STOCKHOLM FORUM on Peace and Development 2019

From Crisis Response to Peacebuilding: Achieving Synergies

14–16 May 2019
Stockholm, Sweden

CAN MEDIATION DE-ESCALATE CONFLICTS IN CYBERSPACE?

INSTITUTIONAL LEAD

Centre for Humanitarian Dialogue

MODERATOR

David Harland
Executive Director, Centre for Humanitarian Dialogue

THEMATIC FOCUS

Conflicts in cyberspace—from intrusions into critical infrastructure to the manipulation of social media to interfere in elections—have so far not proved amenable to the traditional tools of conflict resolution. There continues to be vigorous debate about what constitutes acceptable behaviour in cyberspace, particularly across geopolitical divides. In the meantime, states are rapidly developing their offensive capabilities, which at worst could spill over into conflict in the kinetic realm. This session examined existing diplomatic efforts to promote the stability of cyberspace and considered in what circumstances mediation may help.

SUMMARY

The discussion centred around cyberspace—said to be the next frontier in warfare and conflicts. Cyberattacks, by their nature, are attractive to use because they can be deployed quickly, ignoring geographical boundaries and having a low cost and risk. More importantly, they can be used with plausible deniability and attributing attacks is next to impossible—unlike conventional weapons.

Conflicts and attacks in cyberspace have the potential to be a destabilizing force in international affairs. For the first time, there was a kinetic response to a cyberattack when the Israeli Defence Forces conducted airstrikes in response to an alleged hacking attempt by Hamas in May 2019. Disinformation and hacking campaigns were used by Russia against Ukraine and Georgia and against the United States in the 2016 elections. Civil society is particularly vulnerable to these types of attacks and non-governmental organizations (NGOs), human rights activists and journalists are regularly targeted around the world. There is also a discrepancy in capabilities between larger and smaller states.

The issue of security versus freedom and democracy was also discussed. In trying to counteract content manipulation (i.e. fake news), governments often propose to monitor networks. However, in doing so they build the infrastructure for an authoritarian surveillance regime capable of censoring the internet. Careful attention should be paid to ensure transparency in the process and the possibility for citizens to appeal against content removal.

While the current debate on the topic is largely focused on the technical and technological aspect of cyberspace, it was said that it is important not to forget the human behind the computer screen. Shared learning and research on human behaviour in this context is important for a deeper understanding of this new phenomenon.

The panel unanimously agreed on the importance of this emerging phenomenon and that traditional approaches need to be overhauled. The inclusion of civil society, businesses and academia were seen as key to advancing thought in this area because of the high level of complexity and the decentralized nature of cyberspace. Policy has simply not caught up to the rapid development of new information technologies and this could no longer be considered a marginal problem in international affairs. A bridge between the cyber community and the traditional peacebuilding community was welcomed by the panel to advance thought in the area.

KEY TAKEAWAYS

The potential benefits from technology are considerable—but so are the risks. While there is eagerness to reap the benefits of technological innovation and information technology, there is an increasingly vulnerability to cyberattacks and this is no longer a marginal problem.

Civil society is particularly vulnerable to cyberattacks because it lacks resources and tools to defend itself. Cyberattacks are actively being used against NGOs, human rights activists and journalist around the world.

The international laws and norms that do exist regarding cyberspace are not applied in practice. Because of the decentralized infrastructure of cyberspace, it is key to involve civil society, businesses and academia in this matter.

It is important not to forget the human behind the computer screen. The current debate about cyberconflicts and cyberattacks is largely focused on technological and technical aspects, while the actors—human beings—are absent from the conversation. Further study is needed to understand the human behaviour in this new context.

There is an opportunity and a need to connect the peacebuilding community to the digital community to effectively deal with this paradigm shift and evolve traditional ways of thinking and dealing with conflict mediation in this new space.

Hanna Klinge
@H_Klinge

Discussing mediation and cyberspace @TuijaTa @SIPRIorg @cmioffice #SthlmForum

8 12:49 PM - May 14, 2019

See Hanna Klinge's other Tweets

Screen capture taken by screenshot.guru on Mon, 20 May 2019 11:52:39 GMT.

Permalink: twitter.com/H_Klinge/status/1128281252920995840

"hd Centre for Humanitarian Dialogue
Mediation for peace

This session report was produced onsite at the 2019 Stockholm Forum on Peace and Development hosted by SIPRI and the Swedish Ministry for Foreign Affairs. The report aims to reflect the session discussion. The views, information or opinions expressed do not necessarily represent those of SIPRI, the Swedish Ministry for Foreign Affairs or other institutes associated with the session.