FIVE COUNTRY MINISTERIAL

Emerging Threats
London 2019

COMMUNIQUÉ

1. We, the Home Affairs, Interior, Security and Immigration Ministers of Australia, Canada, New Zealand, United Kingdom and the United States of America (the "Five Countries") have come together in London, United Kingdom on 29–30 July 2019. Guided by our shared responsibility and commitment to build a more peaceful and secure world for our citizens, we affirm our determination to promote our shared values and protect our nations from the existing and emerging security threats faced in our communities, at our borders, or in the cyber space.

Countering Online Child Sexual Exploitation and Abuse: Digital Industry Roundtable

1. In five years, we have seen a near twenty-fold increase in industry referrals of child abuse material to the National Center for Missing and Exploited Children, from 1 million in 2014 to over 18 million in 2018. Driven by the moral obligation to tackle this escalating crisis we met representatives from Facebook, Google, Microsoft, Roblox, Snap and Twitter. Together we heard from Thorn, and survivors, about the devastating and lasting impacts of child sexual exploitation and abuse, including through the continued proliferation of abusive material online long after the actual abuse ceases.
2. All participants agreed that tackling this epidemic requires an immediate upscaling of the global response to ensure that all children across the globe are protected against online sexual exploitation and abuse, and that there is no safe space online for offenders to operate.
3. We note the efforts of digital industry to develop a range of tools to combat the threat, including grooming of children online, and the work being undertaken to support uptake of these tools with

smaller companies. Whilst these are welcome steps, much more must be done at pace – every day that passes more children are being abused, exploited, and re-traumatised online. This must stop.

4. Building on the statement agreed at the 2018 Five Country Ministerial we agreed with industry representatives to collaborate to design a set of voluntary principles that will ensure online platforms and services have the systems needed to stop the viewing and sharing of child sexual abuse material, the grooming of children online, and the livestreaming of child sexual abuse and the ability to report such offences to law enforcement.
5. Today we agreed the core foundations upon which these principles will be based and we call on all digital industry representatives to engage with the Five Countries, through the Digital Industry Engagement Senior Officials Group to collaborate so these can be finalised at the end of September this year. We will be seeking early and ongoing feedback from industry on how these principles are being implemented in their day to day business.
6. Beyond this it is imperative that all sectors of the digital industry including Internet Service Providers and device manufacturers and others to continue to consider the impacts to the safety of children, including those who are at risk of exploitation, when developing their systems and services and deploying encryption.
7. We affirm our support for law enforcement and front line professionals who are bearing the burden of investigating these heinous crimes. We recognise the importance of adequate access to psychological and wellbeing support, as well as continuing to develop means to reduce their exposure to traumatic content by developing technological solutions.
8. We remain resolute in our determination to tackle this abhorrent crime, safeguard children and protect victims and survivors.

Cyber and Online Threats

1. An open, interoperable, reliable, and secure internet is fundamental to the social and economic development of communities across the globe. With it comes a responsibility to tackle the complex and evolving nature of those threats that seek to undermine its potential. We also reaffirm the norms, rules, and principles for the responsible behaviour of states in cyberspace previously endorsed by the UN General Assembly in 2013 and 2015, and commit to continue to work to see these norms strengthened and implemented.

2. It is also vital that Five Countries partners support each other in ensuring coordinated and efficient responses to cyber threats, including incidents at a national and international level, and against different types of victims. We commit to continue to develop and share learning on cyber threats and responses in order to facilitate a collective improvement in both understanding and response capability across the Five Countries.
3. The nature of 5G, whilst bringing unparalleled opportunity, will increase the risks to the integrity of our telecommunications networks. The Five Countries have each individually undertaken or are undertaking substantial reviews of the security risks to 5G networks. There is agreement between the Five Countries of the need to ensure supply chains are trusted and reliable to protect our networks from unauthorised access or interference. We recognise the need for a rigorous risk-based evaluation of a range of factors which may include, but not be limited to, control by foreign governments. We also recognise the need for evidence-based risk assessment to support the implementation of agreed-upon principles for setting international standards for securing cyber networks**.**

Emerging Technologies

1. Emerging technology reflects the growth of increasingly autonomous, intelligent, and connected devices that blur the distinctions between the physical and digital worlds. We recognise the importance of protecting our citizens and economies from threats whilst empowering them to engage with new technology. The security of the Internet of Things (IoT) is a critical issue that requires international cooperation and harmonisation of standards to achieve the required effect across diverse markets.
2. It is essential that nations and their people can trust the technology that will underpin their societies now and in the future. Emerging technologies bring a range of opportunities and challenges, including for our approaches to cyber security. We recognise the importance of open, diverse, competitive, and trusted critical technology markets, where security-by-design is a fundamental principle. Our nations signed a joint Statement of Intent, which will align our approaches to enhancing the security of the Internet of Things devices, to provide better protection to users by advocating that devices should be secure by design. The Statement will encourage our nations to actively seek out opportunities to enhance

trust and raise awareness of best practices associated with IoT devices and reaffirms the need to identify and engage likeminded nations to encourage international alignment on IoT security. We welcome complementary international efforts to improve the security of critical and emerging technologies.

3. In recent years unmanned aircraft systems, often referred to as 'drones', have rapidly evolved in terms of capability, availability, and uptake for commercial and recreational use. Drone technology has the potential to offer significant benefits to economies and quality of life. However, the malicious, unlawful, or inadvertent misuse of drones and the data they collect can pose a risk to public safety, be deliberately used to facilitate or commit a wide range of criminal acts, and also present a threat to our national security. We commit to create a stronger Five Country approach to drones informed through co-ordinated and in-depth information sharing around threat, vulnerabilities, and counter-drone technology. We will also enable the Five Country security community to identify what more could be done at the manufacturing stage to mitigate drone risk by design. Work to commence this will begin immediately and the UK will host a Five Country event at the Home Office Security and Policing Event in March 2020 to enhance cooperation.

Borders and Asylum

1. Facilitating the legitimate movement of people across our borders is essential to our economic prosperity. We acknowledge the importance of safe and regular immigration, protecting refugees, and delivering timely protection to those making genuine asylum claims. We reaffirm the positive benefits that managed immigration, settlement, and integration brings to our societies.

2. We recognise the need to modernise border security systems to deal with evolving threats. We therefore commit to pursue expanded data sharing prior to and at the border to facilitate the secure movement of legitimate travellers and goods and in ways that maintain privacy, data security, and are consistent with domestic law.

3. We reiterate the sovereign right of states to strong border management, including the responsibility to deter, prevent, detect,

and disrupt those who seek to evade or facilitate the evasion of border controls. We also recognise that our ability to deliver timely protection to those genuinely fleeing persecution is hampered by those who abuse or facilitate the abuse of our border and immigration systems, including our asylum systems. We therefore commit to increase our collaboration regarding such activity. We commit to explore enhancing cross-border information sharing on, but not limited to, travelling child sex-offenders, in line with domestic legislation. We further reiterate our commitment to work together and with global partners to secure the efficient removal of individuals without lawful status in our countries.

Countering Foreign Interference - Election Security and Strengthening Democracy

1. Building on last year's commitment to establish a mechanism to share approaches to combating 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— our countries have shared strategies that protect our electoral institutions and democratic processes from foreign interference and other hostile state activity. We commit to maintaining these efforts, and will continue our collaboration to combat foreign interference in other areas such as the economy and academia.