FIVE COUNTRY MINISTERIAL

Emerging Threats
London 2019

Joint Meeting of FCM and Quintet of Attorneys-General

1. On 30 July, Home Affairs Ministers and Attorneys General met together. We discussed countering child sexual exploitation and abuse, countering violent extremism and terrorism both online and offline, foreign terrorist fighters, and encryption.

Countering Online Child Sexual Exploitation and Abuse

1. Noting the pervasiveness of this abhorrent behaviour across the open and dark web, we commit to support more effective prevention, disruption and investigative responses to this grotesque violation of children.
2. We commit to prioritise the sharing of technology, data and expertise between us to help tackle the global threat of online child sexual abuse, recognising the great benefits that would come from closer cooperation, especially as we explore technologies to respond to new threats such as the live streaming of child sexual abuse.
3. We reaffirm our commitment to the WePROTECT Global Alliance, a partnership of Member States, global technology companies and international and non-governmental organisations working together to end online child sexual exploitation and sexual abuse.

Use of the Internet for Terrorist and Violent Extremist Purposes

1. The internet must not be a safe haven for terrorist and violent extremist content and activity. At the same time, our efforts, including with digital industry, to combat terrorist and violent extremist purposes must be undertaken in a manner consistent with national and international law, including protections for human rights and fundamental freedoms.
2. To this end, we reaffirm our commitment to supporting academic and civil society research on all forms of terrorism and violent extremism, including on the challenges of defining and addressing terrorism and violent extremism, better understanding algorithmic confinement, and developing credible counter and alternative narratives.
3. We commit to continue to work with digital industry to establish protocols for emergency situations, as well as safeguards to protect news reporting.

4. We reaffirm our commitment to engage smaller platforms in addressing their exploitation by violent extremists and terrorists, developing and sharing ways to support their efforts to reduce their exploitation and encouraging industry to work together to share understanding and build capacity to tackle the threat across all platforms.
5. We also commit to support increased information flows between digital industry and the Five Countries, including by providing threat-related information to digital industry from the security, intelligence and law enforcement communities to better inform how they moderate content. To build our collective understanding, we also encourage companies to share more data and information about how terrorists exploit their services and their efforts to disrupt this with governments, law enforcement and civil society.
6. We commit to collaborate on progressing the important work that has been undertaken in other likeminded fora, such as the strengthening of the Global Internet Forum to Counter Terrorism and facilitating broad collaboration, drawing on as appropriate the goals of:
    a. The G20 Osaka Leaders' Statement on Preventing the Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism; and
    b. The Christchurch Call to Action.
7. We call on the Countering Violent Extremism Working Group to facilitate information and knowledge exchange on all forms of violent extremism and terrorism.

Online Safety and Encryption

1. Reflecting the statement of principles on access to evidence and encryption agreed in 2018, we are committed to strong encryption, which enables commerce, improves cyber security, and protects the privacy of our citizens' data. We are committed to protecting our citizens from harm. We note the commitments made by tech companies to protect their users' data, their efforts to create a positive environment for their users and their support to properly authorised law enforcement operations. Security enhancements to the virtual world should not make us more vulnerable in the physical world.

2. We are concerned where companies deliberately design their systems in a way that precludes any form of access to content, even in cases of the most serious crimes. This approach puts citizens and society at risk by severely eroding a

company's ability to identify and respond to the most harmful illegal content, such as child sexual exploitation and abuse, terrorist and extremist material and foreign adversaries' attempts to undermine democratic values and institutions, as well as law enforcement agencies' ability to investigate serious crime. Tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain access to data in a readable and usable format. Those companies should also embed the safety of their users in their system designs, enabling them to take action against illegal content. As part of this, companies and Governments must work together to ensure that the implications of changes to their services are well understood and that those changes do not compromise public safety.

3. This is a shared challenge that requires urgent action by Governments, industry and civil society, focused on reasonable proposals, respecting different perspectives and based on core values.

4. We therefore welcome approaches like Mark Zuckerberg's public commitment to consulting Governments on Facebook's recent proposals to apply end-to-end encryption to its messaging services. These engagements must be substantive and genuinely influence design decisions. We share concerns raised internationally, inside and outside of government, about the impact these changes could have on protecting our most vulnerable citizens, including children, from harm. More broadly, we call for detailed engagement between governments, tech companies, and other stakeholders to examine how proposals of this type can be implemented without negatively impacting user safety, while protecting cyber security and user privacy, including the privacy of victims.

Foreign Terrorist Fighters

1. Whilst Da'esh has lost the territory of the so-called 'caliphate', as an international community we remain vigilant against terrorism and the continued threat posed by Foreign Terrorist Fighters (FTFs). Within Syria and Iraq, Da'esh has transitioned back to its covert insurgency roots. Some of its members continue to pose a threat both in the region and more widely, whilst others are detained and best efforts must be made to bring them to justice.

2. The Five countries must continue to take the lead in addressing the issue of FTFs effectively, both in our own countries, and providing appropriate support to those countries most affected. We commit to maintain the international focus on addressing both relocating FTFs, and those now in detention. We commit to:

- Take steps to coordinate, deconflict and prioritise our respective capacity building overseas in third countries, including through effective use of multilateral organisations such as United Nations (UN), and the Global Counter Terrorism Forum (GCTF).

- Support third countries to fully implement UN Security Council Resolution (UNSCR) 2396, including providing support to build capability to collect, process and analyse Advance Passenger Information (API) and Passenger Name Record (PNR) data, to collect and use biometric data, to develop terrorist watchlists and share watchlist information, and contribute to and use Interpol databases, with full respect for human rights and fundamental freedoms, for the purpose of preventing, detecting and investigating terrorist offenses and related travel.

- Support the International Civil Aviation Organisation (ICAO) PNR Task Force to establish a global standard for the responsible use and protection of PNR data that can resolve conflicts of law that inhibit the international transfer and processing of PNR data, as well as to support the work of the UN to build Member States' capability to collect, process and analyse API and PNR data.

- Work together to promote Battlefield Evidence best practice and guidelines to improve global standards for the collection and use of Battlefield Evidence in investigative and judicial processes, including the Guidelines on the collection, use and admissibility of military-collected information presently under development by the UN.

- Share frameworks and tools between the Five Countries on managing residual risk.

Conclusion

1. We reaffirm today the critical importance of the Five Country partnership. Bound by our history of cooperation, united by our shared values, and strengthened by our enduring friendship, we pledge the commitments made today as we seek to share opportunities and address security challenges together.