Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

DCAF
a centre for security, development and the rule of law

PREVENTING VIOLENT EXTREMISM ONLINE THROUGH PUBLIC-PRIVATE PARTNERSHIPS

8 April 2016

Palais des Nations, Salle XXIII

Report

Executive Report

On 8 April 2016, the Federal Department of Foreign Affairs of Switzerland hosted in cooperation with the Geneva Centre for the Democratic Control of Armed Forces (DCAF) a discussion on "Preventing Violent Extremism Online Through Public-Private Partnerships" at the Palais des Nations, in Geneva. It was organized in the context of the Geneva Conference on Preventing Violent Extremism which was organized by the United Nations in partnership with the Government of Switzerland.

The discussion was moderated by Ambassador Benno Laggner, Division for Security Policy at the Federal Department of Foreign Affairs of Switzerland, and was composed of the following experts:

- Mr Steve Crown, Vice-President and Deputy General Counsel at Microsoft;
- Mr Marc Porret, Legal Officer at the UN Counter-Terrorism Committee Executive Directorate (UN-CTED);
- Mr Jonathan Russell, Head of Policy at Quilliam Foundation;
- Mr Peter Stern, Policy Manager at Facebook;
- Representative of the EU Internet Referral Unit at Europol

The side event offered a platform where relevant actors could articulate and discuss their respective needs, challenges, and priorities in preventing violent extremism online. It looked at addressing key challenges in that regard, such as the absence of a commonly accepted definition of what constitutes violent extremism, and the lack of an international consensus around legitimate, human-rights compliant restrictions on certain fundamental rights, such as the right to freedom of expression. Discussions were centred on the issue of misuse of the Internet, in particular of social media platforms, by violent extremist organizations for purposes of recruitment and propaganda.

Panellists emphasized the vital importance of establishing successful and innovative partnerships between the public and the private sector, with active engagement of civil society. It was emphasized that the rule of law and the international human rights law framework were vital pillars for any future actions aiming at preventing violent extremism online. Panellists noted that effectively preventing violent extremism online requires a holistic approach that envisages alternative messaging, developed through active involvement of relevant cultural and religious communities.

Key Findings:

- Multi-stakeholder collaboration is key to preventing violent extremism online. Such collaboration requires efforts in strengthening trust between the public and the private sector, and can only be sustainable if there is active engagement with civil society. In order to build trust between the actors, it is vital to improve channels of communications.

- Any technology can be used for good and for bad. In fact, the Internet was designed to offer infinite opportunities for the economy and society as a whole. It was developed as a tool for sharing and collecting information, for fostering democratic participation, and eventually to promote development.
- There is no “one-size-fits-all” approach for preventing violent extremism online but there is a need for a better understanding regarding ‘push’ and ‘pull’ factors.
- Alternative narratives need to be developed in close consultation with communities and civil society in order to provide people responsive to radical and violent ideas with alternatives. Notably, the message and in particular the messenger have to be trustworthy and authentic.

Preventing Violent Extremism Online Through Public-Private Partnerships

In the context of the Geneva Conference on “Preventing Violent Extremism”, the Federal Department of Foreign Affairs of Switzerland hosted in cooperation with the Geneva Centre for the Democratic Control of Armed Forces (DCAF) a discussion entitled “Preventing Violent Extremism Online Through Public-Private Partnerships” on 8 April 2016 at the Palais des Nations in Geneva.

Presentations were made by:

- Mr Steve Crown, Vice-President and Deputy General Counsel at Microsoft;
- Mr Marc Porret, Legal Officer at the UN Counter-Terrorism Committee Executive Directorate (UN-CTED);
- Mr Jonathan Russell, Head of Policy at Quilliam Foundation;
- Mr Peter Stern, Policy Manager at Facebook;
- Representative of the EU Internet Referral Unit at Europol

The panel discussion was moderated by Ambassador Benno Laggner, Division for Security Policy at the Federal Department of Foreign Affairs of Switzerland.

This summary is based upon the presentations given by the panellists.

Misuse of the Internet and social media platforms

Any new technology can be used for good or bad, and the Internet, and social media platforms in particular, demonstrate this once more. As the online world provides easy and often anonymous access to a large audience, it is not surprising that certain violent extremist organizations have turned to the Internet as a vehicle for propaganda and recruitment. This has been further bolstered by increased use of social media and the ease of sharing images, videos, and texts.

A successful international response to this phenomenon has been hampered by jurisdictional obstacles, the absence of a common definition for “violent extremist content”, and the lack of trust between the public and the private sector. States are adopting new laws intended to regulate this phenomenon, but many of these undermine the concept of an open Internet. In addition, States are increasingly putting pressure on private information and communication technology companies to regulate and remove unlawful online content. At the same time, private companies are attempting to strike a balance between complying with States’ requests and their users’ expectations of the right to freedom of expression and right to privacy.

Therefore, it was considered of vital importance to engage in an effective and open dialogue between the public and private sector and civil society in order to develop a human-rights-compliant understanding of content that should be removed from online platforms.

There is no 'one-size-fits-all' solution

It was noted that there is no 'one-size-fits-all' solution to preventing violent extremism online. This was especially considered true, since there is great divergence between the roles and responsibilities within each group of stakeholders. This was exemplified by the differences private companies are facing when dealing with this issue, e.g. Microsoft Cooperation, compared to social media giants, such as Facebook, Twitter or Google.

However, it was stressed that international human rights law standards and the rule of law are fundamental and consequently must be at the forefront of any future action in preventing violent extremism online. Complying with these standards would necessarily require a transparent and open process, an independent review procedure with regard to content removal, and an effective access to remedy. Transparency reports by information and communication technology companies were considered a first step into the right direction. Moreover, it was noted that private companies do have a self-preserving/economic interest in keeping their respective platforms free from violent extremist content, and many have already developed detailed preventive policies and procedures. It was noted that not only well-established information and communication technology companies have such an interest, but also small start-ups that would like to break into the market, since complying with such standards could offer legitimacy and users' trust.

Social media platforms, such as Facebook or Google, have teams working all over the world in all relevant languages to remove content that contradicts their terms and conditions of use. One panellist further noted that his company was closely collaborating with civil society in order to help facilitating the spreading of successful counter-messages. According to studies, counter-messages seem to be most effective when there is not only text but also photographs, when they are phrased in positive rather than in negative language, and when they are perceived as authentic, which leads to the question of who is an authentic messenger. Furthermore, this company established support groups to assist civil society organizations in their efforts to spread alternative narratives and to share their knowledge and expertise with them. However, participants were reminded that social media platforms do not provide content themselves, but merely provide platforms, implicitly raising the sensitive issues of intermediary liability and the risk of self-censorship by social media companies.

The possibility to have a stricter threshold test for lawful content on social media platforms determined according to the terms and conditions of use of the respective private companies was not seen as problematic, but rather as part of the solution; where a company's policy is in accordance with international human rights law standards.

Content Removal

It was uncontested that international human rights law itself provides for the lawful restriction of the right to freedom of expression under certain circumstances. It was further noted that UNSC resolution 2178 criminalizes the recruitment of foreign terrorist fighters, and that a number of UN Security Council resolutions urge States to criminalise such recruitment, and that Article 20 (2) of the International Covenant on Civil and Political Rights (ICCPR) explicitly prohibits "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence". It was argued that this would provide sufficient legal basis to remove content that apparently is considered unlawful under various resolutions and international conventions. However, other participants noted that not all States are party to the relevant convention and that certain States have made reservations to Article 20 ICCPR.

In addition, it was further acknowledged that removing unlawful online content faces additional challenges, such as definitional and jurisdictional obstacles.

A new public-private initiative launched by the UN Counter-Terrorism Executive Directorate (UN-CTED) in partnership with ICT4Peace to look at these issues was introduced.

Panellists agreed that especially with regard to removing content from online platforms, cooperation with the private sector was key. This need for cooperation was exemplified with regard to the newly established European Union Internet Referral Unit (EU IRU), embedded in Europol. The EU IRU has two main purposes: Firstly, to reduce online content that is considered unlawful. Secondly, to undermine extremist narratives and to actively engage with civil society in developing alternative messages. In all its activities, the EU IRU has to comply with standards and regulations adopted both by the European Union and the Council of Europe. However, due to the fact that most social media companies are located outside of the European Union, and the EU IRU can only act within the territory of Member States, the EU IRU lacks effective enforcement mechanisms and thus has to rely on the voluntary cooperation of these private companies. The decision to remove content nonetheless lies within the discretion of the company. Consequently, it is in the very interest of the EU IRU to have an open dialogue and constant exchange with the private sector.

Need for a holistic approach

It was noted that taking down unlawful content was only one way to address the phenomenon but did not necessarily reflect the whole range of possible actions. It was stressed that understanding the 'push' and 'pull' factors and the reasons why certain extremist organizations were so successful in recruiting people and spreading their narratives were vital in addressing violent extremism online. It was noted that

more research in that regard was needed, and that existing research should be better implemented in actual action plans.

Furthermore, it was underlined that many extremist organizations are constantly using social media, simply because they know that these technologies ease the sharing of peoples' similar views hundreds of miles apart and reinforce their worldviews by building echo chambers. It was stressed that for the moment the overwhelming response has been to shut down technology rather than use it more effectively. Put differently, it is time to get counter-messaging into tweets. Moreover, it was stressed that radicalization starts long before extremist groups get involved. However, these extremist organizations understand how to resonate with a younger demographic segment. In other words, and as one of the panellists noted, these extremist groups "offer a call to action to the Call of Duty generation with an offer that empowers people to do something to change their situation. [They] understand that [their] audience is always plugged in, always activist, always aggrieved but now empowered to do something rash about it." It was noted that the current responses have often been less engaging and less tangible, offering a call to inaction not to action, and failing to connect the online with the offline.

Three recommendations were made. Firstly, to broaden the counter-communication efforts to include all forms of violent extremism. Secondly, to understand the target audiences and the broader trends to build a strategic response. Thirdly, to work better together, meaning public-private partnerships that effectivly engage with young people, civil society, and existing grassroots campaigns.

Summary

It became evident during the discussions that preventing violent extremism online requires effective and innovative public-private partnerships, and that such multi-stakeholder initiatives have to be built on the rule of law and international human rights law standards. It was underlined that prerequisites for these public-private partnerships are rebuilding of trust between the public and the private sector and close cooperation with civil society, in particular with religious and cultural communities.

Violent extremist content removal was considered as one possibility to prevent the spreading of such narratives, and ultimately the recruiting of persons responsive to such violent extremist messages. It was noted that there was a particular role for the private sector to play. Due to the divergent views of what constitutes "violent extremist content" between States, private information and communication technology companies could adopt company policies that define content that should be considered unlawful on their platforms. However, it was stressed that any policy has to comply with international human rights law standards, be transparent, and offer an independent review process, and effective remedies.

It was further noted that only a holistic approach could ultimately be successful. Holistic in the sense of trying to understand the ‘push’ and ‘pull’ factors as well as the reasons why certain people are responsive to these violent extremist narratives. A Holistic approach should then develop, in close cooperation with cultural and religious communities, authentic alternative messages that resonate with people at risk. Finally, it was emphasized that things do not simply start and end in the online world but are always related to the offline world, and this should be considered in any future actions.