OSCE: implementation problems of the Confidence Building Measures (CBMs)

Translation by Daniela Giordano

Original in Russian: https://interaffairs.ru/news/show/18594

Looking at OSCE data, about 47 states around the world have cyber military programs that are currently active and, among these, 10 states have conspicuous military budgets, or are developing offensive cyber technologies. It is clear that in such circumstances, in addition to the uncertainty of the international mechanisms and agreements in the ICT field, there are serious threats for the national and international security. The Organisation for Security and Cooperation in Europe (OSCE) is one of the major international platforms, in which participating States have proposed and are working on the implementation of a set of Confidence Building Measures (CBMs) for cyberspace. The CBMs should increase transparency, enhance cooperation, ensure stability, reduce the risk of intentional cyber-attacks and assist states in the adoption of pondered decisions.

The experts of the Institute for Information Security Issues of the Lomonosov Moscow State University and the OSCE representatives have discussed at length on the applicability of CBMs in cyberspace, during a scientific seminar, organised by the Institute of Moscow State University.

In 2013, as a result of a difficult negotiation, OSCE participating States have accepted the first international document on CBMs in cyberspace to avoid situations of conflict. The participating States of the Organization agreed on eleven measures, which promoted: exchange of best practices; actions of consultation in order to reduce miscommunication and the beginning of political and military tensions; promotion of knowledge and information on the safe use of ICT; introduction of efficient national legislative norms, which allow to simplify the bilateral collaborations and an efficient and prompt exchange of information among competent ministries (included national law-enforcement), so to contrast criminal and terroristic use of ICT, etc.

In February 2016, a second list of CBMs was decided by OSCE participating States. It integrated the previous document with five more points. Some of the measures encompass: development of a public-private partnership; exchange mechanisms of best practices in reaction to the common challenges to ICT security; realization of inter-governmental exchanges in different formats (regional and sub-regional seminars, roundtables, working groups, etc.) and others. However, all the CBMs are voluntary.

Moreover, despite the fact that all participating States have signed the aforementioned documents, the implementation of CBMs have encountered many obstacles. It appears that in this sense the traditional methods of collaboration in the security sector have not achieved anything, yet. The solution for these problems should be found in the so called ‘second way’ diplomacy, enacted by experts and scholars.

Thus, in 2016 a small working group from the University of Florence (which was enlarged by experts from other academic centres, like the Royal College, Oxford University, Brandenburg

Technical School, Tadeusz Kościuszko Polytechnic University of Cracow, MGIMO, etc.) released an analysis of the implementation problems of the CBMs, which were adopted in 2013. The investigation's methodology included data collection in open and closed sources, surveys and interviews of political/ governmental representatives of OSCE participating States. The objective was to understand precisely which technical and practical problems hindered the realisation of these measures and which practical actions would have been necessary in order to overcome the project impasse.

The experts presented the results of the groups' research in many scientific seminars, drawing the following conclusions:

First of all, there are enormous differences among OSCE participating States for what concerns the level of preparation and understanding of ICT security. As was expected, North American and Northern-Central European countries have a higher level of awareness of the cyber-related danger than the Southern Caucasian, Central Asian and even Southern-Western European countries. As a consequence, in those states where there is not a clear awareness of the matter, cyber security is not in the governments' agenda.

Secondly, many participating States of the Organisation are not adequately informed on what the OSCE can do and offer to states, interested in improving their capabilities in the ICT field.

Finally, among participating States there are huge differences in the availability of technological, human, financial and scientific resources for an efficient implementation of the CBMs. The experts have highlighted that the major problem is hidden in the lack of personnel at different levels (technical, governmental, etc).

Starting from these conclusions, it has been decided to pass to the next phase, which means the proposal of some recommendations to solve the existing problems. At the moment, the working group is elaborating a set of mechanisms, which could help the OSCE participating States to apply efficiently the CBMs. However, it is important to recognise that the working group of the University of Florence is not a formal OSCE structure, so all the recommendations proposed will be sent to the inter-governmental working group for the cybernetic issues, which, on the contrary, works within the OSCE framework.

Following the results of the discussion, it was reached an agreement on continuing this cooperation to determine a potential participation of the Institute's representatives to the preparation and realisation of the Working plan for the development of a CBMs system in the cyber security field and the safe use of ICT.

The implementation work of CBMs within OSCE framework is a rather difficult task and a tricky puzzle to solve; however its solution will mark an important step in the creation of a universal stability and a worldwide security.