Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BRIEFING NOTE FOR THE MINISTER

ENCRYPTION

Strategic Objectives

- Reassert Canada's unwavering support to finding common solutions with Five Eyes partners
- Exchange perspectives on the effectiveness of different laws and policies
- Confirm Canada's active engagement to safeguard encryption and mitigate its challenges in collaboration with industry.
- Emphasize the importance for the Five Country Ministerial to make clear that we do not seek to undermine the security of communications services or restrict the spread of in-demand encryption technologies, in accordance with last year's public statement.

Key Messages

Encryption

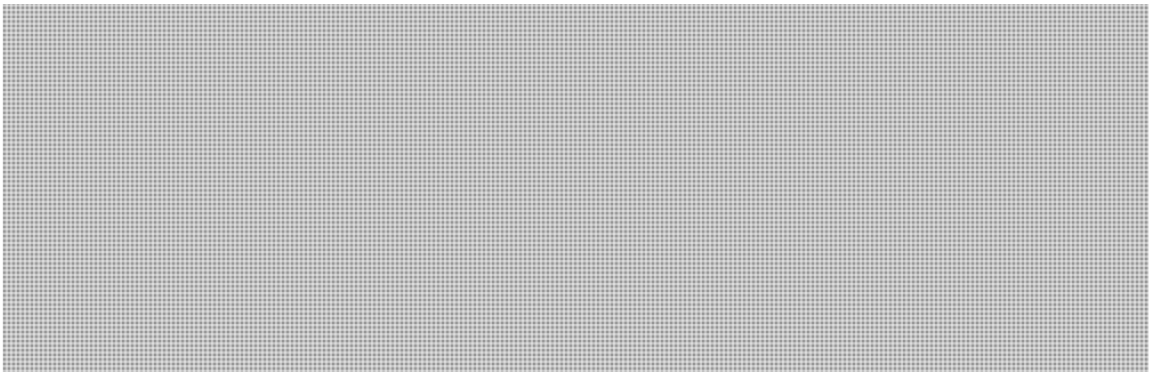
Safeguarding Encryption and Gaining Public Support

- it is also in Canada's interest that encryption technologies remain robust and widely-used in order to safeguard cybersecurity and the digital economy.

- Further action on encryption in Canada will only be possible to the extent that we can reassure Canadians that we do not intend to undermine the security of the communications products and services that they use.

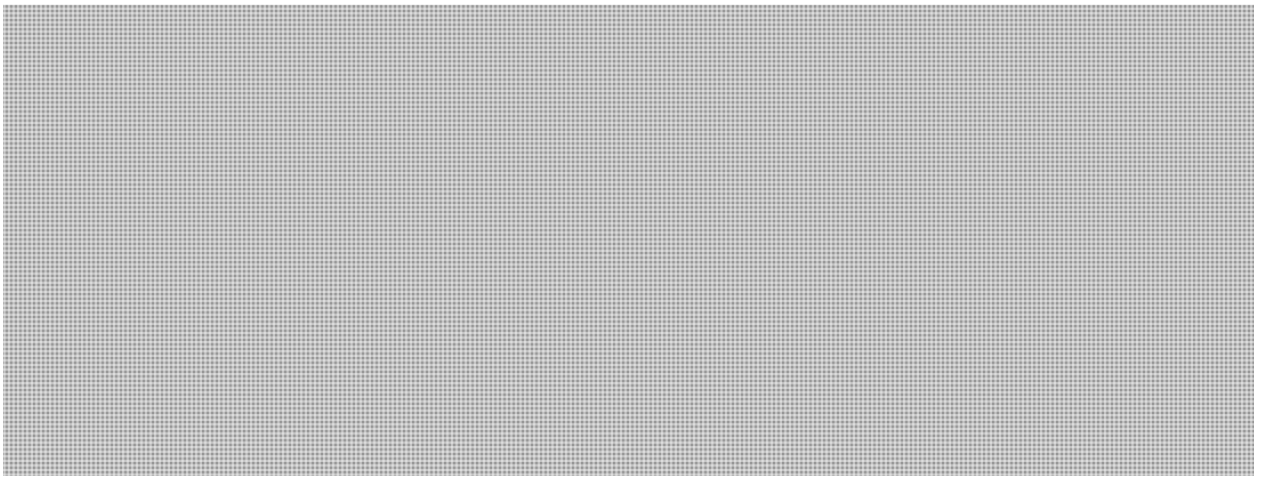
Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Way Forward

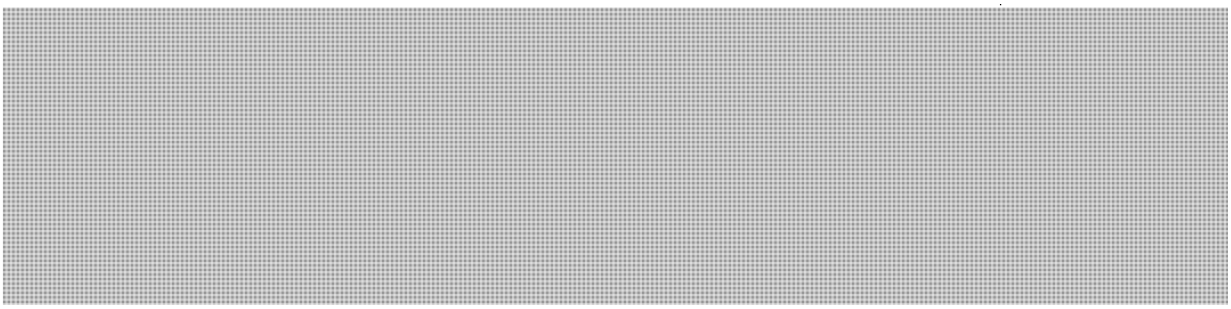


- Canada is supportive of deepening collaboration between investigative agencies and service providers. Our priority is building stronger relationships with industry. We believe that progress can be made if governments are kept informed when decisions regarding new products and services are made.

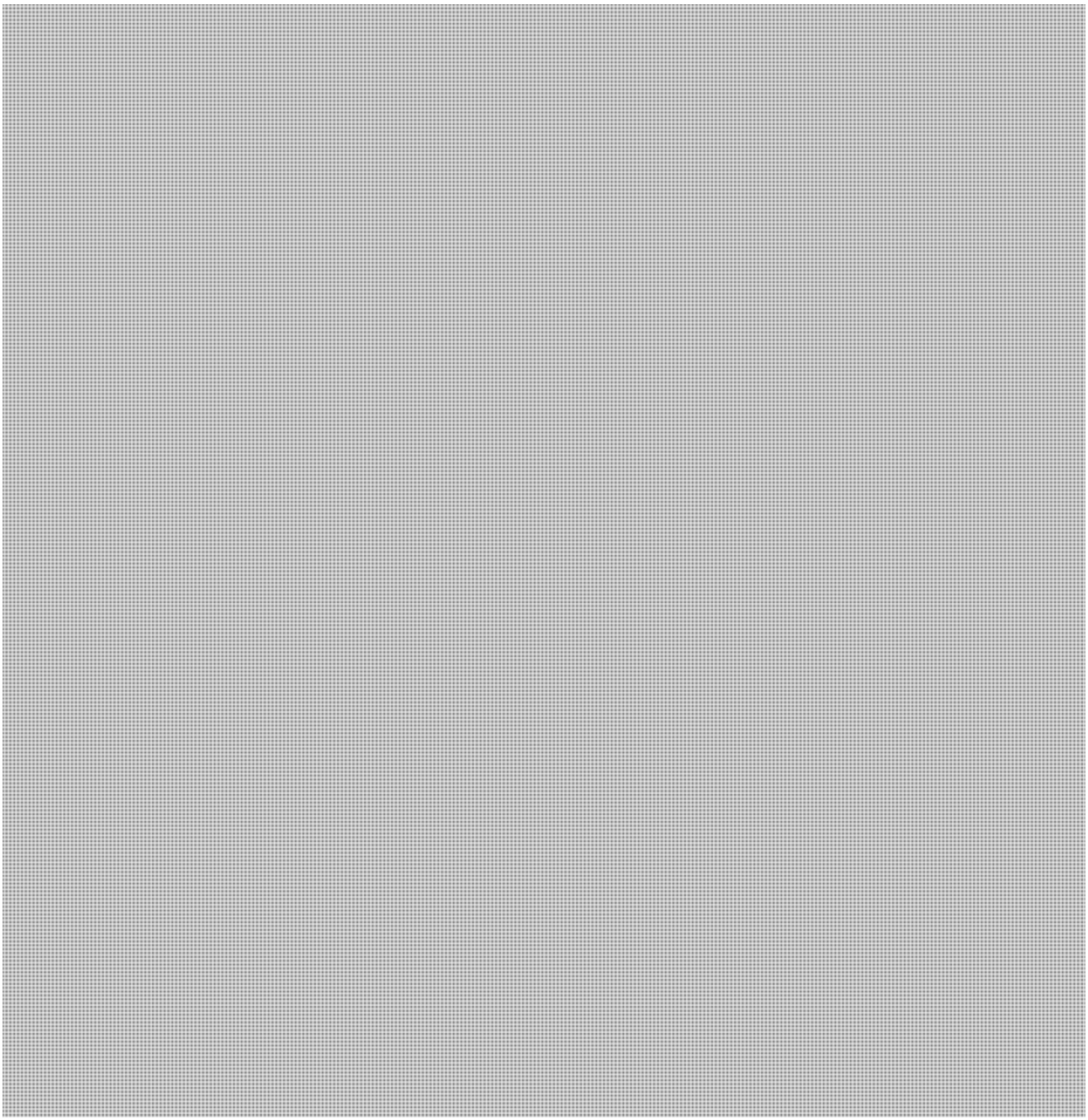
- We believe investigators would have more success in seeking communication service providers' assistance if governments affirm that we do not seek to undermine the security of communications services or restrict the spread of in-demand encryption technologies.



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



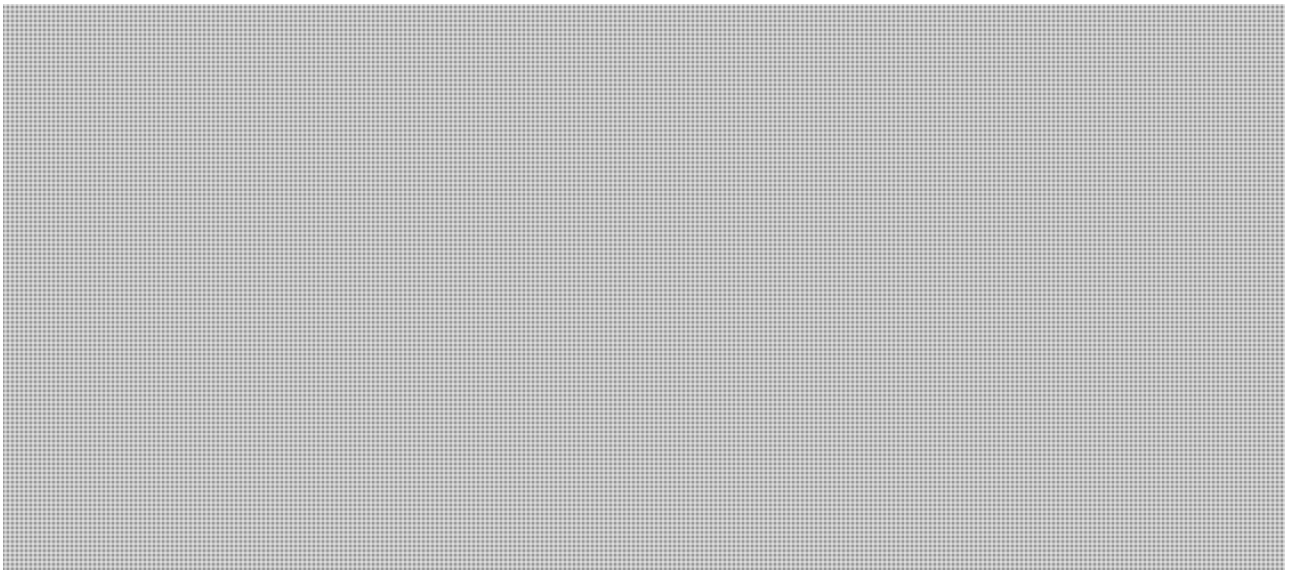
Threat assessment



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

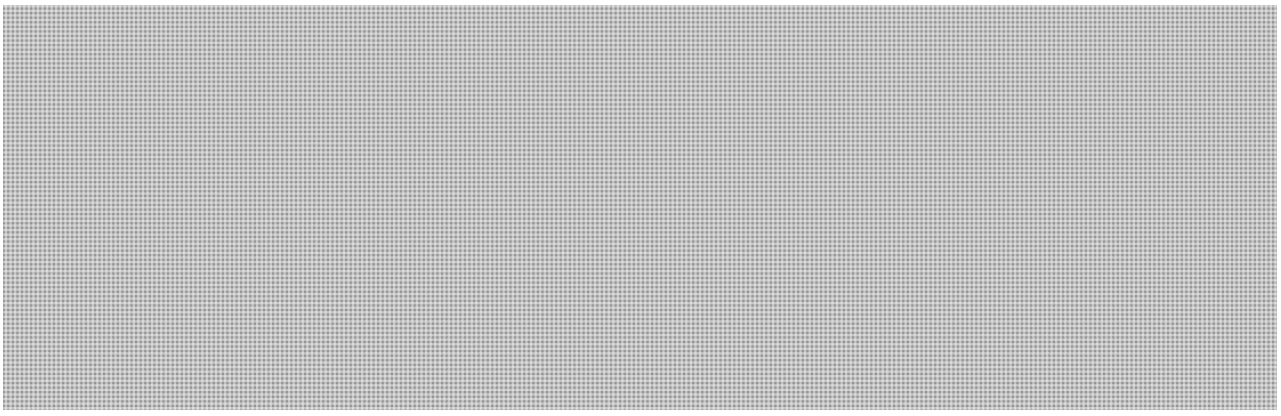
Bilateral engagement

- We are fully in support of coordination among the Five Eyes to find solutions and strategies in approaching the private sector as a united group to discuss how they can support us in light of the diminishing access to the content of communications.



- While we should have a dialogue with the company on the impact of end-to-end encryption on public safety, we should keep in mind that it is a valid and understandable decision for a company to make.

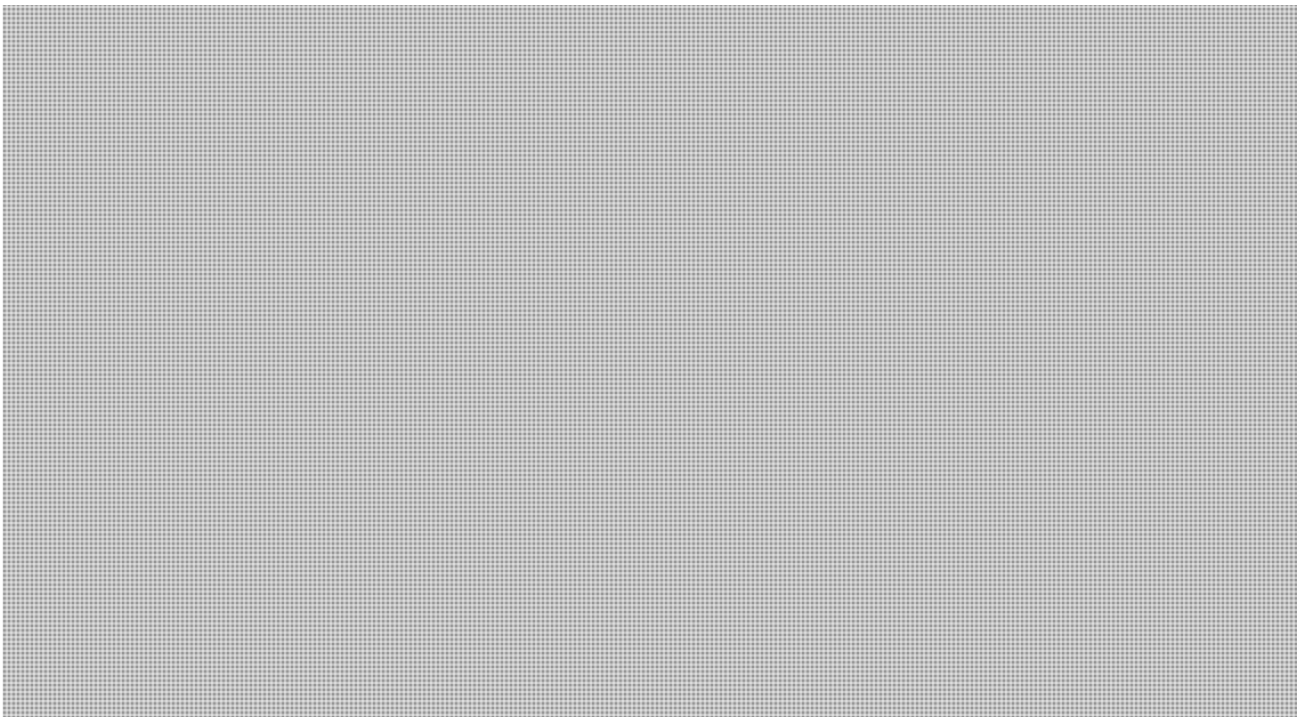
Influence on the decision



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Any convincing alternatives that we propose will need to take into consideration the perception of the public as this may be an essential factor.

- We believe it may be more fruitful to focus on the difficulties for law enforcement and on possible solutions, while avoiding branding end-to-end encryption itself as a threat or a negative development.



Privacy and Digital Charter

- As we go forward with consulting the industry on encryption, we should keep in mind the competing pressure on tech companies as to their privacy protections. For instance, Canada's government has recently released a Digital Charter, that underlines the importance of privacy, and Canada's Privacy Commissioner is currently engaged in litigation with

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Facebook in relation to the need for enhancing privacy protection.

- The launch of the Digital Charter was accompanied by a set of proposals to modernize the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's federal private sector privacy legislation. The Charter's principles provide a set of shared national priorities where citizens have confidence that their data and privacy is protected.

- Notably, the Digital Charter enshrine the principle that Canadians will have control over what data they are sharing, who is using their personal data, and for what purposes, and know that their privacy is protected.

- Going forward, privacy and cybersecurity will increasingly be key concerns for the public as the volume of sensitive and personal data stored online and in electronic devices rises.

Background

2018 Statement of Principles on Access to Evidence and Encryption

As part of last year Five Country Ministerial meeting, the Five Eyes released a Statement of Principles on Access to Evidence and Encryption. The statement stressed the importance of encryption to cybersecurity, [redacted] The need to cooperate with providers of information and communications technology and services was emphasised. Finally, the statement underscored the importance of the rule of law and due process, as well as the freedom of choice for Five Eyes countries to address encryption as they see fit.

The Statement of Principles garnered some media attention, and some criticism. The particular focus of criticism and comments was on what was characterized as a threat made by the five Governments; which was that if service providers did not voluntarily assist in providing

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

unencrypted data, that Governments retain the right to proposed "technological, enforcement, legislative or other measures to achieve lawful access solutions".

Facebook privacy first platform

Earlier this year, Mark Zuckerberg announced proposals to make Facebook a "privacy first platform", principally by moving their three core messaging services (Facebook Messenger, Instagram Direct Messaging and WhatsApp) to a single, end-to-end encrypted environment. The justification for doing so has been built on an analogy that Facebook has enabled people to connect in the "digital equivalent of a town square" but that users increasingly want to be connected privately in the "digital equivalent of a living room". As part of their announcement, Facebook committed to engage Governments on these proposals to discuss how to maintain user safety across their platform.

Existing end-to-end encrypted messenger programs such as WhatsApp or Telegram are already widely exploited by offenders to commit online child sexual exploitation offences, such as luring and grooming children or distributing child sexual exploitation material, in virtual anonymity. This would undoubtedly be magnified with the multi-billion users on Facebook and Instagram messenger platforms, which contrary to the aforementioned programs, are heavily used by youth.

Existing Solution

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Public debate and stakeholders' engagement

While CSPs are receptive to engaging on encryption, they have strongly opposed attempts by governments to mandate access to encrypted data in ways that would undermine the security of their products or jeopardize the trust of their users. When faced with coercive government actions, CSPs have not hesitated to challenge them in court. For example, the associations representing major US CSPs filed amicus briefs in support of Apple during 2016 litigation over access to a dead terrorist's encrypted iPhone. Given the importance of protection of cybersecurity, these concerns would need to be fully addressed by any government policy that attempts to assist law enforcement with the challenge of encryption, both from a substantive perspective, and from a communications perspective.

Another challenge in this respect is that even if the requirements imposed do not in fact inherently weaken the protection provided by encryption, concerns regarding this possibility will likely continue to strongly influence the views of the public and stakeholders, and raise significant privacy concerns.

Drafted: NCSB/NSPD [redacted]
Consulted: RCMP/CSIS/Justice
Approved by: NCSB/NSPD/Davies

Pages 9 to / à 14

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FOR OFFICIAL USE ONLY

FIVE COUNTRY
MINISTERIAL

Emerging Threats
London 2019

DRAFT COMMUNIQUÉ

1. We, the Home Affairs, Interior Security and Immigration Ministers of [redacted] 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 existing and emerging security threats whether faced in our communities, at our borders, or in the cyber space.

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 [redacted] previously endorsed by the UN General Assembly in 2013 and 2015, and commit to continue to work to see these norms strengthened and implemented. [redacted]
2. It is also vital that [redacted] 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 also increase the potential risks to the integrity of our telecommunications networks. [redacted] There is agreement between the [redacted] of the need to ensure supply chains are trusted and reliable to protect our networks from unauthorised access or interference. [redacted]

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 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 [redacted] 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.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The Statement will [redacted] our nations to actively seek out opportunities to enhance trust and raise awareness of best practice 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 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 [redacted] approach to drones informed through co-ordinated and in-depth information sharing around threat, vulnerabilities and counter-drone technology. We will also enable the [redacted] 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 [redacted] 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 and protecting refugees and those seeking asylum and 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 on travellers prior to and at the border to facilitate the secure movement of legitimate 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 [redacted] 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. [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Countering Online Child Sexual Exploitation and Abuse: Digital Industry Roundtable

[redacted]

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. We commit to support more effective prevention, disruption and investigative responses to this [redacted]
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. [redacted] 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.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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 [redacted], 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: [redacted]
    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

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

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. [redacted] 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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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 [redacted] on managing residual risk.

[redacted]

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. [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FOR OFFICIAL USE ONLY

FIVE COUNTRY
MINISTERIAL

Emerging Threats
London 2019

DRAFT 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") ~~nations~~ 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 existing and emerging security threats whether faced in our communities, at our borders, or in the cyber space.

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 also 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

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 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 a joint Statement of

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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 practice 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 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.

Formatted: Font: (Default) Arial

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 and protecting refugees and those seeking asylum and 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 on travellers prior to and at the border to facilitate the secure movement of legitimate 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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

commit to maintaining these efforts, and will continue our collaboration to combat foreign interference in other areas such as the economy and academia.

Countering Online Child Sexual Exploitation and Abuse: Digital Industry Roundtable

[redacted]

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. We commit to support more effective prevention, disruption and investigative responses to this [redacted]
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.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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 [redacted] 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

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

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. [redacted]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 [redacted]-Five Countries [redacted]on managing residual risk.

   - [redacted]

Conclusion

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

1. We reaffirm today the critical importance of the Fi~~-five~~ Ceountry 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.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FIVE COUNTRY
MINISTERIAL

Emerging Threats
London 2019

DRAFT COMMUNIQUÉ

1. We, the Home Affairs, Interior Security and Immigration Ministers of [redacted] 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 existing and emerging security threats whether faced in our communities, at our borders, or in the cyber space.

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 [redacted] 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 also increase the [redacted] risks to the integrity of our telecommunications networks. [redacted] There is agreement between the [redacted] of the need to ensure supply chains are trusted and reliable to protect our networks from unauthorised access or interference. [redacted]

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 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 [redacted] 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 [redacted] our nations to actively seek out opportunities to enhance trust and raise

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

awareness of best practice 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 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 [redacted] approach to drones informed through co-ordinated and in-depth information sharing around threat, vulnerabilities and counter-drone technology. We will also enable the [redacted] 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 [redacted] 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 and protecting refugees and those seeking asylum and 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 on travellers prior to and at the border to facilitate the secure movement of legitimate goods and in ways that maintain privacy, data security, and are consistent with domestic law.

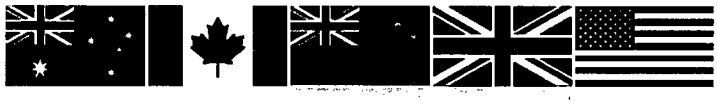
3. We reiterate the sovereign right of states to strong border management, including the responsibility to deter, prevent, detect and disrupt those who seek to evade or facilitate the evasion of border controls. We also recognise that our ability to deliver timely protection to those genuinely fleeing 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 [redacted] 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.

Countering Online Child Sexual Exploitation and Abuse: Digital Industry Roundtable

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



[redacted]

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. We commit to support more effective prevention, disruption and investigative responses to this [redacted]
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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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 [redacted] 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

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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. [redacted] 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 [redacted] on managing residual risk.

[redacted]

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.

Pages 32 to / à 35

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FOR OFFICIAL USE ONLY

FIVE COUNTRY
MINISTERIAL

Emerging Threats
London 2019

DRAFT 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 existing and emerging security threats whether faced in our communities, at our borders, or in the cyber space.

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 also increase the ~~potential~~ 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.

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 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 a joint Statement of

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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 practice 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 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.

Formatted: Font: (Default) Arial

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 and protecting refugees and those seeking asylum and 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 on travellers prior to and at the border to facilitate the secure movement of legitimate 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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

commit to maintaining these efforts, and will continue our collaboration to combat foreign interference in other areas such as the economy and academia.

Countering Online Child Sexual Exploitation and Abuse: Digital Industry Roundtable

[redacted]

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. We commit to support more effective prevention, disruption and investigative responses to this [redacted]
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.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

1. We reaffirm today the critical importance of the Fi~~-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.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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, 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. In particular, encryption must not be allowed to conceal or facilitate the exploitation of children.
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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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:

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- 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.

Pages 51 to / à 56

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Report: FCM 2019 – Bilateral meeting: U.S. AG William Barr

The FCM provided an opportunity for a first bilateral meeting between Minister Goodale and Attorney General Barr.

Report:

[redacted]

Report: FCM 2019- Bilateral meeting: U.S. A/Deputy Secretary DHS David Pekoske

Ministers Goodale and Hussen held a joint bilat with U.S. A/Deputy Secretary of Homeland Security David Pekoske, who was serving as the head of the U.S. delegation for the FCM.

Report:

Terror Listings: Minister Goodale noted that Canada was adding 3 organizations to our list of terrorist entities including two right wing extremist groups [redacted]

Irregular Migration: [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Minister Hussen reiterated Canada's desire to move forward with modernizing the Safe Third Country Agreement (STCA).

- **Guatemala STCA**: Minister Hussen also sought clarity with regard to the recent US announcement of an STCA with Guatemala.

VETUI: Pekoske had attended the Global Internet Forum to Counter Terrorism Summit the previous week.

5G: Minister Goodale asked about the evolving U.S. position on 5G.

Aviation security/ICAO:

Minister Goodale indicated that officials would follow-up with Transport Canada, who has the lead on this matter.

Report: FCM 2019- Bilateral meeting: UK Home Secretary Priti Patel

This was Minister Goodale's first opportunity for a bilateral meeting with Secretary Patel.

Report:

Online Harms: Minister Patel highlighted online harms as a key issue. Minister Goodale called for tech companies to be quicker in taking down content, provide more transparency about algorithms, and to assist smaller companies. He also noted work on online child sexual

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

exploitation in Canada (C3P, Arachnid)

Terror Listings: Minister Goodale enquired about a potential terrorist organization listing. He and the Home Secretary agreed that officials would follow-up to discuss this issue further.

Report: FCM 2019- Bilateral meeting: New Zealand Minister Of Justice Andrew Little

The bilateral meeting between Ministers Goodale and Little focused largely on the Christchurch Call follow-up.

Report:

Terror Listings: Minister Goodale spoke about Canada's decisions to add two right wing extremist groups to our list of terrorist entities. He also discussed a potential terrorist organization listing.

VETUI: Minister Goodale noted Canada's intent to host a youth summit on countering violent extremism online

Report: FCM 2019- Bilateral meeting: Australia Minister of Home Affairs Peter Dutton

Ministers Goodale and Dutton had a short bilateral meeting following the close of the joint FCM-Quintet meeting.

Terror Listing: Minister Goodale raised the potential terrorist listing issue noted in other bilateral meetings

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BILATERAL MEETING WITH
WILLIAM BARR, U.S. ATTORNEY GENERAL

Strategic Objectives

- Highlight the strong relationship and cooperation between Canadian and American law enforcement agencies, and issues of common interest, such as combatting opioids, cybercrime (notably telemarketing and elder fraud) and information sharing [redacted]
- Respond to inquiries about Canada's approach to foreign terrorist fighters and battlefield evidence; as well as encryption.

Key Messages

Law Enforcement Cooperation

- We share common responsibilities regarding domestic law enforcement agencies, and priorities such as opioids and cybercrimes in the field of national security and public safety.
- There are many examples of successful law enforcement cooperation to date, notably between Canadian agencies, the FBI, ATF, and DEA, including:

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Opioids

- There is a common challenge of the opioid crisis and rising problem of methamphetamines on both sides of the border.
- Bill C-37, passed in May 2017, provided new measures to better equip law enforcement and health officials to reduce harms linked to drug and substance use.
  - Notably, it provided the authority to border officers to open packages weighing 30 grams or less, and to take action to prevent the uncontrolled import into Canada of devices that can be used to manufacture illicit drugs.
- Prime Minister Trudeau and President Trump agreed in June to work to develop joint actions.

[redacted] the successful trilateral cooperation under the North American Drug Dialogue.

- China remains the main source of opioids entering Canada [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- What are your views on the main law enforcement challenges related to opioids and are there lessons learned you would share about U.S. efforts?

Information Sharing

- There are robust, collaborative relationships between Canadian security and intelligence communities and their American counterparts.

- Canada is committed to timely information sharing with partners regarding national security threats that impact our countries and shared border – in a manner that protects the rights and privacy of Canadians.

Telemarketing and Elder Fraud

-

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

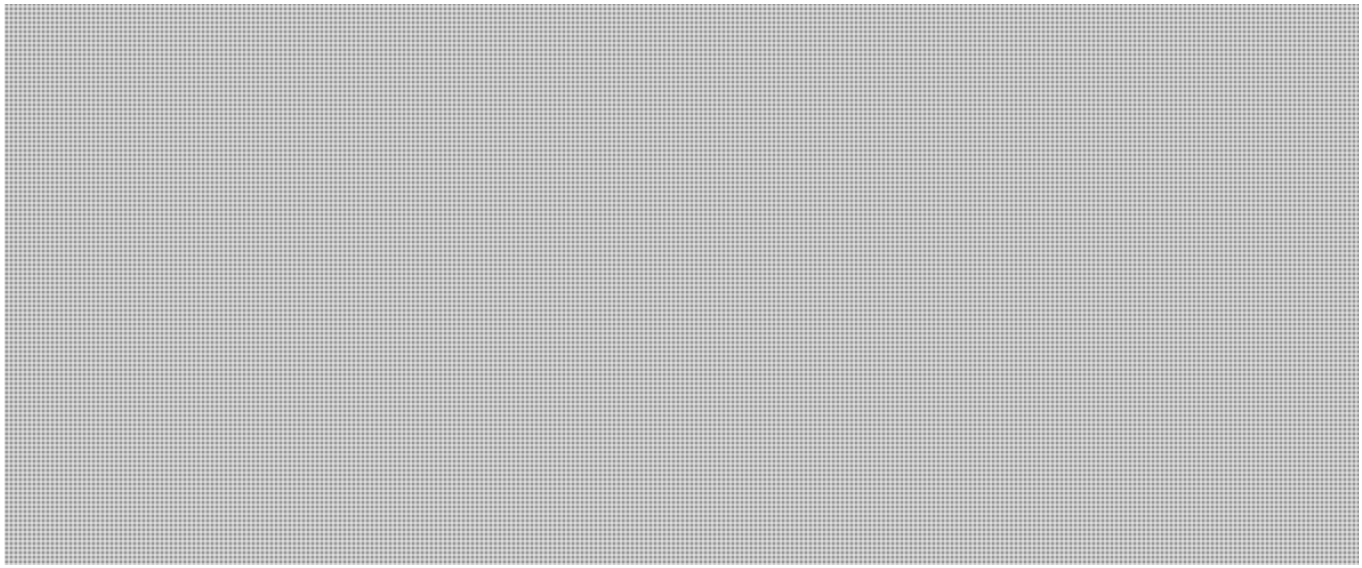
- There are partnerships with the provinces and industry that the Government has invested in to combat these types of crimes and support and educate vulnerable populations such as:
  - The RCMP hosted a national mass marketing fraud strategy meeting in May 2018, with local, provincial, and international policing partners, including U.S. Postal Inspection Service and Federal Trade Commission.
  - The RCMP supported the recent U.S. Department of Justice elder fraud initiative through the International Mass Marketing Fraud Working Group, where the RCMP played a key role in tackling the India Call Centre Fraud.
  - The work carried out by the Canadian Anti-Fraud Centre, which serves as a model around the world, including Canada's Fraud Prevention Forum and Fraud Prevention Month, and continuous efforts to support investigations.

Responsive

Foreign Terrorist Fighters and Battlefield Evidence

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Canada takes the threats posed by foreign terrorist fighters seriously and is actively pursuing a whole-of-government approach to monitor and respond to this threat.
  - Criminal prosecution is a top priority and the preferred course of action.



  - Information must be collected, handled, and processed to satisfy the admissibility requirements for legal evidence, and ensure that post-collection chains of custody adhere to the highest evidentiary standards.

Encryption

- Canada is acutely aware of the difficulties for law enforcement agencies as a result of the widespread adoption of encryption, but the public narrative is very much in favor of an increasing the use of encryption.
- The Five Country Ministerial should make clear that we do not seek to undermine the security of communications services or restrict the spread of in-demand encryption technologies, in accordance with past public statements.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Background

This will be your first meeting with Attorney General (AG) William Barr. It will be an opportunity for you to highlight the strong relationship between law enforcement organisations, and discuss a few common priorities (opioids, [redacted] and combating mass marketing fraud targeted at the elderly).

On June 26, Justice Minister Lametti had his first meeting with the AG and discussed many of the same issues, including [redacted] elder fraud, opioids and battlefield evidence. Given the overlap of topics, Justice Canada's Associate Deputy Minister François Daigle and Assistant Deputy Minister Elisabeth Eid will also be participating in this meeting.

Areas of overlap between the U.S. Department of Justice (DoJ)'s portfolio and that of Public Safety Canada (PS) includes: the FBI and its Terrorism Screening Center (TSC); the DEA; the ATF; United States Marshals Service, and the Bureau of Prisons. There is successful operational cooperation across the PS Portfolio with these agencies to ensure border integrity, cooperate collaborate on law enforcement investigations, and identify threats early.

Existing Law Enforcement Cooperation

[redacted]

Opioids

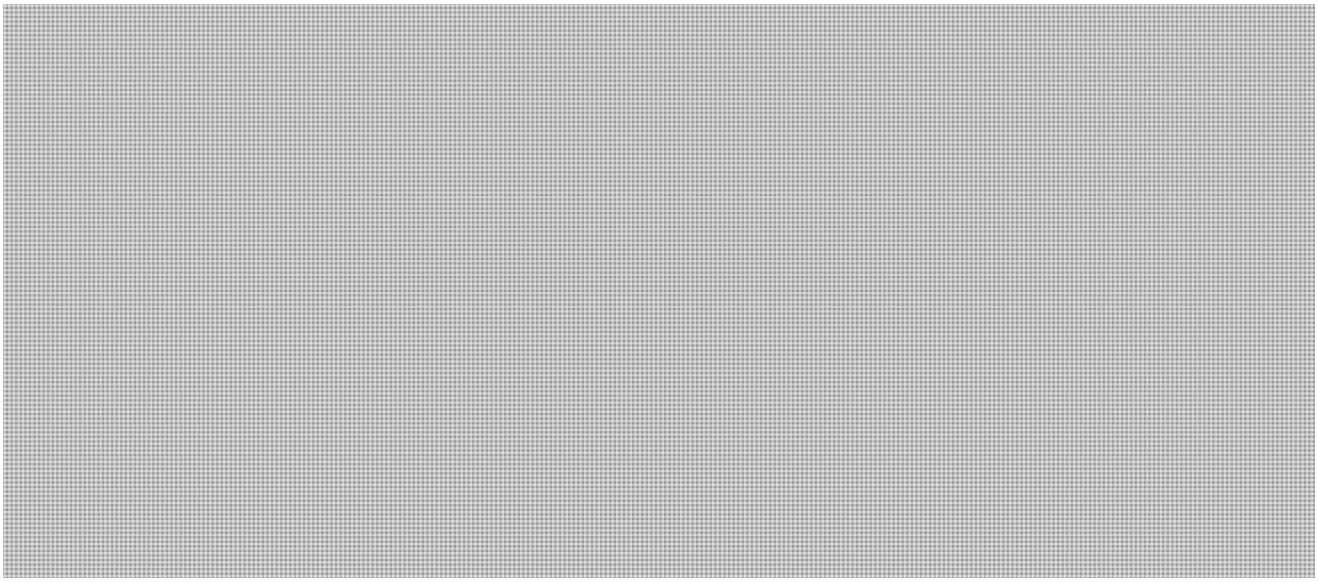
In early 2017, in order to reduce the supply of opioid and related organized crime activities, the RCMP, CBSA and Canada Post Corporation formed the Organized Crime Joint Operations Centre, which provides tactical support to opioids-related investigations by collecting, analyzing and sharing information and intelligence in relations to opioid importation, production and trafficking. This collaboration has led to investigations and arrests of opioid traffickers in Ontario, Quebec, Manitoba and British Columbia.

Canada-U.S. law enforcement cooperation is key in combatting the opioid crisis. For instance, the RCMP and DEA's continued partnership has resulted in the takedown of five different drug vendors operating on the dark web. In the past four months alone, the DEA has seized multi-kilo shipments of fentanyl, heroin, and cocaine in north eastern states. These seizures point to larger

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

and more sophisticated operations, potentially indicating the growing involvement of Mexican cartels in the trafficking of opioids to North America.

On June 20, the Prime Minister and President committed to develop an action plan to address the opioid crisis, through enhanced law enforcement cooperation, sharing of information and best practices. These efforts will include the trilateral work being done with Mexico under the auspices of the North American Drug Policy Dialogue (NADD), such as discussions of ways to improve data collection and sharing on drug seizures, smuggling, and illicit financing and money laundering. Canada hosted the NADD in Ottawa last November, and the U.S. is set to host the next meeting in D.C. in December. Through the NADD, the RCMP developed the second Trilateral Opioids Threat Assessment in partnership with the DEA and Mexico's Criminal Investigation Agency on National Drug Policy, which also noted the rise of Mexican cartels in the illicit fentanyl trade.



Telemarketing and Elder Fraud

In Canada, mass marketing fraud is considered a local police matter although most cases are national and international in scope. Jurisdictional issues pose significant challenges to the investigation and prosecution, as most cases can involve evidence in at least three different countries. The RCMP works with local law enforcement partners in Canada and foreign partners through the International Mass-Marketing Fraud Working Group, including the U.S., Belgium, Europol, the Netherlands, Norway, Spain and the UK.

Federally, telemarketing fraud is headed by the Canadian Anti-Fraud Centre (CAFC) which collects information and criminal intelligence on mass marketing fraud, advanced fee fraud, Internet fraud and identification theft complaints. The Centre is jointly managed by the RCMP, the Competition Bureau and the Ontario Provincial Police. The RCMP leads day-to-day operations. The CAFC manages more than 300,000 calls and 60,000 online fraud reports from Canadians and others world-wide annually, generating more than 70,000 complaints each year. CAFC's Senior Support Unit also offers support and advice to senior victims.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The Trump Administration has made the investigation and prosecution of telemarketing and elder fraud a priority. In March, the U.S. announced the largest nationwide sweep of elder fraud cases in history, involving more than 260 defendants from all parts of the world. In June, the AG established a Transnational Elder Fraud Strike Force, which focuses on investigating and prosecuting individuals and entities associated with foreign fraud schemes affecting American seniors.

Responsive

Foreign Terrorist Fighters (FTFs) and Battlefield Evidence

In September 2017, the U.S. Department of State (DOS), Department of Defense (DOD) and U.S. DoJ launched a battlefield evidence initiative to assist partner nations in using battlefield evidence effectively in civilian criminal justice proceedings. Based on the key issues and themes highlighted during the the interagency working group discussions, DOS, U.S. DoJ, and DOD collectively developed fourteen non-binding guiding principles.

Other like-minded countries like Denmark and the Netherlands have also had some success.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Encryption

The U.S. is renewing its push to have technology companies help law enforcement break encryption. On July 23, at a cybersecurity conference hosted by the FBI and Fordham University in New York, the AG noted that companies may soon be required to act to respond to a "dangerous and unacceptable" status quo, The FBI Director will echo concerns about "the damage being inflicted" by the use of encryption, when he speaks at the conference on Thursday. Should the AG raise this issue, you may wish to note Canada's approach.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

MEETING WITH PRITI PATEL
HOME SECRETARY OF THE UNITED KINGDOM

Strategic Objectives

- [redacted]
- [redacted]
- Register the Canadian approach to the issue of encryption with the Home Secretary.
- Strengthen Canada's cooperation with the UK against hostile state activities.
- [redacted]

Key Messages

Preventing Violent Extremism, including Right Wing Extremism

- Advise the Home Secretary about Canada's addition of Blood & Honour and Combat 18 to the *Criminal Code* list of terrorist entities.
- Highlight Canada and the UK's continued efforts to prevent and counter violent extremism, including online.

Broader Online Harms (including Terrorist Use of the Internet and Child Sexual Exploitation)

Relationship with technology companies

- [redacted]
- Reiterate that technology companies should continue to be called upon to improve transparency and engagement with governments, including law enforcement.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Seek the Home Secretary's view on reforming the Global Internet Forum to Counter Terrorism.

Child Sexual Exploitation and Abuse

- Underscore that Canada's Project Arachnid is being supported by the UK Home Office and allows for unprecedented collaboration between Canada and the UK in identifying child sexual exploitation images for removal from the Internet.

- Emphasize that the Canadian Centre for Child Protection is a non-governmental organization and a key partner under Canada's strategy to combatting child sexual exploitation online,

Encryption

- Stress that Canada is acutely aware of the difficulties for law enforcement agencies as a result of the widespread adoption of encryption, but that the public narrative on this issue is very much in favor of an increasing the use of encryption.

- Ask how the UK is progressing in terms of strengthening the public narrative on this sensitive issue. Seek insight from the UK active engagement in the public debate on encryption and with stakeholders from the industry.

- Emphasize the importance for the Five Country Ministerial to make clear that we do not seek to undermine the security of communications services or restrict the spread of in-demand encryption technologies, in accordance with past public statements.

- Highlight that Canada supports deepening the partnership between investigative agencies and service providers and building stronger relationships with industry, in the belief that progress can be made if governments are kept informed when decisions regarding new products and services are made.

Hostile State Activities

- Note that Canada is implementing new measures aimed at safeguarding our democratic process against foreign interference in anticipation of the fall

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

general election, and seek to learn more about the UK's approach and the best practices they have adopted.

Foreign Terrorist Fighters

- Stress that Canada is pursuing a whole-of-government approach to monitor and respond to this threat. Criminal prosecution is a top priority and the preferred course of action.

- Emphasize the importance of the Five Country Ministerial presenting a unified vision for managing and mitigating the threat posed by foreign terrorist fighters to ensure the safety of each respective country's citizens, while upholding democratic values and human rights obligations.

- [redacted]

Terrorist Listing

- Share information on Canada's intent to add an additional entity to its *Criminal Code* list of terrorist entities, potentially in concert with the UK.

Background

This is your first meeting with Secretary Patel. You had a bilateral meeting with former Home Secretary Javid in April 2019 at the G7 Interior Ministers' meeting in Paris. You discussed violent right-wing extremist (RWE) groups, including the inclusion in 2016 of a racist neo-Nazi group on the UK's list of proscribed terrorist organizations. You also exchanged perspectives on the potential regulation of digital industry, with Secretary Javid outlining the UK's White Paper on Online Harms [redacted]

You will be meeting Secretary Patel together with Minister Hussen, who plans to ask about irregular migration, the Global refugee sponsorship initiative and settlement and integration in the UK.

Violent Right-Wing Extremism (RWE) and Violent Extremist and Terrorist Use of the Internet (VETUI)

On June 26, Canada published an update to the *Criminal Code* list of terrorist entities that included, for the first time, two RWE groups with a presence in Canada: Blood & Honour (B&H), and Combat 18 (C18). Both groups were founded in the UK.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Canada and the UK both recently participated in the Christchurch Call to Action Summit on May 15, 2019, hosted by New Zealand Prime Minister Ardern and French President Macron.

Canada and the UK also recently joined the G20 Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism. It encourages digital industry to bolster their efforts to prevent and counter VETUI, as well as preserve content for evidentiary purposes. It also encourages reform and expansion of the Global Internet Forum to Counter Terrorism (GIFCT, led by Facebook, Google, Microsoft and Twitter).

Broader Online Harms

The UK is taking a broad online harms approach to combatting VETUI, child sexual exploitation and abuse (CSEA) and foreign interference and disinformation. The Cabinet Office's National Security Secretariat provides an internal coordination function for all content policy. The Home Office is still responsible for online counterterrorism.

In April 2019, the UK government released an Online Harms White Paper as a precursor to bringing forward online safety legislation to address terrorist use of the internet, CSEA online, disinformation, gang culture and violence, and bullying and psychological abuse. The White Paper recommends reinforcing the role of technology in the development of solutions, building a global coalition of countries, and renewing public confidence in technology companies. It also proposes the development of a new regulatory framework for digital industry based on a "duty of care", as well as the development of a new independent regulator to enforce this framework. The Government Response to the White Paper is expected to be tabled in fall 2019.

The Canada Centre is attending the upcoming annual GIFCT Summit in California at the end of July and expects GIFCT companies to announce new initiatives to better address the threat of VETUI.

The GIFCT is actively working on ways to become more effective in its activities and partnerships with government and civil society, but is in need of reform. In a Five Eyes context, our contribution to this process may be best led at the working level, such as through the Digital Industry Senior Officials Group (DIESOG).

Child Sexual Exploitation and Abuse (CSEA)

For the most serious online offending such as terrorism and CSEA, the UK White Paper proposes that companies go much further than for other harms, and demonstrate the steps taken to combat the dissemination of associated content and illegal behaviours.

In Canada, the RCMP's National Child Exploitation Coordination Centre (NCECC) is the central point of contact for investigations related to online CSEA. In 2016, the Canadian Centre for Child Protection (C3P) launched Project Arachnid, a technological tool which identifies child sexual

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

exploitation images for removal from the Internet, which is also being supported by the UK Home Office and allows for unprecedented collaboration between Canada and the UK in the field.

C3P is very supportive of the UK approach to CSEA, including its work to engage with the digital industry to put in place a set of voluntary guiding principles and best practices to guide their role in addressing CSEA.

[redacted]

Data and technology sharing is a crucial component of law enforcement's ability to address online child sexual exploitation and abuse internationally. Canada is supportive of enhanced information sharing related to investigational data, technological challenges, requirements and solutions; however there is a need to distinguish between technology and criminal-related personal information sharing. Canadian privacy protection legislation and our constitutional framework require maintaining the case-by-case approach for personal information sharing.

In Canada, the Sex Offender Information Registration Act (SOIRA), which was implemented in 2004, and the National Sex Offender Registry (NSOR) established thereunder, is the federal database of convicted sex offenders (child and otherwise) in Canada. The NSOR is administered by the RCMP and accessible to all accredited Canadian police agencies for specific preventive or investigative purposes through provincial/territorial registration centre. The NSOR is an offence-based model and inclusion is automatic upon conviction for a range of sex offences; it is not determined by the offender's level of risk.

Canadian law enforcement officials are authorized to disclose to foreign police services information collected under SOIRA or under the NSOR, on a case by case basis as long as the threshold is satisfied specifying that sharing information is necessary to assist a police service outside Canada with the prevention or investigation of a crime of a sexual nature. Prohibitions on systematic disclosure of this information ensure consideration of the registered sex offender's privacy interests and fundamental rights under the Canadian Charter of Rights and Freedoms.

Encryption

2018 Statement of Principles on Access to Evidence and Encryption

As part of last year Five Country Ministerial meeting, the Five Eyes released a Statement of Principles on Access to Evidence and Encryption. The statement stressed the importance of encryption to cybersecurity, as well as the challenges it creates for law enforcement and national security agencies. The need to cooperate with providers of information and communications technology and services was emphasised. Finally, the statement underscored the importance of the rule of law and due process, as well as the freedom of choice for Five Eyes countries to address encryption as they see fit.

The Statement of Principles garnered some media attention, and some criticism. The particular focus of criticism and comments was on what was characterized as a threat made by the five

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Governments; which was that if service providers did not voluntarily assist in providing unencrypted data, that Governments retain the right to proposed "technological, enforcement, legislative or other measures to achieve lawful access solutions".

Existing solutions

[redacted]

Public debate and stakeholders' engagement

While CSPs are receptive to engaging on encryption, they have strongly opposed attempts by governments to mandate access to encrypted data in ways that would undermine the security of their products or jeopardize the trust of their users. When faced with coercive government actions, CSPs have not hesitated to challenge them in court. For example, the associations representing major US CSPs filed amicus briefs in support of Apple during 2016 litigation over access to a dead terrorist's encrypted iPhone. Given the importance of protection of cybersecurity, these concerns would need to be fully addressed by any government policy that attempts to assist law enforcement with the challenge of encryption, both from a substantive perspective, and from a communications perspective.

Another challenge in this respect is that even if the requirements imposed do not in fact inherently weaken the protection provided by encryption, concerns regarding this possibility will likely continue to strongly influence the views of the public and stakeholders, and raise significant privacy concerns.

Hostile State Activity (HSA)

[redacted]

The UK has launched a parliamentary review of the impact of disinformation during the Brexit Campaign. Following its investigation on the roles played by Facebook and Cambridge Analytica, the Parliamentary Committee on Digital, Cultural, Media and Support (DCMS) published an interim report on July 29, 2018. The report outlined the incident, the threats, and provided recommendations to the Government.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Like Canada, the UK is a member of the European Union Centre of Excellence on Hybrid Warfare (Hybrid CoE). The UK is a member of the G7 Rapid Response Mechanism (RRM), led by Canada, established at the G7 Summit in June 2018.

Foreign Terrorist Fighters (FTFs)/Returns

A successful initiative within CONTEST, the UK counter-terrorism strategy, is the Channel program, which involves local police, health, and community agencies who come together to assess cases and design tailored interventions to guide individuals away from violent extremism.

The UK's *Terrorism Act* provides stop and search powers to assist police and border forces in the prevention, disruption, and detection of terrorism. Among measures available, Terrorism Prevention and Investigation Measures, which are similar to Canada's Peace Bonds, can be issued by the Home Secretary.

The Home Secretary may deprive individuals of their citizenship through executive power. Between 2006 and March 2019, the Home Secretary denaturalized 373 Britons, 53 of whom had alleged links to terrorism. The UK Home Secretary takes the decision to denaturalize British citizens on a case-by-case basis, with the direction of the Government of the UK legal counsel. Under international law, the UK can only revoke citizenship of a dual national. The UK is not permitted to revoke citizenship to make an individual stateless.

Recently, the US and Kurdish authorities have requested source countries to repatriate their nationals. Canada has thus far not repatriated any of its nationals, including children. Under section 6(1) of the *Charter of Rights and Freedom*, Canadian citizens have the right to enter Canada; however, in most cases, Canada has no positive obligation to provide repatriation assistance. Canada has no diplomatic presence in Syria and, as such, its ability to provide consular assistance there is extremely limited.

The repatriation of children presents a number of complex challenges. Notwithstanding, concern about the welfare of the children being held in Al Hol has been growing. Pressure from local officials, the UN, non-governmental organizations (NGOs) and activists to repatriate these children based on moral and humanitarian grounds is intensifying. Media attention on this issue has increased significantly since April, when Germany reportedly repatriated several children. Three children have been repatriated to the UK. However, the UK's policy is not to repatriate.

Terrorist Listing

Canada is considering adding additional groups to its *Criminal Code* list of terrorist entities. As part of this process, you may wish to raise the prospect of listing an entity in concert with the UK.

Consulted: CSCCB, NCSB, NSOD, and PACB/Canada Centre.

Pages 76 to / à 93

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Medium-Term Planning – Violent Extremist and Terrorist Use of the Internet

Violent extremists and terrorists (VET) continue to use the internet and online space for a variety of purposes, including for recruiting, promoting, financing, planning and glorifying their activities, and there are real-life consequences from exposure to such content. Canada has not been immune to incidences of violence whereby the internet has played a role.

The Government of Canada (GoC) is committed to protecting Canadians from violent extremist and terrorist use of the internet (VETUI), and equipping law enforcement, practitioners and civil society with the tools necessary to identify and address VET activity online, in a way that respects fundamental human rights and freedoms. In advancing these efforts, Public Safety Canada, through the Canada Centre for Community Engagement and Prevention of Violence (Canada Centre)[1], continues to work directly with digital industry [redacted] The Canada Centre also collaborates with and provides financial support to academia and civil society for research and initiatives to address VETUI in Canada. Given the cross-border nature of the internet, the Canada Centre is also working alongside ally and partner countries bilaterally and multilaterally through forums such as the Five Country Ministerial, G20 and G7, and processes such as the Christchurch Call to Action to make coordinated demands on digital industry and find opportunities to coordinate government efforts to address VETUI.

[redacted]

CONSIDERATIONS

Issue:

The growing link between VET attacks and the online space has increased domestic and international attention on VETUI. For example, in 2017, Alexandre Bissonnette murdered six and injured 19 others in a shooting at a Quebec City mosque. His radicalization was influenced by neo-Nazi and violent right-wing extremist content online. In 2018, Alek Minassian killed 10

[1] The Canada Centre for Community Engagement and Prevention of Violence (Canada Centre) was established in 2017, and serves as a centre of excellence on countering radicalization to vioelence. Housed in Public Safety Canada, the Canada Centre is responsible for the Government of Canada's response to violent extremist and terrorist use of the internet.

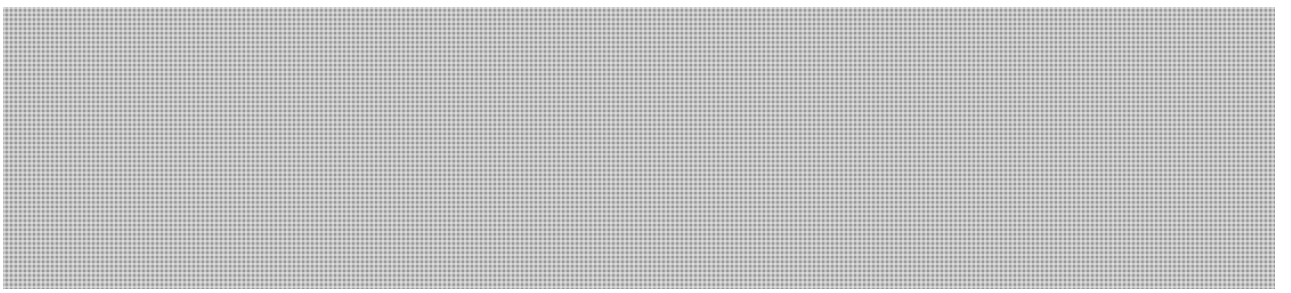
[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

and injured 16 when he drove a van onto a busy pedestrian street in Toronto. Minassian was influenced by the "incel" (involuntarily celibate) movement online, with which he engaged on the platform Reddit.

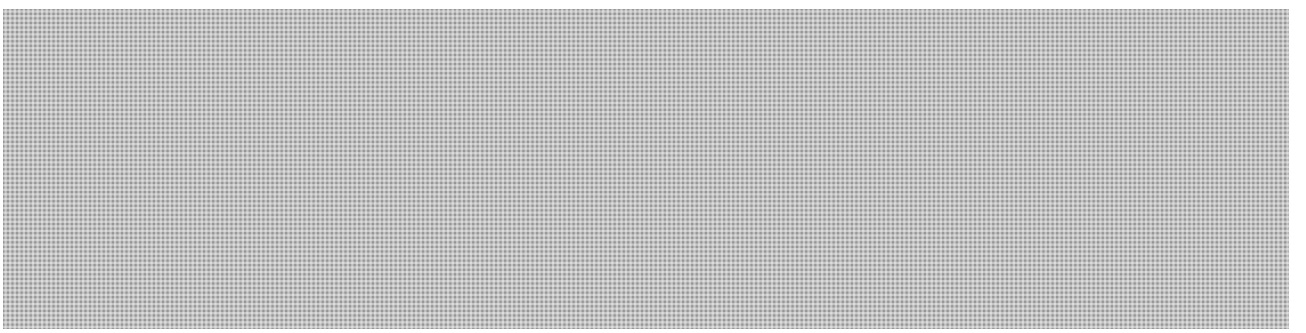
Nearly all Five Eyes and G7 partners have experienced one or numerous violent extremist and/or terrorist attacks in the last ten years that had a nexus to the online space. In March 2019, New Zealand experienced a terrorist attack that killed 51 and injured 50 at two mosques. The alleged perpetrator was influenced by online right-wing extremist and neo-Nazi propaganda. The attack was livestreamed on Facebook, shared on other platforms and reached millions of views worldwide. YouTube reported that the video was shared at a rate of once per second. Most recently, during the first weekend of August 2019 the U.S. experienced two separate shootings which killed a total of 31 people. One of the shooters in El Paso is believed to have used the online platform 8chan to share white nationalist and anti-immigration views prior to the attack.

The internet offers many societal benefits, including improved communication and interconnectedness. However, it has also enables VETs to more rapidly and effectively recruit, groom, finance, promote, and incite violence. Social media and content-sharing platforms are favoured by VETs for a number of reasons: (1) they can be used to disseminate messages to a broad and global audience; (2) they often provide encrypted communication services, making it challenging to identify and remove content (i.e. WhatsApp or Telegram);
(3) they employ recommendation algorithms that direct users to content related to (and sometimes more extreme than) their search histories (i.e. YouTube); (4) they provide a level of anonymity to users (i.e. Gab or 4chan); and (5) they often function based on lenient and/or unenforced Terms of Service.



Existing efforts:

The Canada Centre leads efforts within the GoC to prevent and counter VETUI. This includes: providing policy guidance; working with digital industry; engaging with international partners in multilateral forums and bilaterally, including committing to efforts to prevent and counter VETUI at the Five Country Ministerial, G7, G20, and Christchurch Call to Action; and supporting research and initiatives with civil society and academia to better understand VETUI.



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The Canada Centre is also working with each company bilaterally to increase our respective understanding of VET content in the online space and increase capacity to address VETUI. For example, in October 2018 the Canada Centre hosted a "hackathon" in Facebook's Toronto office with students from across the Greater Toronto Area to help them learn how to develop counternarratives against VET content online.

Morover, in June 2019, the GoC announced up to $1 million for Tech Against Terrorism to create a digital repository that will notify smaller companies when new terrorist content is detected, which will support them in quickly removing it.

International engagement

The Canada Centre engages with like-minded international partners both bilaterally and multilaterally on VETUI.

The Canada Centre also engages in a variety of international and multilateral forums and processes on VETUI, including the G7 Security/Interior Ministers' Meetings and Leaders' Summit, the G20, the Five Country Ministerial, the Aqaba Process, and the Christchurch Call to Action. Canada has led VETUI discussions in these summits in the last few years; in 2018, Canada included VETUI as a key agenda item during the Security Ministers' Meeting during its presidency and in 2019, Canada co-led the VETUI discussion with New Zealand at the FCM. Canada has signed onto a number of VETUI-related commitments in these forums over the last three years, including: the G7 Joint Communiqué of Interior Ministers in 2017 and the Toronto Commitments and Charlevoix Leaders' Summit Communiqué in 2018; the G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism; the 2018 FCM Statement on Countering the Illicit Use of the Online Space, and the 2019 Joint Communiqué; and the Christchurch Call.

Finally, Canada is engaging at the United Nations (UN) to coalesce support for efforts to prevent and counter VETUI, although there are opportunities for greater engagement. The Canada Centre attended the UN General Assembly (UNGA) last year, The Canada Centre also engages, when necessary, with the UN Counter Terrorism Executive Directorate (CTED) on VETUI priorities and issues, including on Tech Against Terrorism's activities.

Canada also actively engages in the Global Counter-Terrorism Forum (GCTF), a multilateral counter-terrorism platform that works closely with UN bodies and other international and regional organizations to counter terrorism and the violent extremist ideologies that underpin it.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Terrorist misuse of the internet is a key area of focus for the GCTF's CVE Working Group.

[redacted]

Supporting research and initiatives with civil society and academia

The Canada Centre collaborates closely with civil society and academia through policy, research and programming to counter radicalization to violence in Canada. The *National Strategy on Countering Radicalization to Violence* highlights the Canada Centre's commitment to support research and programming to better understand VETs behaviour online. It also emphasizes support to civil society for developing digital literacy guidelines and alternative narratives. Through the Community Resilience Fund (CRF), the Canada Centre has funded several research projects and initiatives designed to counter VET within the online space. For example, in 2018, the CRF funded Moonshot CVE's *Canada Redirect* project, which uses online advertising tools and internet video channels to direct individuals to reliable third-party content that challenges extremist propaganda.[4]

[redacted]

[4] Other examples of CRF funding related to countering violent extremism in the online space include: "Pushing back against hate in online communities" by MediaSmarts, which will examine the experiences of young Canadians towards hate speech and violent radicalization; and "Updating the environmental scan of right-wing extremism in Canada" by the University of Ontario Institute of Technology, which is establishing an updated, comprehensive review of the beliefs, motivations, activities and connections that characterize the right-wing extremist movement in Canada, including in the online space.

[redacted]

Pages 98 to / à 100

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 101 to / à 105

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FOR OFFICIAL USE ONLY

FIVE COUNTRY
MINISTERIAL

Emerging Threats
London 2019

DRAFT COMMUNIQUÉ

1. We, the Home Affairs, Interior Security and Immigration Ministers of [redacted] 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 existing and emerging security threats whether faced in our communities, at our borders, or in the cyber space.

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. [redacted]
2. It is also vital that [redacted] 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 also increase the [redacted] risks to the integrity of our telecommunications networks. [redacted] There is agreement between the Five Eyes of the need to ensure supply chains are trusted and reliable to protect our networks from unauthorised access or interference.

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 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 [redacted] 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 [redacted] our nations to actively seek out opportunities to enhance trust and raise awareness of best practice associated with IoT devices and reaffirms the need to

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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 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 approach to drones informed through co-ordinated and in-depth information sharing around threat, vulnerabilities and counter-drone technology. We will also enable the 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 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.

2. We recognise the need to modernise border security systems to deal with evolving threats. We therefore commit to pursue expanded data sharing on travellers prior to and at the border to facilitate the secure movement of legitimate 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 and detect those who seek to evade or facilitate the evasion of border controls. We 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 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.

Countering Online Child Sexual Exploitation and Abuse: Digital Industry Roundtable

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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, and countering violent extremism and terrorism both online and offline, foreign terrorist fighters, and encryption.

Countering Online Child Sexual Exploitation and Abuse

1. We commit to support more effective prevention, disruption and investigative responses to this
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.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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 [redacted] 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 [redacted] 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 [redacted] 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 [redacted]

Online Safety and Encryption

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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. [redacted] 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 [redacted] 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 [redacted] on managing residual risk.

[redacted]

Pages 111 to / à 119

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 120 to / à 125

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information