Auswärtiges Amt

OSCE Workshop on Cyber/ICT Security in the Context of Regional and International Security

Tashkent, 20-21 May 2015

Building Confidence between States

Karsten Geier
Head,
Cyber Policy Coordination Staff

Federal Foreign Office
Berlin, Germany

- Numerous states are pursuing military cyber-capabilities.
- Cyber capabilities are not limited to great military powers.
- Cyber security is not a problem that is limited to rich Western countries and some Far-Eastern “Tigers”.
- Cyber security goes beyond cyber-crime.
- Cyber stability is affecting international security.

Four scenarios for cyber conflict:

(1) All-out cyber-war.

(2) Limited use of cyber capabilities as part of a larger warfighting effort.

(3) Use of cyber capabilities as an element in hybrid conflicts.

(4) International military crisis developing from a cyber-action.

Cyber action is not limited to cyber space. It can create real damage in the physical world.

Diplomats and international security experts have to ask themselves how to respond.

Cyber capabilities do not fit well into traditional political-military strategies:

- Deterrence and denial require that the consequences of any attack be clearly and credibly communicated to any potential adversary; this is difficult in cyber-space.
- Empirical data on "mutual entanglement" is ambiguous at best.
- If political-military strategies fail to account for cyber capabilities, so does traditional arms control.

Cyber capabilities make offense easy, while defence is difficult. They introduce a degree of uncertainty into international relations, which has the potential to be destabilizing.

Things we can do:

1. Make our systems more resilient, reducing vulnerability.
2. Define norms and principles of responsible state behavior in cyber space to enhance transparency and predictability.
3. Agree regional security- and confidence building measures.

Regional organizations bring together those states that are most likely to have difficult relations. Regional organizations provide a forum for such neighbors to talk, and, ideally, to resolve their grievances. This is especially valuable regarding cyber-conflict.

Increasing transparency:

- Exchanging information on relevant domestic structures and institutions,
- Sharing their national cyber security strategies, and
- Exchanging white books or national doctrines relevant to cyber security.

Trust building:

- Sharing views on the rules of international law that apply to cyber conflict,
- Designating points of contact, and
- Establishing channels of communication for crisis situations.

Risk reduction and stabilization:

- Establishing Computer Emergency Response Teams (CERTS),
- Exchanging experiences and promoting cooperation between national CERTS,
- And conducting joint CERT exercises.

OSCE three-step approach :

1. December 2013 – Agreed first set of cooperative measures aiming at transparency-building.
2. Since 2014 – engaging in the implementation of these measures, while discussing a second set, aiming at trust-building and cooperation.
3. Beyond 2015 – hope to arrive at a third set geared toward increasing stability.

Deliberative process aiming at identifying those measures to which all can agree.

Agreed OSCE **transparency-building** measures:

- Providing national views;
- Facilitating co-operation;
- Holding consultations;
- Sharing information;
- Using the OSCE as a platform for dialogue;
- Nominating contact points;
- Providing a list of relevant national terminology.

OSCE should make better and more systematic use of the information exchanged:

- Systematic processing of information exchanged.
- Results of such analysis could feed expert talks to prepare policy discussions and negotiations by more senior officials.
- Better focus the provision of information: Developing questionnaires, to which Participating States would respond.

Ideas for the second set aiming at OSCE **trust-building and cooperation**:

- Organizing workshops, seminars, trainings and roundtables;
- Conducting joint trainings or exercises;
- Promoting (information) exchanges/visits;
- Sharing information on newly discovered risks;
- Promoting public-private partnerships.

Discussions on a third set of Confidence Building Measures for **stabilization** are at a very early stage.

Thank you for your attention.