Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

NATIONAL DEFENCE COLLEGE

Confidence Building Measures in Cyberspace

NATO's 2010 Strategic Concept linked cyber issues to NATO's core business. The Alliance's cyber focus includes cyber defense of its own infrastructure and building Allied nations' cyber capacity. In parallel, NATO's core purposes include promotion of cooperation on defense and security issues to build trust and, in the long run, prevent conflict in all domains, including cyberspace.

The objective of confidence and transparency building measures in relation to conventional threats has been to prevent the outbreak of war and escalation in a crisis, increase trust so as to avoid escalation, enhance early warning and predictability, and modify and transform or improve relations between states.

NGOs and regional organizations, the OSCE being the most prominent, have translated existing confidence building measure (CBM) concepts to the cyber domain and working to broker common approaches to cyber CBMs. In line with the non-duplication principle, NATO's mandate in CBMs is limited to monitoring the evolution of rules in the area and supporting the development of national efforts. Through its Science for Peace and Security Programme (SPS), NATO seeks to enhance cooperation and dialogue on emerging security challenges by gathering insights from member states and partner countries.

Within this framework, twenty-six experts from fifteen countries gathered in Stockholm from March 25-27 to build on existing work by ICT4Peace, OSCE, CCDCOE, and others to discuss challenges and opportunities of existing confidence measures and more fully develop a small number of cyber specific CMBs.

The workshop format included intervention by selected speakers, followed by a facilitated discussion in three key areas- CBMs leading to restraints in state behavior in cyberspace, CBMs through which states can de-escalate cyber conflicts, and CBMs which the private sector can use to de-escalate conflicts in cyberspace.

The substance of the discussions focused on confidence building measures that lead to de-escalation at the early stages of cyber conflict where states conduct activities below the armed conflict threshold and the challenges posed by involvement of patriotic hackers in the conflict. The participants agreed that the set of CBMs formulated in the work of other organizations are a step in the right direction, the challenge remains operationalization of these measures.

In the area of CBMs leading to **restraints on state behavior in cyberspace** the existing body of international law provides various examples of rules that can be applied in cyberspace. As confirmed by the UN GGE, international law applies in cyberspace and accordingly international humanitarian law restrictions on means and methods of warfare also apply in cyberspace. The discussion confirmed that the

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

outstanding questions remain – how is international law applied in cyberspace and the establishment of red lines of what constitutes illegal actions in peacetime?

Considering both peacetime and armed conflict situations, the discussion focused on formulating confidence building measures that would lead to the acceptance of restrictions on disruptive attacks on assets and entities during peacetime and result in protected status for critical cyber entities during armed conflict.

Discussants suggested that because of the nature and possible effects of cyberattacks, assets such as the Internet backbone, major IXPs, finance, aviation, and undersea cables should be declared off-limits to cyberattacks. Borrowing from the international humanitarian law concept of protected personnel and entities, the discussants suggested that during cyber armed conflict, protected status should be granted for critical cyber entities, including personnel and private organizations.

To achieve these end goals, a range of CBMs were suggested by the participants. The suggested CBMs included joint research work on the interpretation of principles of international law applicable in cyberspace, commitments to work towards an understanding on the need to define specific assets and entities that should be granted protective status, and commitments to develop common understanding of what constitutes critical cyber infrastructure both in terms of technical infrastructure, entities maintaining critical services, and personnel.

The participants pointed out that there are no foreseeable endeavors to clarify international law in a formal treaty manner but stressed that traditional multilateral approaches to CBMs should be complemented by unilateral steps that can introduce transparency in state practices in cyberspace. Unilateral declarations and statements laying out the limitations states self-imposed on their cyber activities were pointed to as examples achieving the desired goals.

Discussants emphasized, during the conversation on **CBMs through which states can de-escalate conflicts in cyberspace**, that the two biggest challenges for states in responding to patriotic hackers and proxies are inadvertent escalation and loss of escalation control. Because of the complexity of attribution, activating rules on state responsibility for actions of proxies and patriotic hackers remains difficult but not impossible. The participants agreed that wider sets of indicators and warnings should be considered in attribution analysis.

Participants analyzed typology of patriotic hackers and proxies and stressed, that while private industry is the most apt and experienced in dealing with bottom tier malicious actors, the actions of top level, sophisticated and hybrid actors requires state engagement.

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

Turning to solutions for the risk of loss of escalation control in conflicts involving patriotic hackers and proxies, the participants suggested a set of communication CBMs would support the transparency and de-escalation objective of CBMs.

Experts submitted that a set of fully developed escalatory contacts and a broad set of hotlines at individual state level could serve as CBMs. These frameworks for crisis communication would require bureaucratic alignment and shared understanding of escalation dynamics between states. Establishment of broader sets of hotlines would follow through creation of net centric, secure, and around the clock available lines of communication that would be routinely tested and serve as an integral part of crisis management exercises.

According to participants the risk of inadvertent escalation could be mitigated through states' commitment to the development of an attribution regime for adjudication, with focus on accountability. The regime would include technical, political, and legal standards for attribution, created through joint education, exercises, and training. Work between states on differentiating CNA and CNE to avoid escalatory spiral could serve as further means of building confidence and transparency.

Discussants suggested that existing intergovernmental forums, such as OSCE and regional security organizations, such as NATO, could serve as structures for the establishment and development of these rules. The progress would be facilitated by standing cooperation and established standards and collaboration in the areas of exercises and education.

When discussing the **role of the private sector in de-escalating conflicts involving patriotic hackers and proxies**, experts pointed out, it is private sector actors who have their hands deep in cyberspace and their empowerment and engagement is crucial for stabilizing cyberspace.

Involvement of the private sector and individuals in stabilizing cyberspace could be encouraged through development of collaboration frameworks outside of established channels. These frameworks would not only encourage the use unaffiliated security personnel to work together on Internet security and stability projects but also serve as an outlet to counter the activities of potentially destabilizing actors. states should enable these engagements through supporting the harmonization of groups that work on the same problems, disseminating information about the existence of such groups, and providing guidance on how to engage with them.

As for the implementation of these measures, the experts suggested that the regime does not have to be cross-stakeholder, but efforts, results, and language should be harmonized. Organizations such as ICAAN or IGF would be best suited for states to accommodate their efforts on development of these CBMs, complemented by organizations such as NSP SEC whose efforts would not become subsumed to government to government dialogue.

NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

NATIONAL DEFENCE COLLEGE

Throughout the discussions, participants pointed out that beyond traditional confidence building measures, measures that build confidence and predictability should be unilaterally pursued by states. Unilateral measures adopted by states are easily achievable transparency measures.

Selected measures discussed during the workshop will be developed in future Atlantic Council issue briefs.

NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme