RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE STUDIES

Occasional Paper

Advancing Confidence Building in Cyberspace: Sub-regional Groups to Lead the Way

Piret Pernik

November 2014

Summary

OSCE seems to not be ready to adopt more advanced confidence building measures. Closer cooperation will be more likely within smaller like-minded groups or geographically close states. The electricity and telecommunications sectors urgently need a close public-private partnership and enhanced intergovernmental collaboration to reduce vulnerabilities stemming from cross-border and cross-sector dependencies including agreements on common minimum security standards.

Organization for Security and Cooperation in Europe (OSCE) has, for many years now, been promoting the implementation of confidence building measures (CBMs) aimed at reducing the risk of conflicts stemming from the use of ICT technology. Last December OSCE member states adopted an initial set of 11 CBMs,[1] and agreed to explore the development of additional measures. Last week in Vienna 57 OSCE members and 11 partner countries, in collaboration with experts from the private sector, think-tanks and academia, reviewed the existing applications of CBMs and discussed a way forward for further development.

The discussions indicated that for now OSCE seems to not be ready to adopt restraint measures, such as a moratorium on critical infrastructure attacks or the use of offensive cyber capabilities more broadly. Advanced cooperation will be more likely within smaller like-minded groups or geographically close states. Further, the electricity and telecommunications sectors urgently need a close public-private partnership and cross-border cooperation, as well as agreements on common minimum security standards and measures.[2]

[1] Most of the measures pertain to greater exchange of information concerning threats, national measures taken to secure internet, national organization and strategies, policies and programs of cyber security, and national terminology. The measures also envision holding consultations in case of emergencies, maintaining regular dialogue and exchanging best practices. To facilitate information exchange states are encouraged to put in place modern and effective national legislation and nominate a national contact point. The measures include also a regular meeting format within the OSCE working group at least three times per year.

[2] For example, OSCE's good practices guide on the protection of non-nuclear critical infrastructure from cyber-related terrorist attacks could be adapted and extended to other threats.

 ISSN 2228-0294

Misperceptions about the cyber capabilities and intentions of a potential adversary could potentially lead to kinetic conflict. In light of this sobering fact, OSCE's efforts are particularly praiseworthy. It is among many international organisations that have sought to agree on special transparency, collaboration, and stability measures for cyberspace in order "to dispel mistrust that otherwise lead to armed conflict."[3] CBMs, historically successfully applied to avoid escalation between states concerning conventional and nuclear weapons, increase trust, early warning, and predictability; and, in the long run, can increase stability and lay the groundwork for the development of more robust international norms and agreements. Cyberspace is believed to be the next frontier for the development of such norms and agreements.

In the kinetic world, the implementation of CBMs is a straightforward effort. The very nature of cyberspace, however, complicates attempts to institute similar measures to regulate state activity. First, a risk of miscalculation or cognitive biases when analysing the intentions of other actors in cyberspace is greater than in the real world.[4] Malicious activities targeted at national security apparatuses or essential public services are anonymous and attribution is difficult. Often perpetrators are non-state actors to whom intergovernmental treaties do not apply. Worse, some criminal groups, terrorists and political hacktivists are backed by the vast resources of a government. Second, in order to maintain superiority in cyberspace, states tend to conceal their cyber skills and weapons, thus verification mechanisms and deterrence in the traditional understanding are impossible. Since the most likely - and from the national security perspective, the most alarming - targets of a major cyber attack are critical infrastructures (largely owned by the private sector), effective implementation of CBMs for cyberspace must engage not only governments, law enforcement and military establishments, but also critical infrastructure operators from the private sector. The greater the number of stakeholders, the more burdensome bureaucratic consultation and negotiation processes become.

Not surprisingly - and perhaps also due to a short period of time that has passed since the adopting of the measures - the progress in the implementation has been modest. Only one third of the committed states submitted all required information (less than 20 states out of 57 OSCE member states). Slightly more than half of the states shared information on their cyber security organization, strategies, policies and programs; 40% shared information on national points of contacts for coordinating incidence response; and 35% shared views on national and international cyber threats. Information sharing regarding military and

[3] S. Tulliu and T. Schmalberger, Coming to Terms with Security: A Lexicon for Arms Control, Disarmament and Confidence-Building, UNIDIR, 2003, p. 135, in UNIDIR, The Cyber Index International Security Trends and Realities (UNIDIR Publication 2013/3).

[4] Dr Katharina Ziolkowski, *Confidence Building Measures for Cyberspace – Legal Implications*, CCD COE, Tallinn 2013.

national security capabilities and activities were considered particularly sensitive, and full transparency in this area seems unlikely in the near future.

Given the political and ideological differences (including views on online values and fundamental freedoms), it would be naive to expect quick transition from principles to practice among the OSCE member states. Rather than proposing additional CBMs, speakers at the November Vienna conference tended to agree that further work should focus on determining modalities of the existing measures to improve the information collection and analysis, as well the exploration of particular aspects within smaller sub-regional groups. Collaboration on a smaller scale has already proven a success given the progress many regional groups have achieved by sharing basic cyber information such as national contact points and conducting regular joint exercises.[5]

At the same time larger collaboration formats like UN, OSCE, and others, should continue work on less contentious aspects of cyber security discussing national terminology, strategy, policies, military doctrine, budgets, organizational arrangements and the like in order to build up the basic level of trust. Most importantly, these negotiations should include civil society and the private sector and in this respect, the November conference was a welcome initiative of the Swiss chairmanship. In addition to fine-tuning the existing OSCE CBMs (e.g. through the formulation of consultation procedures, identification of communication channels, formats and other modalities) the regional organisation should launch programs to facilitate closer contacts between think-tanks, academics, and the private sector, as well as exchanging information on academic and scientific research.

Cooperation between geographically close countries who have already established the basic level of trust and transparency should be taken to the next level, with cooperation evolving from political and strategic to technical and operational levels. In smaller like-minded or regional settings, states could commit politically to act consistently with international law for cybercrime, and refrain from harming or supporting cyber activities that intend to damage other parties' critical infrastructure. They should enhance cooperation in law enforcement (including an obligation to investigate cybercrime activities by non-state actors residing in their territory) and between law enforcement, CERTs and militaries, as well as for the protection of critical infrastructure. With the gradual increase of trust more advanced cooperation could follow. This includes sharing threat perceptions, risk assessments, and real-time intelligence; joint mechanisms for crisis management and early warning; joint exercises; and in the area of digital forensics establishing regional centres of excellence, conducting

[5] Within Europe, Visegrad and Baltic-Nordic countries are most advanced in this respect, but there are others such as the Asia-Pacific cooperation forum, GUAM, OAS, etc.

joint investigations, as well as developing common linguistics for law enforcement, CERTs and prosecutors. In time these voluntary codes of conducts could be spread to other regions and eventually become universally accepted norms. The European Union and NATO, as well as Nordic-Baltic region are excellent cooperation fora to lead the way.

Using these kinds of smaller collaborative efforts, governments must urgently make greater efforts to share information and best practices with each other and the private sector in energy and telecommunications sectors since these "supercritical infrastructures" are essential to all other public services.

The private sector has set up measures to defend against lower-end threats (common worms and viruses, cyber criminals and the like), but lack the information and resources to stop higher-end threats such as advanced persistent threats (APTs), nation-state espionage, attacks against industrial control systems.

Within the OSCE's larger framework, many states still are far from committing to a code of state conduct for cyberspace; thus attempts to set up international norms are not feasible. Apart from some states, there seems to be greater consensus - as expressed by the United Nations' Group of Governmental Experts, NATO, the Tallinn Manual, and many individuals countries - that the existing international law applies to cyberspace, thus new international agreements are not needed.

In conclusion, despite the present hesitancy to develop more advanced stability and restraint measures, regional and international organizations including OSCE should continue work to build basic trust within bigger groups of states; facilitate close cooperation in smaller sub-regional and like-minded groups; support joint exercises as tools to build trust in both formats; as well as work out concrete measures (guidelines, standards, etc.), to reduce vulnerability of cross-sector and cross-border supracritical infrastructures.