Australian Government
Department of Foreign Affairs and Trade

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE SUBMISSION TO THE SELECT COMMITTEE ON FOREIGN INTERFERENCE THROUGH SOCIAL MEDIA

13 March 2020

TERMS OF REFERENCE

On 5 December 2019, the Senate resolved to establish a Select Committee on Foreign Interference through Social Media to inquire into and report on the risk posed to Australia's democracy by foreign interference through social media, with particular reference to:

a. use of social media for purposes that undermine Australia's democracy and values, including the spread of misinformation;

b. responses to mitigate the risk posed to Australia's democracy and values, including by the Australian Government and social media platforms;

c. international policy responses to cyber-enabled foreign interference and misinformation;

d. the extent of compliance with Australian laws; and

e. any related matters.

INTRODUCTION

The Department of Foreign Affairs and Trade (DFAT) provides foreign, trade and development policy advice to the Government. We work with other government agencies to ensure that Australia's pursuit of its global, regional and bilateral interests is coordinated effectively.

In line with these priorities, this Submission addresses the Terms of Reference clauses:

c. international policy responses to cyber-enabled foreign interference and misinformation; and

e. any related matters.

AUSTRALIA’S COUNTER FOREIGN INTERFERENCE STRATEGY

The Australian Government has defined foreign interference as activities carried out by, or on behalf of, a foreign actor, which are coercive, covert, deceptive or corrupting, and are contrary to Australia’s sovereignty and national interests. Foreign interference is distinct from foreign influence, which is a normal aspect of open and transparent international relations and diplomacy.

In April 2018, the Australian Government appointed a National Counter Foreign Interference Coordinator (NCFIC) within the Department of Home Affairs. NCFIC is leading efforts across Government to respond to foreign interference, in partnership with other agencies, through Australia’s Counter Foreign Interference (CFI) Strategy.

Australia’s CFI Strategy is country agnostic.

COUNTER FOREIGN INTERFERENCE DIPLOMATIC STRATEGY

The Government’s strategy to counter foreign interference includes a substantial diplomatic component, which DFAT is leading – the CFI Diplomatic Strategy pilot program. This focuses on cooperation with regional partners to enhance their resilience, as well as efforts to build support for stronger international norms against foreign interference.

The CFI Diplomatic Strategy mobilises Australia’s whole-of-government international engagement capabilities to support Australia’s wider CFI objectives as a core component of Australia’s wider foreign policy aims. The broad goals of diplomatic action under the CFI Diplomatic Strategy are country-agnostic and seek to counter foreign interference activity by:

- delivering clear messaging to ensure foreign actors understand what kinds of actions Australia finds unacceptable and that foreign interference is viewed as a core national security concern;
- showing foreign interference actors that their actions can and will be revealed and will generate a meaningful response;
- convincing foreign interference actors that their actions will have costs – and that these costs outweigh the benefits – including through international reputational damage and by underscoring both the strength of Australia’s systems and the sophistication of our detection and enforcement capabilities;
- demonstrating that the opportunities for foreign interference are narrowing in Australia and the region, including by increasing regional awareness, reducing vulnerabilities, strengthening institutions; and
- mobilising international collaboration to counter foreign interference and establish globally accepted norms of behaviour.

Whole-of-government international engagement efforts are focusing on building relevant capabilities and awareness in Southeast Asia and the Southwest Pacific, using targeted technical assistance and other forms of collaboration. We are also focusing on the mitigation of information interference and misinformation. To ensure effective integration, harmonisation and efficiency, these efforts are largely being implemented within the frameworks of broader engagement strategies and action plans developed and managed by relevant regional divisions in DFAT as well as other departments and agencies.

These international engagement efforts are aimed directly at reducing vulnerabilities and cultivating a less-permissive environment for foreign interference in the region. This will enable Australia and our regional partners to engage more effectively and reduce opportunities for inappropriate interference. They will also reduce the foreign interference risk to Australian interests and those of regional neighbours.

Diplomatic efforts will also seek to mobilise international collaboration to counter foreign interference. We aim to strengthen normative principles that discourage foreign interference actions, increase reputational costs and provide a supportive, internationally-accepted architecture for Australia's international efforts.

INTERNATIONAL POLICY RESPONSES TO CYBER-ENABLED FOREIGN INTERFERENCE AND MISINFORMATION

New activities under DFAT's CFI Diplomatic Strategy pilot program will build counter foreign interference awareness and capability in Southeast Asia and the Southwest Pacific with the aim of closing vulnerabilities and cultivating a less-permissive environment for foreign interference in Australia's near region. This includes activities that seek to strengthen awareness of disinformation and misinformation, including through social media.

DFAT delivered the first significant pilot program activity – a workshop on Building Strategic Communications Capability to Counter Disinformation – from 4 to 5 March 2020 in Singapore. The workshop was delivered in collaboration with the United Kingdom and hosted by an independent think tank, the Singapore Institute of International Affairs (SIIA). DFAT also engaged the Australian Strategic Policy Institute (ASPI) to deliver a non-government overview of the challenges of disinformation at the workshop.

The workshop raised awareness and built the capability of mid-level officials from the governments of ASEAN nations to better understand and counter hostile disinformation.

AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY AND CYBER COOPERATION PROGRAM

DFAT leads implementation of Australia's International Cyber Engagement Strategy (ICES), released in October 2017, which sets an ambitious agenda across the full spectrum of cyber affairs. The DFAT developed, whole-of-government ICES encompasses whole-of-government activity, coordinated by the Ambassador for Cyber Affairs and Critical Technology. Like the CFI Strategy, it is part of the suite of Government policy tools aimed at reinforcing internationally the robust measures we have taken at home. The overarching objective of the ICES is to maintain an open, free and secure cyberspace that drives economic growth, protects national security and fosters international stability.

- An open cyberspace is interoperable across borders and accessible to all; it facilitates unrestricted participation and the free flow of information, driving inclusive online collaboration, innovation and growth.
- A free cyberspace means people are not burdened by undue restrictions on their access to and use of cyberspace; and their human rights are protected online as they are offline so that cyberspace remains a vibrant force for economic, social and cultural development.
- A secure cyberspace is safe, reliable and resilient; it fosters an environment of trust so that individuals, businesses and governments can engage online with confidence and realise the opportunities and minimise the risks of the digital age.

Reflecting Australia's broad view of cyber affairs, the ICES has seven key themes, outlining Australia's plans to:

- maximise opportunities for economic growth and prosperity through digital trade;
- foster good cyber security practices;
- reduce the risk of cybercrime;
- promote peace and stability in cyberspace;
- advocate for multi-stakeholder Internet governance;
- promote respect for human rights and democratic principles online; and
- encourage the use of digital technologies to achieve sustainable development.

Freedom of expression is a fundamental part of a vibrant democracy and a culture of accountability. It underpins good governance and strong institutions. Australia's international cyber policy initiatives, including responses to cyber enabled foreign interference and misinformation, place a heavy emphasis on protecting the core human right to freedom of expression. Australia has played an active part in promoting Human Rights Council resolutions on freedom of expression, the safety of journalists, human rights defenders, human rights and the Internet, and civil society. We are committed to ensuring individuals are able to enjoy the same human rights online as they enjoy offline.

DFAT is an active participant in two concurrent United Nations (UN) processes that are considering the rules of state behaviour in cyberspace: a sixth Group of Governmental Experts (GGE) (comprising 25 countries, represented by experts) and an inaugural Open Ended Working Group (OEWG) (open to all 193 UN members, represented by diplomats). Previous GGEs, including the 2013 group that was chaired by Australia, agreed that existing international law applies to states' activities in cyberspace, and agreed 11 voluntary norms of responsible state behaviour to complement states' existing legal obligations. Previous GGE reports also recommended a number of confidence building measures (aimed at increasing transparency, minimising miscommunication and preventing escalation to conflict), as well as capacity building (to support all countries to implement the recommendations of the GGE reports). Every GGE report has been endorsed, by consensus, by the UN General Assembly.

The Cyber Cooperation Program was announced by the Minister for Foreign Affairs in May 2016, originally as a $4 million investment over four years. The size of the Cyber Cooperation Program has rapidly increased over time – at the launch of Australia's International Cyber Engagement Strategy (ICES) in October 2017, the Foreign Minister announced an additional $10 million to support activities that aligned with the ICES.
In March 2018, $1 million was announced at the ASEAN-Australia Special Summit.

In November 2018, $9 million was announced to support activities in the Pacific. In March 2019, an additional $10 million was announced bringing the total investment to $34 million out to 2023.

An investment strategy guides the delivery of activities against five priority outcome areas:

- an international cyber stability framework to engender responsible state behaviour in cyberspace [including by deepening understanding of the application of international law and norms of state behaviour in cyberspace];
- stronger cybercrime prevention, prosecution and cooperation [including cyber awareness, cybercrime legislation and training for law enforcement, prosecutors and judges];
- enhanced cyber security response capability for a strong and resilient cyber security posture [including CERTs and operational response networks];
- best practice use of technology to support economic growth and sustainable development [including through integrating cyber security by design]; and
- advocating and protecting human rights and democracy online [including freedom of expression online]. Activities under this pillar of work aim to advocate and ensure respect for the protection of human rights and democratic principles online; explore the linkages between human rights, technology and/or cyber security; and increase capacity to respond to and manage harmful online content in support of human rights.