over 30 States in September.

Thank you for your attention!