Exploratory Meeting

on

"Countering Violent Extremism Online – The Dual Potential of the Internet"

Minutes

24 February 2016

The meeting was conducted under the Chatham House Rule: "When a meeting or a part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

The first exploratory meeting on "*Countering Violent Extremism Online – The Dual Potential of the Internet*" was held on 24 February 2016 at the *Maison de la Paix*, Geneva. It gathered participants from eight States, two international organisations, and five research institutions. The first exploratory meeting aimed to offer participants the opportunity to articulate concerns and experiences in countering violent extremism offline as well as online, and to express their needs and priorities going forward.

The meeting was structured into three sessions. The first was dedicated to setting the scene in regard to countering violent extremism. The participants had the opportunity to express their concerns and experiences in countering violent extremism online. The second session was dedicated to a presentation on "*How Does Islamic State Use Social Media to Achieve Its Aims?*" This case study mainly focused on the recruitment techniques by ISIS. The last session of this first exploratory meeting allowed for the continuation of discussion and provided the opportunity to discuss the way forward for effectively countering violent extremism online.

Opening of the Meeting

In the opening remarks the need for an effective multi-stakeholder initiative to help prevent and counter violent extremism online was addressed. In particular, it was highlighted that one could learn from the experiences and expertise of DCAF Operations IV (Public-Private Partnerships) in successfully developing and implementing multi-stakeholder initiatives, such as the Voluntary Principles[1]the Montreux Document and the International Code of Conduct for Private Security Service Providers respectively[2]. With regard to countering/preventing violent extremism online, it was stressed that the Internet's inherent characteristics provide both opportunities as well as risks, and that recent terrorist attacks demonstrated that the Internet, and in particular social media, can be used as a vehicle for recruitment and propaganda by extremist organisations. It was noted that the Internet helped enable those who wanted to use cyberspace for terrorist purposes to do so from virtually anywhere in the world: if blocked from operating in one State, they could simply relocate to another or go into the "dark net", and therefore the Internet could offer a virtual safe haven defying national borders and traditional governmental regulation and oversight. In that regard, effectively preventing and countering violent extremism online required innovative and smart public-private partnerships across States, civil society organisations, regional and international organisations, and the private sector. This would require a clear understanding of the challenges that needed to be addressed, as well as the spheres of effective control of each stakeholder, in order to design a multistakeholder framework that could effectively prevent and counter violent extremism online.

Session I: Countering Violent Extremism Online – The Dual Potential of the Internet: Setting the Scene

The discussion was structured around the guiding questions indicated in the concept note, and began by addressing current initiatives and campaigns on countering and preventing violent extremism. State representatives shared their experiences, stressing that a proactive approach, especially the need to develop effective counter-narratives, was required to tackle the phenomenon. However, jurisdictional and linguistic obstacles were considered most challenging. A participant described an Indonesian approach to countering violent extremism,

[1] For more information please see following link http://www.securityhumanrightshub.org/
[2] For more information please see following link http://www.icoca.ch/en/icoc-association

where in the aftermath of terrorist attacks photos and images were not published in order to reduce the likelihood of glorification of such attacks.

In discussing public-private cooperation, it was argued that the main stakeholders in cyberspace were currently "vulnerable" enough to work together on C/PVE. Another participant noted that each stakeholder had its own sphere of control, and that it was crucial to understand what this was and what each stakeholder could reasonably expect the other stakeholders to contribute to such cooperation. It was observed that C/PVE put tremendous pressure on all stakeholders to provide high virtual and physical security standards, and to keep the Internet open and safe.

One participant referred to the UN General Assembly resolution 68/167, stipulating the "offline-is-online"-dictum, or what is illegal offline is also illegal online, as a minimum common denominator. However, this was seen to be difficult to implement in practice as there are different standards for freedom of expression among states, and this could hinder finding a consensus. Another participant generally agreed that there was less global consensus with regard to Article 19 and Article 20 of the International Covenant on Civil and Political Rights, though expressing the opinion that existing hard and soft laws, e.g. UN General Assembly resolutions, General Comments by the Human Rights Committee, case law, etc., provided enough common ground to build on. Nevertheless, it was stressed that any approach required creative and transnational thinking, and must be guided by the principle of legality and proportionality. One participant stressed the high degree of fragmentation of national legislation, referring to the Global Survey of the Implementation of Security Council Resolution 1373(2001) by Member States, as evidence for that. Another participant expressed concern with regard to the principle of legality, and consequently the risk of too broad definitions of "terrorism" and "incitement to terrorism" in national legislations, which could be abused by governments, and be counterproductive and dangerous.

Consequently, it was noted that public international law, in particular the international human rights framework, offers guidance for how to decide which restrictions on human rights would be lawful, i.e. legitimate aim, necessity, and proportionality. Nevertheless, this did not address the challenge of jurisdiction. One participant proposed the idea of a group of like-minded States and other relevant stakeholders working towards a common multistakeholder governance vision. It was further noted that as challenges were dynamic and evolving, it was important to adopt an approach that could respond accordingly. With regard to the call for a

multistakeholder approach, it was stressed that there were already similar initiatives by social media companies, and that it was vital to develop an initiative that included civil society and the private sector in the discussions. Concerning setting international-law based standards for the private sector, a participant described his/her own experience of working in multistakeholder fora to identify and develop clear standards for how companies could implement policies and provide services that were consistent with international human rights standards—both freedom of expression and right to life.

The discussion turned to the question of terminology and definitional challenges. A participant suggested that "preventing violent extremism" (PVE) should be the phrase of choice, since "countering violent extremism" was considered another synonym for countering "terrorism". An innovative project involving religious community leaders in preventing violent extremism was shared with the group. It was highlighted that clear rules and guidance were needed to identify what "violent extremism" constituted in order to bring clarity to discussions. Furthermore, the Rabat Plan of Action was mentioned as offering a threshold test for determining whether content was such that it incited violent extremist behaviour. However, another participant countered that one should not bother too much with definitions, since this might only hinder constructive dialogue, but instead should use broader categories. It was further stressed that the Internet was a self-regulating body, where the private sector developed its own terms and conditions of use, which often go beyond what is contemplated under international human rights law. Moreover, access to remedy was considered another important element.

The ongoing encryption debate between Apple Inc. and the Federal Bureau of Investigation was discussed, recognizing that there were passionate opinions on the matter. It was noted that different States took different approaches, such as countering violent speech with more speech, and that one should be cautious about over-criminalising the exercise of freedom of expression. It was further acknowledged that radicalisation was not happening solely through Internet platforms, often requiring an element of personal contact. However, it was acknowledged that the Internet facilitated access to information, including material promoting violent extremism.

The following discussion focused on the dual potential of the Internet as both a vehicle to facilitate and prevent violent extremism. It was highlighted that there was a tendency to simply block content online, neglecting another powerful asset of the Internet – the use of it

for counter-messaging and for dispelling myths around extremist views. As an example, the United Kingdom's campaign for counter-messaging was mentioned. It was further stressed that the Office of the High Commission of Human Rights put real emphasis on promoting tolerance and diversity, and that it was currently undertaking research on effective counter-narrative initiatives. The issue of to what extent the social media community could actually contribute to effectively counter-messaging was further discussed. It was pointed out that it might be worthwhile to allow the Internet community itself to address violent extremist speech, since the great majority of Internet users oppose that kind of ideas and narratives. It was further noted that there was a need to safeguard against abuse of social media platforms, but that providing guidance was not an easy task, primarily due to the different contexts and jurisdictions.

One participant called for addressing the root causes of radicalisation, since this was an important part of a holistic counter-narrative strategy, and emphasized the highly contextualised nature of radicalisation. The participant further pointed out that merely taking down content was not constructive, since e.g. ISIS had the capacity to develop its own secure communication apps as soon as other channels were blocked. Another participant highlighted that one must not forget an additional actor: traditional media platforms.

When working with the private sector to counter-violent extremism online, it was considered extremely important to ensure appropriate and effective check and balances as well as transparency. The latter was particularly crucial, since many times Internet users were deprived of their right to remedy because they did not know why their content was taken down. It was pointed out that some social media companies included a right to appeal in cases where content was removed (YouTube being one example). Nevertheless, some participants were uncomfortable with social media companies acting as judges and deciding whether or not content was lawful and protected by the freedom of expression.

Session II: Case Study "How the Islamic State Use Social Media to Achieve Its Aims?"

The presentation "*How Does Islamic State Use Social Media to Achieve Its Aims?*" served as a case study and focused on the use of social media for recruitment. The presentation showed that ISIS used different means and memes for recruiting people and spreading its messages. Themes identified were: the "good life" under the ISIS regime, evoking comparisons of life under ISIS to popular videogames, copying and repurposing of popular social media memes and trends, and messages specifically targeting women. ISIS was portrayed as having

developed a highly sophisticated and effective media campaign. After the presentation, one participant observed that ISIS had created two stories: one reflecting the adventurous aspect of life within ISIS, and the other with regard to its "ideal" society, where one can find stability and security. Consequently, the question of what effective counter-stories would look like was raised, in particular what kinds of messages could effectively counter ISIS narratives about western democracies. In that regard, it was stressed that democratic societies had to tolerate a certain amount of critical expression, even if it was disturbing and/or offensive, because that is part of the human right to freedom of expression. Moreover, the shift to intermediary policing by online platforms was seen as something problematic, since it should not be the role solely of Internet companies to regulate and restrict speech. Finally, it was proposed to include an educational aspect in any future initiative as part of a proactive approach that takes into account lessons-learned from the offline-world.

Session III: Wrap-Up

Participants agreed on the importance of developing innovative and effective multi-stakeholder initiatives for countering and preventing violent extremism in the online world, and to learn from already existing public-private partnerships. The following elements were identified as priority areas for follow-up:

- The need to understand how online recruitment for violent extremist groups works, in particular, what makes people respond to existing social media campaigns.
- Closely linked to the first element, an understanding of what is required for counter messaging campaigns to be effective.
- The need to develop clear guidance for internet companies regarding content which should not be hosted on their platforms, as well as
- A shared understanding of the kinds of information governments can and should not request from companies, in line with international human rights standards.
- The need for a relatively small group of like-minded actors from all stakeholder groups to work together on these elements, and to identify the areas in which each stakeholder group enjoyed effective control in order to more effectively structure public-private partnerships that could prevent and counter violent extremism.

The meeting ended with a consensus that the discussions should be continued in subsequent meetings.