Five Country Ministerial 2018

Official Communiqué

1. We, the Homeland Security, Public Safety, and Immigration Ministers of Australia, Canada, New Zealand, the United Kingdom, and the United States met on the Gold Coast, Australia, on August 28-29 2018, to discuss how we can better collaborate to meet our common security challenges. We reaffirmed that the close and enduring five country partnership, developed following the Second World War, remains fundamental to the security and prosperity of our nations.
2. The 2018 Five Country Ministerial (FCM), which in previous years has achieved advancements in information and intelligence sharing on border protection and counter-terrorism, has matured to become the pre-eminent forum for collaboration among the five countries on domestic security issues. This year's FCM meeting recalibrated the forum to focus on tangible deliverables and practical collaboration on counter-terrorism, countering violent extremism, cyber security, countering foreign interference, protecting critical infrastructure, border management and law enforcement.

A free, open, safe and secure internet

3. The internet and digital technologies are increasingly central to contemporary life and to the social and economic development of our societies. Global connectivity enables faster communication, better access to services, and new ways to conduct business and share news and information. We affirmed our vision for a free, open, safe, and secure internet, which is fundamental to our economic growth and prosperity.
4. Just as the internet provides many benefits, it also provides opportunities for people to carry out crimes and spread illicit content. Terrorism, child sexual abuse and exploitation, violent extremism, and coercive acts of interference and disinformation are enduring concerns of government. The anonymous, instantaneous, and networked nature of the online environment has magnified these threats and opened up new vectors for harm. Governments have a responsibility to protect those within our borders against both physical and digital threats, and to ensure that the rule of law prevails online, as it does offline. We have a responsibility to tackle these challenges in a coordinated and effective way.
5. While senior digital industry representatives did not accept our invitation to participate in discussions on pressing issues regarding the illicit use of online spaces, we reiterated the need for digital industry to take more responsibility for content promulgated and communicated through their platforms and applications. We agreed to a Joint Statement on Countering the Illicit Use of Online Spaces, outlining our communities' high expectations of digital industry companies, with a focus on countering online child sexual abuse and exploitation, and violent extremist and terrorist material. We called for the further development and expansion of capabilities to prevent upload of illicit content, and to execute urgent and immediate takedowns. We reiterated the importance of industry investment in human and automated detection capabilities, underscoring the need for major companies to set industry standards and to help smaller companies deploy these capabilities to their platforms, including through the Global Internet Forum to Counter

Terrorism (GIFCT). And we called for increased efforts to counter foreign interference and disinformation conducted via online platforms.

6. We also undertook to enhance feedback loops between government and industry on intelligence and information, including trends and sources of illicit content, with the aim of more comprehensively responding to malicious actors online, to facilitate faster identification and removal of illicit content, and increase public awareness of the sources of disinformation and other forms of malicious foreign interference.

Countering the threat of terrorism

7. Globalised terrorist networks and violent extremists pose a real and unabating threat to our communities. Ongoing efforts to bring about the decline and depletion of terrorist networks operating in the Middle East have created new risks as many foreign terrorist fighters return to their countries of origin or move to other regions, disseminating their capabilities. We committed to the expanded sharing of information about known or suspected terrorists between our national security and border protection agencies, reiterating that the detection of international movements of terrorists and their associates relies on the rapid sharing of information between partners. We re-affirmed that alerts and intelligence relating to the movement of known and suspected terrorists will be shared between all five partners quickly and effectively. And we committed to continue our cooperation to support effective whole of government efforts to identify and—where domestic laws allow—prosecute returning foreign terrorist fighters, and share best practices for rehabilitating and reintegrating their family members.
8. Building on the framework for cooperation in United Nations Security Council Resolution 2396, we committed to work together to build the capability of other States in border security and measures to monitor, screen, track, and share information on returning foreign terrorist fighters and local terrorist networks. The aviation environment continues to be seen as a high-value target by terrorist and criminal networks. We committed to establish a new group, the 'Aviation Security 5', to better share information about emerging threats in the aviation sector and support existing fora to raise global standards for aviation security.

Cyber security and resilience of critical infrastructure

9. The increasingly digitised and networked nature of all aspects of our economies and societies means that cyber security and resilience is of the highest priority. The cyber domain is a vector for threats posed by hostile state actors, criminals, terrorist networks and hacktivists. A cyber attack *is* an attack on our communities and our sovereignty. We affirmed our collective resolve to deter malicious cyber activity, including improving domestic resilience, and coordinating technical attribution and operational response policies to mitigate significant cyber incidents. We agreed to further strengthen connectivity between our cyber watch offices to enhance shared 24/7 monitoring of hostile cyber activity.
10. We committed to work together to protect critical infrastructure and support the development of secure critical infrastructure supply chains that are advanced, affordable, reliable and trusted. We undertook to share risk assessments and certification practices on

supply chains to underpin the continued resilience of our respective cyber networks and prepare for new and emerging technologies.

Migration and border management

11. The interconnection and interdependence of our economies and communities manifests in increasing volumes of people and goods moving across borders. Facilitating the legitimate movement of people and goods is essential to our economic prosperity. The five countries are at the forefront of emerging border technologies, with a history of driving new technologies to simultaneously enhance border security and achieve faster movement of lawful travellers and goods. We committed to work together with industry to build the 'touchless' border at ports of entry for legitimate travellers and trade. We agreed to a strategy to leverage our investments in emerging technologies, including digitalisation and artificial intelligence, to improve facilitation and mitigate risks through real-time intelligence and information sharing, while protecting privacy.
12. Collectively, we are among the most generous countries on earth in terms of humanitarian aid and refugee resettlement. Given the increasing volume of irregular movements, resettlement alone will not solve the problem. We must work with government partners, international organisations, non-government organisations and the private sector to build capacity in countries of origin and their regions. We acknowledged the importance of safe and legal migration and asylum pathways, and migrants' awareness of these pathways, and reaffirmed the positive benefits that managed migration, settlement, and integration bring to our societies. We also reaffirmed our commitment to coordinated, global action to respond to large and irregular movements. We reiterated the sovereign right and responsibility of states to strong border management, consistent with international *non-refoulement* obligations, to deter and detect those who seek to evade border controls. And we reaffirmed the responsibility of all states to accept the return of their nationals, agreeing to increase cooperation to support timely and effective removals of non-citizens who have no right to remain in our countries, including consideration of joint consequences.
13. We committed to strengthen efforts to combat the scourge of modern slavery, forced labour, and human trafficking, which devastate the lives of the most vulnerable across the globe. We undertook to establish a senior officials' taskforce to develop concrete measures to tackle these problems, including promoting transparency in global supply chains, and developing common approaches to engage industry on trafficking facilitated through the internet and other digital technologies. The taskforce will report back to Ministers in the first quarter of 2019. We further agreed to consolidate and strengthen intelligence sharing, investigative, and enforcement efforts, including deploying sophisticated national capabilities to local law enforcement.
14. We re-affirmed the need to effectively manage migration flows through the utilisation of enhanced screening techniques, sharing intelligence and more effectively reaching into new sources of data, consistent with civil liberty protections, including social media, to ensure foreign nationals who would do us harm cannot cross our borders. We agreed to enhance collaboration on targeting, analysis, and disruption operations to counter organised threats to our border and national security.

Joint meeting of FCM and Quintet of Attorneys-General

15. On 29 August, we were joined by our ministerial colleagues who met as the Quintet of Attorneys-General. Together we discussed emerging issues and collaboration in countering foreign interference, the challenges posed by ubiquitous encryption, criminal information sharing and addressing the financing of transnational crime and terrorism.

Countering Foreign Interference

16. We condemned foreign interference, being the coercive, deceptive and clandestine activities of foreign governments, actors, and their proxies, to sow discord, manipulate public discourse, bias the development of policy, or disrupt markets for the purpose of undermining our nations and our allies. Foreign interference threatens a nation's sovereignty, values and national interests — it can limit or shape the polity's ability to make independent judgements, erode public confidence in our political and government institutions, and interfere with private-sector decision making. We agreed the five countries would work collectively to counter foreign interference, protect our individual sovereignty, and ensure our values and interests are upheld.
17. We agreed to draw upon the strengths of our cohesive societies, our public and private institutions, and our global partnerships to reduce the risk that foreign interference poses to domestic and global prosperity and stability. We committed to establish a mechanism for the five countries to share developments in our respective approaches to confronting the foreign interference challenge. We undertook to share information on foreign interference activities with a view to advancing our collective knowledge of how to counter such threats. In the event of a severe foreign interference incident within our sovereign nations, we agreed the five countries would coordinate on appropriate responses and attribution.

Encryption

18. Encryption is vital to the digital economy, a secure cyberspace and the protection of personal, commercial and government information. The five countries have no interest or intention to weaken encryption mechanisms. We recognise, however, that encryption, including end-to-end encryption, is also used in the conduct of terrorist and criminal activities. The inability of intelligence and law enforcement agencies to lawfully access encrypted data and communications poses challenges to law enforcement agencies' efforts to protect our communities. Therefore, we agreed to the urgent need for law enforcement to gain targeted access to data, subject to strict safeguards, legal limitations, and respective domestic consultations. We have agreed to a Statement of Principles on Access to Evidence and Encryption that sets out a framework for discussion with industry on resolving the challenges to lawful access posed by encryption, while respecting human rights and fundamental freedoms.

Criminal information sharing

19. Increasing interconnection between serious and organised crime networks have globalised threats such as drugs, cybercrime, child exploitation, and financial crimes. Reaffirming our commitment to sharing criminal and law enforcement information, we tasked our senior officials to convene an extraordinary meeting of operational and policy agencies with responsibility for law enforcement, border protection, and criminal justice. Drawing on the work of the Five Eyes Law Enforcement Group, the Border Five, and the Migration Five, the meeting will advise Ministers on the necessary enhancements to information sharing and collaboration to support more effective responses to serious criminal threats.

Beneficial ownership and illicit finance

20. We agreed to support G20 and Financial Action Task Force (FATF) efforts to combat illicit finance by increasing the transparency of legal persons and arrangements, and enabling timely access to beneficial ownership information by law enforcement agencies. We also agreed to encourage collaboration between 'five eyes' financial intelligence units to enhance the sharing of intelligence and experience. And we agreed to work closely with the private sector to promote the adequate and accurate collection of beneficial ownership information.

Conclusion

21. We affirmed today the importance of the five country partnership in addressing complex homeland and national security challenges. Our history of cooperation, our shared values, and our enduring friendship provide solid foundations to face the challenges and opportunities of the 21st century together. We are committed to building on this past cooperation and together pledge the commitments made today.