FRANCE
BIARRITZ
2019

FOR A SAFER WORLD

POUR UN MONDE
PLUS SÛR

OUTCOME DOCUMENT

COMBATING THE USE OF THE INTERNET FOR TERRORIST AND VIOLENT EXTREMISTPURPOSES

The terrorist attack perpetrated on 15 March 2019 in Christchurch was live streamed online and disseminated across a range of large and small online platforms. This enabled within minutes thousands worldwide to view, duplicate and broadcast millions of copies of the video of the mass shooting before extensive action could be taken to remove the terrorist content. The Christchurch tragedy highlighted once more the use that can be made of the Internet for terrorist and violent extremist purposes.

Worldwide, a large number of terrorist groups, ranging from Da'esh to far-right violent extremists, contribute to putting online information related to the preparation, funding, displaying or claiming of terrorist acts. The Internet thereby plays a key role in terrorist radicalisation processes and terrorist attacks, including those perpetrated recently in G7 countries.

In spite of losing its last-held territory in Syria, Da'esh still maintains an online presence and continues disseminating its propaganda on the Internet in order to radicalize, recruit, and inspire new followers to plan and lead terrorist attacks on a global scale, including in G7 countries.

Therefore, preventing and countering violent extremism and terrorism inevitably requires an active role by governments and Internet companies. For this reason and since the G7 meeting of the Ministers of Interior in Ischia, the G7 Ministers of Interior and the major Internet companies have undertaken a constructive dialogue on the importance of removing online terrorist and violent extremist content quickly, in October 2017. Furthermore, G7 countries have also established bi- and multilateral dialogues with Internet companies in efforts to prevent and counter the use of the

Internet for violent extremist and terrorist purposes. In Europe this has occurred within the framework of the EU Internet Forum. The Toronto G7 Security ministers' commitments recognized the Global Internet Forum to Counter Terrorism (GIFCT) as the main representative of Internet companies on this issue by providing a collective, industry-wide voice and coordinating efforts of Internet companies. All of these dialogues have helped raise awareness among the major Internet companies about the risks related to the use of the Internet for terrorist and violent extremist purposes, and associated reputational risk.

However, the results and the effectiveness on content removal remain varied, especially when it comes to smaller platforms. Some countries and regional organizations have decided so far to continue to support voluntary collaboration only, while some have decided to use, in addition, a legislative approach to make sure Internet companies cooperate and swiftly remove content identified as online terrorist and violent extremist content. This is the approach that the European Union has opted for, and legislation is currently in the process of being adopted to this effect.

In addition, in some cases, investigation and prosecution services still encounter challenges in accessing the digital evidence needed for counter-terrorism investigations. Indeed, search warrants for digital evidence are often not able to be executed because of the difficulties for law enforcement services to get lawful access to data, in particular to encrypted electronic communications., Faster access to this digital evidence, pursuant to lawful authority and with respect for human rights and fundamental freedoms, is important for investigation and prosecution services to fulfil their mandates and to ensure the effectiveness of investigations. A key consideration is to ensure that law applies online. Proposals in this area must nevertheless enable society to continue to access and maintain confidence in the many benefits of encryption.

Thus, the G7 Ministers of Interior commit to implementing the following:

- Call on Internet companies to improve communication and transparency around their efforts to prevent and counter the use of the internet for violent extremist and terrorist purposes, both with our governments and citizens;

- Reiterating the G7 Toronto Commitment, call on Internet companies to continue to more swiftly identify and remove all terrorist and violent extremist content within one hour of upload, as technically feasible without compromising accuracy, and to assess as a matter of priority notices from

trusted flaggers and provide feedback on action taken through the development and responsible use of relevant technological means and the allocation of a dedicated workforce;

- Request that Internet companies establish protocols in emergency situations to remove violent extremist and terrorist content, inclusive of safeguards to protect legitimate news reporting;

- Request the Internet companies to continue to take proactive measures to protect their services against the uploading of terrorist and violent extremist content, and furthermore swiftly identify and establish procedures to ensure the removal of violent extremist and terrorist content, with the possibility to law enforcement services to get access to this content if needed, and prevent its reappearance online and dissemination across platforms, including through consistent expansion and use of the GIFCT's shared database of hashes;

- Encourage the major Internet companies to continue to support small platforms abilities to identify and to remove online violent extremist and terrorist content, by making technical means available and facilitating their access to the GIFCT's shared data base of hashes, in particular through increased support to "Tech Against Terrorism" affiliated with the Counter-Terrorism Executive Directorate of the United Nations and non-governmental organisations;

- Promote further Internet companies' support of relevant stakeholders, including researchers and academics in G7 countries, to better understand how to prevent and counter the use of the Internet for violent extremist and terrorist purposes, in particular through sharing of data, in accordance with the applicable data protection laws and regulations;

- Encourage Internet companies to have appropriate safeguards in place to prevent the erroneous removal of online content, taking into account the fundamental importance of the freedom of expression and access to information in an open and democratic society;

- Reiterate the G7 Toronto commitment to encourage Internet companies to include in their Terms of Service information on the consequences, under the applicable national law, of sharing violent extremist and terrorist content and clearly outline the process of reporting such content to all users;

- Build digital and media resilience through education, training initiatives, which empower people to think critically and identify misleading information, including through collaboration with civil society organisations;

- Furthermore some G7 countries may choose to adopt national or regional legislation to impose the removal of online violent extremist and terrorist content to Internet companies within the hour following a removal order and endeavour to appoint a legal representative in each of the States they are based in, as well as a 24/7 operational contact point;

- Urge Internet companies to continue to create tools to address algorithmic confinement regarding violent extremist and terrorist content, notably by promoting positive alternative and counter-narratives developed by relevant stakeholders, including civil society;

- Encourage Internet companies to establish lawful access solutions for their products and services, including data that is encrypted, for law enforcement and competent authorities to access digital evidence, including when it is removed or hosted on IT servers located abroad or encrypted, without imposing any particular technology and while ensuring that assistance requested from internet companies is underpinned by the rule of law and due process protection. Some G7 countries highlight the importance of not prohibiting, limiting or weakening encryption;

- Continue to jointly explore with Internet companies the means to allow access of law enforcement services to removed terrorist content in order to ensure consistent and systematic exploitation of such content to identify, locate and pursue perpetrators portrayed in terrorist materials, as well as to facilitate forensic data analysis, in a manner that complies with applicable law;

- Consider taking the necessary measures to ensure that Internet companies address production orders sent by law enforcement and competent authorities, when it is appropriate; Some G7 countries may choose to establish legal frameworks at national, regional, and international scale

- Explore opportunities for enhanced legal cooperation to address the evolution of cloud storage, through consideration of a Second Additional Protocol to the Budapest Convention on Cybercrime;

- Implement the aforementioned commitments in full compliance with human rights obligations, including those relating to freedom of expression, privacy and due process.

The G7 Ministers of Interior call on the Roma-Lyon Group to ensure the monitoring of these commitments' implementation, including within the existing frameworks of dialogue with Internet companies, and assess the possibility of extending them to matters of wider online harms calling to violence.

In addition, the G7 Ministers of Interior request the Roma-Lyon Group, building on the work of its High-tech Crime Subgroup, to establish a full picture of the security risks that could impact law enforcement services with regard to counterterrorism and cybercrime in the context of the roll-out of the new generation of 5G mobile communication networks, through continuous and instant data transfer.