Organization for Security and Co-operation in Europe

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

osce.org

Transnational Threats Department – Velimir Radicevic – 09.10.2018

The cyberspace “status quo”

Cyber-war, -espionage, -crime – the new reality?

- We have observed an increase in significant cyber/ICT security* incidents in the past years, such as but not limited to (spear) phishing attacks, (distributed) denial of service attacks, ransomware and destructive malware attacks
- Commonly known examples include the WannaCry ransomware attack in 2017, the wiper attack NotPetya in 2017.
- We have reason to believe that this trend is likely to continue in the future.

The political dimension of a cyber-attack

- Cyber-attacks 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 (see Georgia, Ukraine etc.);
- UNIDIR (2013): 47 States tasked their militaries with developing offensive/defensive cyber tools, we have reason to believe that this number increased significantly over the last five years;

The political dimension of a cyber-attack (cont.)

- The Council on Foreign Relations' (CfR) Cyber Operations Tracker counts 19 States suspected of sponsoring cyber operations;
- In 2016 NATO has elevated cyberspace to fifth dimension of warfare after Land, Sea, Air and Space (article 5 applies);
- We are witnessing a slowly evolving arms race in cyberspace.

Cyberspace is complex, and carries uncertainties

- **Legal framework** ➔ States disagree on how rules, principles, laws, treaties and conventions can be applied to cyberspace!

- There is an absence of treaty or customary law – no equivalent of a Treaty on Open Skies, as done with conventional arms;

- Closest thing that was done was a consensus report of the UN GGE in 2015 that international law applies to cyberspace.

What has been happening on the international level?

The United Nations as a critical stakeholder

- The need for action was clear – and the UN became the foremost organization to tackle cyber stability between all States, not just like-minded ones;
- A dedicated group for addressing cyber/ICT security issues was established in December 2003 through A/RES/58/32 - the newly formed Group was titled “Group of Governmental Experts (UN GGE) on the Developments in the Field of Information and Telecommunications in the Context of International Security ”;
- 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.

Three UN GGE Reports and their main take-aways

2010 Report:

- Provided overview of threats States face, focusing on confidence-building and norm setting, while charting a path for future UN GGEs.

2013 Report:

- Elaborated on previous conclusions, but also cited international law*, the UN Charter in particular, and derived norms, rules and principles as applicable and essential to maintaining an open and secure ICT environment**.

*"International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment"

**"state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory"

Three UN GGE Reports and their main take-aways (cont.)

2015 Report:

- Established a detailed four-pillar system for guaranteeing cyber stability between States, made up of: a) norms and int. law ; b) CBMs; c) capacity building and d) enhancing co-operation.

Future of the UN GGE:

- The 2016/2017 Group failed to produce a consensus report, putting the future of the Group in question. New formats to be proposed at the September UNGA.

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

CBMs are critical components of any cyber stability mechanism!

- **Norms need to be socialised through CBMs to ensure buy in** ➔ While developing norms, rules and principles for the responsible behaviour of States is vital, States need to have the confidence that others adhere to the same rules
- **CBMs serve can be the vector for States to implement and follow norms** ➔ If States do not have the capacity to engage in cyber stability mechanisms, CBMs can help them build up their national capacities to become an active contributor and increase its international engagement efforts
- **CBMs serve as practical mechanisms in crisis situations** ➔ What happens if norms and rules are broken? The CBMs kick in!

Introduction to the OSCE Cyber/ICT security CBMs

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.

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)

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 (CBM 3)

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

How does this factor in with the technical community (e.g. CERTs)?

Jointly promoting cyber resilience – with both the policy and technical communities

1. Building confidence between States is an important step for opening up States, but also facilitating cross-sectoral co-operation and co-ordination;

2. Complementary with existing mechanisms – for instance, the CBM 8 network, open to both technical and policy PoCs…

3. Encouraging proactive co-operation, for instance, through scenario-based discussions and activities;

4. Going forward, building cyber/ICT security capacities of policy makers - incident classification, facilitated visits between policy and technical PoCs, research support.

Thank you for your attention!