Review of "Hate and Violent Extremism from an Online Sub-Culture"

By Prof. Raphael Cohen-Almagor

I have read Dr Oboler's extensive report with great interest. The report is very thorough and important. Hate and terrorism are of significant concern worldwide. Increasingly, the relationships between hate speech, hate crime and terror is becoming very clear. We need to balance one against the other two important principles: freedom of expression and social responsibility. Social responsibility is no less important than freedom of expression. Freedom without responsibility in this era of political extremism might prove to be dangerous as hate mongers and terrorists exploit Internet freedom and abuse it to target their victims.

The forefathers of the Internet had the vision of creating a free highway, a public space where everyone can say what he or she has in mind. This wonderful innovation of unfettered platform has backfired. The Internet is open for use and abuse. We should provide and promote responsible use and we should also fight against those who abuse. Their abuse corrupts public space and is posing many challenges on all levels: individual, the community, the state and the international community. We are in the early stages of learning how to cope and how to combat the abuse. Slowly we are developing the necessary tools to enjoy innovation and freedom while, at the same time, we are adopting safeguards and rules of responsible conduct.

In historical terms, the Internet is an infant. It came into our lives in 1993-1994, thus it is less than thirty-year old. The western world has been slow to devise ways to fight Internet abuse and left much responsibility to the Internet Giants. They have failed to deliver safe and secure environment and are still permitting much abuse. Dr Oboler suggests that "Content services should create mechanisms that enable them to restrict access to specific content on their service for users from countries where that content is illegal."

Indeed, what is important in this report is that Dr Oboler makes concrete recommendations for action. I agree with him that any effective response will require the active participation, cooperation and investment of governments, technology companies, and civil society as partners with a shared interest in combating hate and terror that have become a significant threat to our globalised societies.

The Internet

The Internet burst into our lives in the early 1990s without much preparation or planning, and changed them forever. It has affected virtually every aspect of society. It is a macro system of interconnected private and public spheres: household, literary, military, academic, artistic, business and government networks. The Internet has produced major leaps forward in human productivity and has changed the way people work, study and interact with each other. The mix of open standards, diverse networks, and the growing ubiquity of digital devices undermines traditional media and challenges existing regulatory institutions based on national boundaries. The Internet has created new markets and has changed the way people interact, find leisure, explore the world and think about human phenomena. In the Internet age, people often have cyber life in addition to their offline life. The two -- real life and cyber life -- are not necessarily one and the same.

Undoubtedly, the Internet has obvious advantages for modern terrorism. It is diffused and decentralized; it is lacking a coherent structure; it is global and quite chaotic. The threat of terrorism is real and significant. As the Internet became a major arena for modern terrorists, we need to devise appropriate methods to forestall their activities and establish security.

While a great deal is dependent on how we use the Internet, a great deal is also dependent on the Internet gatekeepers. These companies possess immense power. Power without responsibility is dangerous. Power without responsibility is corrosive. Power without responsibility undermines our well-being. Therefore, we must insist that Internet intermediaries will take responsibility and ensure that Netusers will be able to enjoy the vast capabilities of the Internet without putting themselves in danger. The Internet's way should not be in harm's way. The Internet's way should be enlightening, innovative, entertaining, productive, giving a voice to the best of humanity. To enable this, boundaries should be introduced, antisocial and violent activities should be curbed, safe environment should be established. This is a combined effort of Netusers, business, countries and the international community at large.[1]

[1] Raphael Cohen-Almagor, *Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway* (NY and Washington DC.: Cambridge University Press and Woodrow Wilson Center Press, 2015).

The role of Internet intermediaries

Internet intermediaries are gatekeepers and, therefore, they bear responsibility for their conduct. The Internet brings together like-minded people and creates a forum for them to discuss and exchange ideas. While the Internet is not the cause of terrorism, it does support and accelerate terror. Unfortunately, we are living in an age of terrorism and political violence. The recent surge in terrorism has been aided by the Internet. Dr Oboler rightly notes that attempts to reduce level of terrorism should include reducing opportunities provided by the Internet to access terrorist information. The electronic environment is more than incidental to behaviour. It is shaping behaviour and influence conduct. The Internet has frustrated security agencies as it has increased the amount of terrorist information as well as the number of individuals accessing that information.

Internet intermediaries have a central role to play. There legal obligations vary across jurisdictions. Presently much depends on their self-regulation and the extent of their cooperation with security agencies. All major ISPs have codes of conduct. Codes of conduct should ensure that Internet content and service providers act in accordance with the law and with principles of social responsibility. These codes should meet community concerns and industry needs, operating as an accountability system that guarantees a high level of credibility and quality. Because of the transnational nature of Internet communications, Dr Oboler accentuates that coordinated activity among Internet intermediaries in different jurisdictions needs to be an essential element of self-regulation. And there should be widespread use of rating and filtering technology. To this end, content providers should be mobilized to label their content voluntarily, and filters must be made available to empower Netusers to make effective choices about information received. Jurisdictions that endorse intermediaries' self-regulation should measure the effectiveness of such regulatory mechanisms in order to determine what national and transnational measures – if any – are necessary to compensate for their deficiencies.

Large Internet intermediaries should have active cyber patrols that search for violent content. They should also have integrity teams, instructing providers to take off inappropriate content.

Large Internet intermediaries should also have easily identifiable and accessible hotlines to enable Netusers to report illegal activities. In this regard, Dr Oboler asserts: "Platforms should take all reasonable steps to facilitate and encourage the reporting of material depicting and promoting violent extremism, as well as all other

reasonable steps to identify such material themselves. They should expeditiously remove such material once they become aware of it. Provided the above steps are taken, there should be a clear safe harbour protecting platforms from liability for material they are unaware they are hosting."

The major Internet intermediaries are, for the time being, American. They see the Internet as a free highway for exchange of opinions and for making money. They are products of the First Amendment and the Land of the Free. These companies have been enjoying much freedom until now as the world is learning to cope with the Internet constant innovations.

YouTube

Most certainly, Internet intermediaries should not be conduit to illegal and anti-social activities. Take YouTube as an example. YouTube has Respect the YouTube community standards.[2] One of them concerns violent or graphic content. It says: "It's not okay to post violent or gory content that's primarily intended to be shocking, sensational, or disrespectful. If posting graphic content in a news or documentary context, please be mindful to provide enough information to help people understand what's going on in the video. Don't encourage others to commit specific acts of violence."[3] YouTube is not enforcing its own standards. Having community standards and not enforcing them is a sham. In this regard, Dr Oboler suggests that "All companies providing Internet infrastructure should have clear terms of service which prohibit the use of their service for inciting hate or violence. They should also give notice that the service may be terminate without notice for serious breaches of this rule. Companies may further wish to require that any customer they provide a service to includes a similar statement in its terms of service."

YouTube is not only a video hosting site. It is also a formidable social networking forum. Contributors can draw the attention of registered subscribers who then are able to comment on video uploads and communicate with the source. Users are able to subscribe to each other's feeds based on mutual interests.

Producing and distributing media for foreign terrorist organizations constitutes material support for terrorism. Service providers that knowingly assists in the

[2] http://www.youtube.com/yt/policyandsafety/communityguidelines.html

[3] http://www.youtube.com/yt/policyandsafety/communityguidelines.html

distribution of terrorist media are also culpable. Internet intermediaries must be made to realize that they can neither turn a blind eye to the use of their services by terrorist organizations, nor can they continue to put the onus of identifying and removing terrorist media on private citizens. While I find it hard to believe that Google, operator of YouTube, has an interest in promoting terrorism, and while Google has taken some steps to address the danger emanating from YouTube, Google can and should do more. As Google and other companies are reluctant to take the necessary steps, it is the role of governments to step in and demand far more efficient proactivity in fighting online terrorism. In this regard, Do Oboler advises: “Google should commit to supporting the Christchurch Call across all parts of the business without exception. This includes preventing Google’s search engine being used to access material promoting terrorism”.

Facebook

Dr Oboler mentions that in March 2019, a terrorist murdered 49 people and wounded 48 others in shootings at two mosques in Christchurch, New Zealand. This was the nation's deadliest attack. The terrorist live streamed the rampage at Al Noor mosque to Facebook from a head-mounted camera. The live-stream of the attack lasted for 17 minutes. Through social media, the terrorist conveyed his racist, hateful and violent messages that quickly found their way onto the front pages of some of the world's biggest news websites in the form of still images, gifs, and even the full video. One version of the video was left live on Facebook for at least six hours, while others were available on YouTube for at least three hours. The footage was viewed more than 4,000 times before being taken down. It took 29 minutes to detect the livestreamed video, which was eight minutes longer than it took police to arrest the terrorist. About 1.3m copies of the video were blocked from Facebook but 300,000 copies were published and shared. Facebook spokesman Simon Dilner said that it could have done a better job and was prepared for regulatory action. Dr Oboler recommends: “When a violent extremist attack is livestreamed the platform that was used to stream the incident and / or host the initial video of the incident should provide transparency on exactly when the livestream and/or video was first reported to them and when exactly they acted to remove it.”

Several companies, including the ANZ and ASB banks, have stopped advertising on Facebook after the company was widely condemned by the public.

Under pressure to mend ways, in May 2019 Facebook announced it was tightening rules around its livestreaming feature. The announcement came ahead of a meeting of world leaders aimed at curbing online violence in the aftermath of a massacre in New Zealand. French President Emmanuel Macron wishes to introduce new rules which would punish any site that publishes violent content or extreme opinions.[4] In this respect, Dr Oboler argues: "Governments should consider law reforms to create a system of sanctions that could be imposed on companies outside their jurisdiction who, after suitable notice, continue to provide unlawful content inciting hatred or violent extremism to users in that country in breach of the country's law. Such law reform could also create sanctions that impose penalties for any company within the country's jurisdiction who engaged in business with a company on the sanctions list."

Following the Christchurch terror attack, Facebook announced that it is investing in research to build better technology to quickly identify edited versions of violent videos and images and prevent people from re-sharing these versions. Calls to include significant time delays in live streams are impractical as the result might be detrimental to legitimate live streaming of many good causes critical to the public interest.

The Christchurch terrorist cited white genocide conspiracy theory as the main justification for the terror attack. That conspiracy theory has been spread by several Facebook pages. For many years, Facebook has allowed extreme groups who endorse violence, including Nazi groups and white supremacists, to use the company's platform as its business model is to enable the widest possible freedom of expression. Facebook now realises that at stake is far more than freedom of expression.

Conclusion

Hatred is an extremely sensitive matter, with horrendous results as racism leads to crimes and increasingly, especially after the Anders B. Breivik attack in Norway in 2011, to terrorism. In order for us to understand the danger, we need to know what

[4] David Reid, "Tech companies face stiff criticism for their inability to prevent extremism from spreading via their platforms", *City AM* (May 14, 2019), http://www.cityam.com/277554/big-tech-must-take-lead-against-hate

words hate mongers and terrorists are using to promote their goals. Dr Oboler rightly notes that incubated by a globalised, toxic, anonymous online culture, incitement to hate now all too frequently leads to violent extremism that manifests offline, and has cost the lives of dozens of innocents, including children. Participants and spectators of this newly forged online culture encourage, support and celebrate the serious crimes that they commit, and revel in the chaos and destruction they inflict.

More than 25 years after the Internet entered its mass commercial phase, we can now conclude that self-regulation does not work. Self-regulation does not work when offline media is concerned, and it is certainly failing online. Governments must step in and enforce cohesive and protective rules of conduct to prevent harm, protect vulnerable populations and save life. Now that we have learned the hard way the consequences of having a powerful free highway of technology, I join Dr Oboler in thinking it is time for change.