THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Implications of the COVID-19 pandemic for Australia's foreign affairs, defence and trade

20 July 2020

Submission to the Joint Standing Committee on Foreign Affairs, Defence and Trade

Committee Secretary
Joint Standing Committee on Foreign Affairs, Defence and Trade
PO Box 6021
Parliament House
Canberra, ACT 2600

jscfadt@aph.gov.au

Contact: **David Edney**
President, NSW Young Lawyers

Katlyn Kraus
Chair, NSW Young Lawyers International Law Committee

Submissions Coordinators: Tara Peramatukorn and Joshua Clarke

Contributors: Tara Peramatukorn and Joshua Clarke

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

The NSW Young Lawyers International Law Committee **(Committee**) makes the following submission in response to the Inquiry into the implications of the COVID-19 pandemic for Australia's foreign affairs, defence and trade (**Inquiry**).

NSW Young Lawyers

NSW Young Lawyers is a division of The Law Society of New South Wales. NSW Young Lawyers supports practitioners in their professional and career development in numerous ways, including by encouraging active participation in its 15 separate committees, each dedicated to particular areas of practice. Membership is automatic for all NSW lawyers (solicitors and barristers) under 36 years and/or in their first five years of practice, as well as law students. NSW Young Lawyers currently has over 15,000 members.

The International Law Committee (**ILC**) is committed to providing a platform to young lawyers and law students with a key interest in international law (both public and private) to discuss among peers and learn from experts in the field through selected seminars, as well as providing networking opportunities. The ILC currently has over 1,700 members and has established working relationships with the Australian Institute of International Affairs, the Australian Dispute Centre, the Australian Centre for International Commercial Arbitration, International Law Association and the Rule of Law Institute of Australia. As one of its primary goals, the ILC endeavours to broaden the knowledge of international law within the legal profession and the Australian legal system. In doing so, the ILC seeks to promote informed discussion amongst its members and the wider legal community on international law in Australia.

Summary of Recommendations

The Committee makes the following recommendations for the Inquiry into the implications of the COVID-19 pandemic for Australia's foreign affairs, defence and trade.

On term of reference **(2) threats to the global rules based order that emerged due to actions by nation states during the pandemic, and how such threats can be mitigated in the event of future crises**, the Committee submits the Australian Government should:

1. continue to meet its financial obligations to the World Health Organization (**WHO**) in accordance with its treaty commitments;

2. continue to support global health governance by leveraging Australia's status as a health leader in the Western Pacific region; and

3. support evidence-based reforms to the existing multilateral framework for global health security that makes it more effective.

On **(5) what policy and practical measures would be required to form an ongoing effective national framework to ensure the resilience required to underpin Australia's economic and strategic objectives**, the Committee submits the Australian Government should:

1. consider enacting legislation or regulations to mandate a minimum standard of cybersecurity measures that Australian businesses are required to implement;

2. immediately implement the mandated cybersecurity requirements for governmental entities at federal, state and territory level; and

3. create a dedicated ministerial portfolio for cyber affairs.

This submission now turns to each term of reference and the detailed suggestions made by the Committee regarding each of them.

How threats to the global rules based order that emerged due to actions by nation states during the pandemic can be mitigated in the event of future crises

On **(2) threats to the global rules based order that emerged due to actions by nation states during the pandemic, and how such threats can be mitigated in the event of future crises**, the Committee submits the Australian Government should:

1. continue to meet its financial obligations to the WHO in accordance with its treaty commitments;

2. continue to support global health governance by leveraging Australia's status as a health leader in the Western Pacific region; and

3. support evidence-based reforms to the existing multilateral framework for global health security that makes it more effective.

Introduction

At the foundation of Australia's strategic objectives is the maintenance of our security and way of life.[1] In this respect, the COVID-19 pandemic has clearly demonstrated two things: firstly, that a critical component of Australia's security and way of life is the country's health security; and secondly, that Australia's health security is inextricably linked to the health situation in the Western Pacific region and around the world.

Global health experts and leaders have been warning of the ever-increasing risk of worldwide outbreaks of disease since prior to the current crisis.[2] They have identified an urgent need for states to take action domestically as well as to cooperate with one another, in order to effectively address this global health risk. The WHO plays a critical role in assisting individual governments to implement resilient health systems and provides a framework for global health coordination within the existing rules-based order — both of which are needed to guard against the "very real threat" of a scenario like the COVID-19 pandemic but with potentially far worse consequences.[3]

The Australian Government recognises that its interests are served by respect for the rules-based international order and the support of international institutions.[4] This is especially true when discussing Australia's health security.[5] Therefore, the prospect of nation states withdrawing support and funding from the WHO, especially in the midst of an ongoing global health crisis — as is currently transpiring in the case of the WHO's biggest donor, the United States — is a real threat to Australia's strategic interests and against the spirit of international legal developments of which Australia has long been a key proponent.

---

[1] See below at Introduction to Term of Reference 5 at page 12 of this Submission; Mike Scrafton, 'What are Australia's strategic objectives?', *The Strategist* (online, 5 November 2018) <https://www.aspistrategist.org.au/what-are-australias-strategic-objectives/>; Department of Defence, *2020 Defence Strategic Update*, July 2020, 3; Department of Defence, *2016 Defence White Paper*, February 2016, 9.
[2] See, e.g., Global Preparedness Monitoring Board, *A World At Risk: Annual Report on Global Preparedness for Health Emergencies* (Report, September 2019).
[3] Ibid 6.
[4] See, e.g., Department of Defence, *2020 Defence Strategic Update*, July 2020, 24; Department of Foreign Affairs and Trade, *2017 Foreign Policy White Paper* (Report, 2017); Department of Foreign Affairs and Trade, 'Australia and the world: Looking outward' (Web Page) <https://www.dfat.gov.au/about-australia/australia-world/Pages/looking-outward>; World Health Organization, *Australia-WHO Country Cooperation Strategy 2018–2022* (2017).
[5] World Health Organization, *Australia-WHO Country Cooperation Strategy 2018–2022* (2017).

In the Committee's view, the COVID-19 pandemic has reinforced the need for Australia to continue supporting multilateralism and international institutions in the pursuit of its strategic agenda, especially where health security is concerned.

An ever-increasing risk of pandemics

In a portentous report released in September 2019, the Global Preparedness Monitoring Board (**GPMB**) — an independent group of health experts co-convened by the WHO and World Bank — stated:

> "*Epidemic-prone diseases such as influenza, Severe Acute Respiratory Syndrome (SARS), Middle East Respiratory Syndrome (MERS), Ebola, Zika, plague, Yellow Fever and others, are harbingers of a new era of high-impact, potentially fast-spreading outbreaks that are more frequently detected and increasingly difficult to manage*".[6]

Months prior to the COVID-19 outbreak, the GPMB forecasted that the chances of a global pandemic are growing and concluded that the world was not prepared for a fast-moving, virulent respiratory pathogen pandemic.[7] The WHO issued a similar warning in the wake of the H1N1 Influenza pandemic of 2009.[8] The GPMB stated:

> "*The world is at acute risk for devastating regional or global disease epidemics or pandemics that not only cause loss of life but upend economies and create social chaos*".[9]

The GPMB foreshadowed the 'very real' possibility of a rapidly moving, highly lethal pandemic of a respiratory pathogen killing 50 to 80 million people and wiping out nearly 5% of the world's economy.[10]

Accordingly, the GPMB had urgently recommended that governments consider, as an integral part of their national security, the dedication of domestic resources to disease outbreak preparedness, and support cooperation between states and an international response system as an essential 'global safety net'.[11] The Lancet Commission on the Legal Determinants of Health reinforces this point, stating in the opening words of a 2019 report:

> "*Health risks in the 21st century are beyond the control of any government in any country. In an era of globalisation, promoting public health and equity requires cooperation and coordination both within and among states*".[12]

---

[6] Global Preparedness Monitoring Board, *A World At Risk: Annual Report on Global Preparedness for Health Emergencies* (Report, September 2019) 12.
[7] Ibid 15.
[8] World Health Organization, *Strengthening Response to Pandemics and Other Public-Health Emergencies: Report of the Review Committee on the Functioning of the International Health Regulations (2005) and on Pandemic Influenza (H1N1) 2009* (Report, 2011) 119.
[9] Ibid 11.
[10] Ibid 6.
[11] Ibid 7, 36.
[12] Lawrence O Gostin et al, 'The Legal Determinants of Health: Harnessing the Power of Law for Global Health and Sustainable Development' (2019) 393 *Lancet* 1857.

Australia is awake to the need to continue to improve its high standards of health security domestically, while working with regional partners and international organisations, in order to combat diseases that spread faster and more unpredictably than ever before due to our increasingly interconnected world.[13]

The role of the WHO in combating global disease outbreaks

The WHO has an important role on both the domestic and international fronts in the fight against global disease outbreaks.

Among its many functions, leading and guiding global efforts for pandemic preparedness is a key role of the organisation[14] — and an increasingly critical one, in light of the proliferation of infectious disease outbreaks around the world in the past decade.[15] As the GPMB states of domestic preparedness, "*[a]ction and investment prior to an emergency are essential to provide the best possible protection*".[16] Through the International Health Regulations (2005) (**IHR (2005)**), the WHO assists governments to develop national core capacities; to strengthen national health systems so that they are capable of managing acute public health events with the potential to cross borders and threaten populations worldwide.[17]

Further, as recent events have shown, the WHO performs a crucial role once a disease outbreak has emerged. A pneumonia of unknown cause detected in Wuhan, China was first reported to the WHO China Country Office on 31 December 2019.[18] Since then, the WHO has directed and coordinated the international health response to the COVID-19 outbreak. In this function, the WHO has:

(i) worked to improve country preparedness and response;

(ii) accelerated research and development;

(iii) coordinated across regions to assess, respond to and mitigate risks; and

(iv) communicated about how people can protect themselves and others.[19]

Although the WHO's response to particular outbreaks has been the subject of criticism in the past (and more recently), the cooperative mechanisms built into the organisation are what have enabled the containment of infectious disease outbreaks.[20]

---

[13] Department of Health, *Australia's National Action Plan for Health Security: Implementation of the Recommendations from the Joint External Evaluation of IHR Core Capacities* (December 2018) 3; World Health Organization, *Australia-WHO Country Cooperation Strategy 2018–2022* (2017).
[14] *Constitution of the World Health Organization*, opened for signature 22 July 1946, 14 UNTS 185 (entered into force 7 April 1948) art 2; Belinda Bennett, 'Updating Australia's Pandemic Preparedness: The Revised Australian Health Management Plan for Pandemic Influenza (AHMPPI)' (2015) 22 *Journal of Law and Medicine* 506, 507.
[15] Global Preparedness Monitoring Board, *A World At Risk: Annual Report on Global Preparedness for Health Emergencies* (Report, September 2019) 12.
[16] Ibid 18.
[17] World Health Organization, *Joint External Evaluation of IHR Core Capacities of Australia* (2018) viii.
[18] World Health Organization, 'Rolling updates on coronavirus disease (COVID-19)' (Online Noticeboard, 11 June 2020) <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen>.
[19] World Health Organization, 'How is WHO responding to COVID-19?' (Web Page, 2020) <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/who-response-in-countries>; See generally World Health Organization, 'Alert and Response Operations' (Web Page, 2020) <https://www.who.int/csr/alertresponse/en/>.
[20] See, e.g., Charlotte Owens, 'The Case for the World Health Organisation', *Interpreter* (online, 22 April 2020) <https://www.lowyinstitute.org/the-interpreter/case-world-health-organisation>.

Australia and the WHO

Australia played an active role during the negotiations at the 1946 International Health Conference, from which the WHO originated, culminating on 22 July 1946 when a representative signed the Constitution of the WHO (**WHO Constitution**) subject to the approval and acceptance of the Government of the Commonwealth of Australia.[21]

On 11 December 1947, the *World Health Organization Act 1947* (Cth) (**WHO Act**) came into force, whereby Parliament:

(i) approved Australia's becoming a member of the WHO;[22]

(ii) accepted the arrangement for the initiation of the program of the WHO under an Interim Commission, of which Australia was also a member;[23] and

(iii) incorporated the text of the Constitution as a schedule to the WHO Act.[24]

On 2 February 1948, Australia formally accepted the WHO Constitution and became a member of the WHO.[25] The WHO Constitution entered into force on 7 April 1948 upon its ratification by the 26th Member State.[26]

Australia has since enjoyed an exceptionally strong relationship with the WHO and worked closely with the organisation over its 70 years in existence.

Australia benefits from the international health treaties and instruments negotiated under the auspices of WHO, such as the IHR (2005), which support new policy approaches in Australia and the development of effective, efficient and resilient health systems.[27] In turn, Australia has leveraged its vast experience and technical expertise in health to assist WHO in its mandate and mission in the Western Pacific region.[28] As of 2017, when the most recent Australia–WHO Country Cooperation Strategy was released, Australia had 46 WHO collaborating centres that worked directly with the organisation on a range of technical priorities.[29]

In recent years, Australia and the WHO partnered to strengthen Australia's ability to manage acute public health events. In 2017, Australia voluntarily undertook a Joint External Evaluation of the nation's core capacities under the IHR (2005) (**JEE**), an initiative administered by the WHO.[30] Australia was only the second high-income country in the Western Pacific Region and the first in the Pacific to voluntarily conduct a JEE.[31] The JEE mission in Australia found that the nation demonstrated a very high level of capacity against the IHR

---

[21] World Health Organisation Interim Commission, *Summary Report on Proceedings, Minutes and Final Acts of the International Health Conference held in New York from 19 June to 22 July 1946*, WHO ICOR 2 (1948).
[22] *World Health Organization Act 1947* (Cth) s 5(a).
[23] Ibid s 5(b); Second Schedule.
[24] Ibid First Schedule.
[25] *Constitution of the World Health Organization*, opened for signature 22 July 1946, 14 UNTS 185 (entered into force 7 April 1948) art 79; World Health Organization, *Basic Documents* (49th ed, 2020) 233; World Health Organization, 'World Health Organization in Australia' (Web Page, 2020) <https://www.who.int/australia/about-us>.
[26] *Constitution of the World Health Organization*, opened for signature 22 July 1946, 14 UNTS 185 (entered into force 7 April 1948) arts 79–80; World Health Organization, *Basic Documents* (49th ed, 2020) 233 fn 1.
[27] World Health Organization, *Australia-WHO Country Cooperation Strategy 2018–2022* (2017) 17.
[28] Ibid v.
[29] Ibid vii.
[30] World Health Organization, *Joint External Evaluation of IHR Core Capacities of Australia* (2018) viii; Department of Health, *Australia's National Action Plan for Health Security: Implementation of the Recommendations from the Joint External Evaluation of IHR Core Capacities* (December 2018).
[31] World Health Organization, *Joint External Evaluation of IHR Core Capacities of Australia* (2018) viii.

(2005) requirements.[32] In 2018, following this exercise with the WHO, Australia released a 2019–2023 National Action Plan for Health Security (**NAPHS**) to set out a plan for implementing the 66 recommendations of the JEE Mission Report. The Committee commends the Australian Government for leading by example in its preparedness commitments under the IHR (2005), which is consistent with best practices encouraged by the GPMB.[33]

Australia is cognisant of the importance of the WHO's work in the region for Australia's own health security and strategic interests. As set out in the 2018–2022 Australia–WHO Country Cooperation Strategy:

> "*While Australia does not share any land borders, rapid air travel and trade mean that outbreaks of new and re-emerging diseases in one country can become global concerns in a matter of hours. In Australia's immediate vicinity, the Western Pacific Region faces a range of health security threats: infectious diseases including drug- resistant forms of tuberculosis and malaria; emerging infectious diseases such as avian and pandemic influenza; natural disasters, including earthquakes, droughts and cyclones; and global threats such as antimicrobial resistance (AMR). Close cooperation with WHO on protecting and promoting regional health security is in Australia's domestic and regional interests*".[34]

This cooperation is underscored by Australia's obligations to the world at large under the IHR (2005), of which Australia played a lead role in the negotiation and drafting.[35] These obligations include:

(i) maintaining effective disease surveillance and laboratory systems;

(ii) reporting newly emerging diseases that could spread internationally; and

(iii) maintaining the necessary infrastructure to respond to health emergencies.[36]

The WHO considers that Australia's high capacity domestically means there is an obligation on Australia to proactively support the other Member States in the region to achieve their core capacities under the IHR (2005), which it recognises Australia is actively doing.[37] Australia similarly appreciates its role as a global health leader above and beyond its minimum international health obligations, stating in the NAPHS:

> "*Maintaining connections to our international partners, including the WHO and the World Organisation for Animal Health and our fellow Member States, is also central to strengthening global health security. It is in the best interests of the global community, and a moral imperative, to build the capacities of other countries to respond to public health threats*".[38]

This is consistent with a broader theme of Australia's foreign policy, being that "*[o]ur investment in the stability and resilience of developing countries works to improve our own security and prosperity*".[39]

---

[32] Ibid 3.
[33] Global Preparedness Monitoring Board, *A World At Risk: Annual Report on Global Preparedness for Health Emergencies* (Report, September 2019) 7.
[34] World Health Organization, *Australia-WHO Country Cooperation Strategy 2018–2022* (2017) 19.
[35] Ibid.
[36] World Health Organization, *International Health Regulations (2005)* (3rd ed, 2016); Global Preparedness Monitoring Board, *A World At Risk: Annual Report on Global Preparedness for Health Emergencies* (Report, September 2019) 18.
[37] World Health Organization, *Joint External Evaluation of IHR Core Capacities of Australia* (2018) 2.
[38] Department of Health, *Australia's National Action Plan for Health Security: Implementation of the Recommendations from the Joint External Evaluation of IHR Core Capacities* (December 2018) 3. See also Department of Foreign Affairs and Trade, *Health for Development Strategy 2015–2020* (June 2015).
[39] Department of Foreign Affairs and Trade, *2017 Foreign Policy White Paper* (November 2017) 11.

The future of the WHO?

In the midst of the ongoing COVID-19 pandemic, the WHO has come under scrutiny for its management of the crisis.[40] Since April, the United States — currently the WHO's largest donor[41] — temporarily suspended and has been threatening to permanently cease its funding to the WHO due to asserted inadequacies of the organisation and its response to the coronavirus outbreak.[42] On 6 July 2020, the United States took the step of formally notifying the United Nations that the United States will withdraw from the WHO, effective 6 July 2021.[43] This would likely impede the ability of the WHO to continue to effectively deliver programs in countries with weaker health systems and lower income countries, which improve health security globally.[44] Further, the erosion of confidence in health institutions such as the WHO only serve to increase the risk posed by infectious disease outbreaks of the future.[45]

Within the WHO's legal framework, Member States are obliged to make minimum assessed contributions towards the organisation's budget, which are calculated according to the particular country's wealth and population.[46] For example, according to the scale of assessments set by the World Health Assembly, the United States is obliged to contribute 22% of the portion of the WHO's 2020–2021 budget derived from assessed contributions,[47] in order to continue to enjoy the full rights of a Member State of the organisation.[48] Significantly, however, assessed contributions have made up less than a quarter of the WHO's financing for several years now, making voluntary contributions the primary source of funds for the organisation.[49] During the 2018–2019 period, the United States' voluntary contributions to the WHO were nearly triple its mandatory, assessed contribution.[50]

Australia's assessed contribution for the 2020–2021 biennium was set to 2.2101%,[51] however Australia's voluntary contributions during the 2018–2019 period were over double its assessed contributions in that period.[52] We are considered a leading contributor of voluntary flexible funds to the WHO.[53]

---

[40] Charlotte Owens, 'The Case for the World Health Organisation', *Interpreter* (online, 22 April 2020) https://www.lowyinstitute.org/the-interpreter/case-world-health-organisation.
[41] World Health Organization, '2018–19 Contributors' (Web Page, 2020) <http://open.who.int/2018-19/contributors/contributor>.
[42] Jordan Fabian and Eryk Bagshaw, 'Trump threatens to cut off WHO funding permanently', *Sydney Morning Herald* (online, 19 May 2020) <https://www.smh.com.au/world/north-america/trump-threatens-to-cut-off-who-funding-permanently-20200519-p54uee.html>.
[43] Katie Rogers and Apoorva Mandavilli, 'Trump Administration signals formal withdrawal from W.H.O', New York Times (online, 7 July 2020) <https://www.nytimes.com/2020/07/07/us/politics/coronavirus-trump-who.html>.
[44] Erin Handley and Michael Walsh, 'What happens if the US stops funding the WHO in the middle of the coronavirus pandemic?', *ABC News* (online, 16 April 2020) <https://www.abc.net.au/news/2020-04-16/coronavirus-who-explainer-what-does-trump-funding-decision-mean/12151080>.
[45] Global Preparedness Monitoring Board, *A World At Risk: Annual Report on Global Preparedness for Health Emergencies* (Report, September 2019) 15.
[46] *Constitution of the World Health Organization*, opened for signature 22 July 1946, 14 UNTS 185 (entered into force 7 April 1948) art 56.
[47] *Scale of Assessments for 2020–2021*, Agenda Item 15.5, WHA 72.17 (28 May 2019).
[48] *Constitution of the World Health Organization*, opened for signature 22 July 1946, 14 UNTS 185 (entered into force 7 April 1948) art 7.
[49] World Health Organization, 'Assessed Contributions' (Web Page, 2020) <https://www.who.int/about/finances-accountability/funding/assessed-contributions/en/>.
[50] World Health Organization, '2018–19 Contributors' (Web Page, 2020) <http://open.who.int/2018-19/contributors/contributor>.
[51] *Scale of Assessments for 2020–2021*, Agenda Item 15.5, WHA 72.17 (28 May 2019).
[52] World Health Organization, '2018–19 Contributors' (Web Page, 2020) <http://open.who.int/2018-19/contributors/contributor>.
[53] World Health Organization, *Australia-WHO Country Cooperation Strategy 2018–2022* (2017) 14.

While Australia's obligations under the WHO Constitution are unlikely to require Australia to continue making further voluntary contributions to the WHO, Australia is committed to pay its assessed contributions as membership dues of the organisation in accordance with the principle of *pacta sunt servanda*.[54] Australia's ratification of the WHO Constitution was a "*positive statement by the executive government of this country to the world and to the Australian people that the executive government and its agencies will act in accordance with the [Constitution]*".[55] This is reinforced by Parliament's passing of the WHO Act, in which it approved Australia's membership of the WHO and, arguably by extension, its minimum mandatory financial obligations as a Member State.[56]

The Committee recognises that the Australian Government appears to remain committed to meeting its funding obligations to the WHO, notwithstanding calls for reform to the organisation.[57] Encouragingly, Australia's continued advocacy for a strong and effective WHO, as an essential institution in global public health, is a foreign policy stance that currently enjoys bipartisan support.[58] Owing to Australia's world-class health system and demonstrated regional and global leadership on a range of priority health issues,[59] the Committee considers that the Australian Government is well-placed to urge other Member States to maintain their current or greater levels of financial support of the organisation. As submitted above, Australia benefits from the work of the WHO — both within and outside of the country — and enjoys a substantial degree of influence in global health matters through the organisation's multilateral framework. Consequently, the ongoing viability of the WHO should be a matter of national interest.

The Committee would also support expert-led, evidence-backed proposals for reform of the WHO, given its essential role in the face of increasing risk of infectious disease outbreak globally.[60] This is consistent with Australia's stated support for "*WHO's ongoing efforts to transform itself into a more efficient, transparent, fit-for-purpose, country-focused organization"*, which forms part of the foundations of Australia's current strategic agenda for cooperation with the WHO.[61] Accordingly, the Committee commends the Government in its co-sponsorship and support of the World Health Assembly resolution committing to an independent and comprehensive evaluation into the global response to COVID-19, including, but not limited to, WHO's performance.[62] The Committee considers that Australia's continued use and support of multilateral approaches to improving global and national health security are in Australia's best interests.

---

[54] See *Commonwealth v Tasmania (the Tasmania Dam Case)* (1983) 158 CLR 1, 219–220 (Brennan J); *Vienna Convention on the Law of Treaties*, opened for signature 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980) art 26.
[55] *Minister for Immigration & Ethnic Affairs v Teoh (1995) 183 CLR 273, 291 (Mason CJ and Deane J).*
[56] *World Health Organization Act 1947* (Cth) s 5(a).
[57] Malcom Farr, 'Australian PM pushes for WHO overhaul including power to send in investigators' *Guardian* (online, 22 April 2020) <https://www.theguardian.com/australia-news/2020/apr/22/australian-pm-pushes-for-who-overhaul-including-power-to-send-in-investigators>.
[58] Marise Payne, 'Australia and the world in the time of COVID-19' (Speech, National Security College, Australian National University, 16 June 2020) <https://www.foreignminister.gov.au/minister/marise-payne/speech/australia-and-world-time-covid-19>; Daniel Hurst, 'Labor warns Australia cannot afford to turn its back on global bodies like the World Health Organization' (online, 18 April 2020) <https://www.theguardian.com/australia-news/2020/apr/18/labor-warns-australia-cannot-afford-to-turn-its-back-on-global-bodies-like-the-world-health-organization>.
[59] World Health Organization, *Australia-WHO Country Cooperation Strategy 2018–2022* (2017) vii, 11, 19.
[60] See, e.g., Lawrence O Gostin et al, 'The legal determinants of health: harnessing the power of law for global health and sustainable development' (2019) 393 *Lancet* 1857.
[61] World Health Organization, *Australia-WHO Country Cooperation Strategy 2018–2022* (2017) 18.
[62] *COVID-19 Response*, Agenda Item 3, WHA 73.1 (19 May 2020); World Health Organization, 'Historic health assembly ends with global commitment to COVID-19 response' (News Release, 19 May 2020) <https://www.who.int/news-room/detail/19-05-2020-historic-health-assembly-ends-with-global-commitment-to-covid-19-response>.

Policy and practical measures required to form an ongoing effective national framework to ensure the resilience required to underpin Australia's economic and strategic objectives

On **(5) what policy and practical measures would be required to form an ongoing effective national framework to ensure the resilience required to underpin Australia's economic and strategic objectives**, the Committee submits that the Australian Government:

1. consider enacting legislation or regulations to mandate a minimum standard of cybersecurity measures that Australian businesses are required to implement;

2. immediately implement the mandated cybersecurity requirements for governmental entities at federal, state and territory level; and

3. create a dedicated ministerial portfolio for cyber affairs.

Introduction

One of the implications of the COVID-19 pandemic has been its uncovering of how unprecedented threats, both in type and scale, can threaten national economic and strategic objectives. As the terms of reference have not defined the contents of Australia's economic and strategic objectives, the Committee has taken a broad approach to defining these terms for the purposes of this submission:

(i) Australia's economic objectives are defined as those objectives which are concerned with furthering Australia's economic development[63] as well as support the economic prosperity and welfare of the people of Australia;[64] and

(ii) Australia's strategic objectives are defined as those objectives which are concerned with the protection of Australia from aggression, and with the maintenance of our security and our way of life.[65]

During the pandemic, there has been an increase in the number of cyber incidents reported against the Australian Government and Australian companies.[66] This has also been experienced by other countries worldwide.[67] Such cyber attacks have put pressure on governments pursuing existing economic and strategic objectives, as well as new objectives to counter the pandemic's negative effects on lives and livelihoods of Australians.

Additionally, to keep the economy running in a safe manner, Australian State and Territory Governments as well as other governments worldwide, have transitioned workers to work-from-home arrangements where possible. These changes arising from the pandemic have accelerated the rate of digitisation of our daily lives. This has resulted in increased internet usage across Australia – the NBN saw an increase in internet demand

---

[63] See, e.g., Department of Defence, *2016 Defence White Paper*, February 2016.
[64] See *Reserve Bank Act 1959* (Cth) s 10(2)(c).
[65] Mike Scrafton, 'What are Australia's strategic objectives?', *The Strategist* (online, 5 November 2018) <https://www.aspistrategist.org.au/what-are-australias-strategic-objectives/>.
[66] Alastair MacGibbon, 'Recent cyber attacks just the tip of the iceberg for Australia', *Australian Financial Review* (online, 18 May 2020) <https://www.afr.com/technology/recent-cyber-attacks-just-the-tip-of-the-iceberg-for-australia-20200515-p54thf>.
[67] See, e.g., Dan Sabbagh, 'Hackers targeting UK research labs amid vaccine race – GCHQ chief', *The Guardian* (online, 5 June 2020) <https://www.theguardian.com/uk-news/2020/jun/04/hackers-targeting-uk-research-labs-amid-vaccine-race-gchq-chief>.

by around 70% and 80% at the end of February 2020.[68] More people are in remote working arrangements, resulting in a growing interconnectedness between work and personal computer systems which previously existed, however to a much lesser extent. The transition to working from home has also prompted questions about whether these arrangements may become more permanent once the pandemic subsides.[69]

This increasing reliance on cyberspace opens up an increased vulnerability to attacks on Australia's national security, economy and society.[70] The parallels between the pandemic and previous cyber attacks – rapid and indiscriminate propagation of a virus in an increasingly connected global society – have prompted some to warn that the next global crisis will be a cyber crisis.[71]

In the Committee's view, the effects of the pandemic have highlighted the need for Australia to take active steps to increase its cyber resilience against malicious actors online. This part of the submission will discuss concerns about cybersecurity in Australia and make recommendations on how Australia can improve its cyber resilience to underpin the pursuit of its economic and strategic objectives.

International law in cyberspace

There is no core or collection of international treaties which state that international law is applicable in cyberspace, or which dictate new international law rules applicable in cyberspace. However, there is general agreement among academics[72] and the international community[73] that existing rules of international law apply to activities in cyberspace.

Australia supports this position. On 16 April 2020, Australia provided its comments on the initial "Pre-draft" of a report by the UN Open Ended Working Group in the field of information and telecommunications in the context of international security (**OEWG**). The OEWG allows United Nations Member States to express their views on the international security dimensions of information communication technologies, and is mandated to produce a consensus report following these discussions.[74] In its comments, Australia states that it strongly supports the reaffirmation in the Pre-draft that international law is applicable in cyberspace.[75]

---

[68] Liz Hobday and Nick Sas, 'Coronavirus affecting internet speeds, as COVID-19 puts pressure on the network', *Australian Broadcasting Corporation* (online, 1 April 2020) <https://www.abc.net.au/news/2020-04-01/coronavirus-internet-speeds-covid19-affects-data-downloads/12107334>.
[69] Alex Hern,'Covid-19 could cause permanent shift towards home working', *The Guardian* (online, 13 March 2020) <https://www.theguardian.com/technology/2020/mar/13/covid-19-could-cause-permanent-shift-towards-home-working>.
[70] Liam Nevill and Zoe Hawkins, 'Deterrence in cyberspace: different domain, different rules', *The Strategist* (online, 27 July 2016) <https://www.aspistrategist.org.au/deterrence-cyberspace-different-domain-different-rules/>.
[71] See, e.g. Katherine Mansted and Finn Robinsen, 'Australia needs volunteers to be ready for a cyber conflagration', *The Strategist* (online, 22 May 2020) <https://www.aspistrategist.org.au/australia-needs-volunteers-to-be-ready-for-a-cyber-conflagration/>; Tim Watts, 'Time to prepare for a cyber version of the coronavirus crisis', *The Strategist* (online, 1 May 2020) <https://www.aspistrategist.org.au/time-to-prepare-for-a-cyber-version-of-the-coronavirus-crisis/>.
[72] See, e.g., Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2nd ed, 2017).
[73] *Developments in the field of information and telecommunications in the context of international security*, GA Res 70/237, UN GAOR, 70th sess, Agenda Item 92, UN Doc A/RES/70/237 (30 December 2015) 2 <https://undocs.org/A/RES/70/237>.
[74] United Nations, *Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security*, March 2020, [6] <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf>.
[75] Department of Foreign Affairs and Trade, *Australia's comments on the Initial "Pre-draft" of the report of the UN Open Ended Working Group in the field of information and telecommunications in the context of international security (OEWG)*, 16 April 2020, 2 <https://www.dfat.gov.au/sites/default/files/australias-response-to-the-oewg-pre-draft-report-april-2020.pdf>.

Toby Feakin, Australia's Ambassador for Cyber Affairs, has also recently stated that:

> "*Countries have agreed at the United Nations that existing international law applies in cyberspace … Countries have also agreed that it is contrary to norms of responsible state behaviour to use cyber tools to intentionally damage or impair critical infrastructure providing services to the public*".[76]

This was a statement made in response to the increase in malicious cyber activity during the pandemic. It also called for all countries to immediately cease any cyber activity inconsistent with these international obligations.

Potential for malicious acts in cyberspace to threaten Australia's economic and strategic objectives

In its 2016 Defence White Paper, the Australian Government's Department of Defence identified that increasing security threats in cyberspace would be a key driver in shaping Australia's security environment over the next two decades.[77] Of this evolving threat, the Defence White Paper stated:

> "*The cyber threat to Australia is growing. Cyber attacks are a real and present threat to the ADF's warfighting ability as well as to other government agencies and other sectors of Australia's economy and critical infrastructure*".[78]

Malicious acts in cyberspace have shown the potential to perpetrate a very wide range of conduct, which may directly or indirectly threaten Australia's ability to achieve its economic and strategic objectives.

Australia has sought to safeguard itself against cyber attacks that include unauthorised access, modification or impairment of data.[79] These legislative changes allowed Australia to accede to the Convention on Cybercrime, which aims to harmonise national laws with respect to cybercrime.[80] However, as the recent spate of cyber incidents have demonstrated, this legislation on its own will not provide complete protection.

Economic objectives

The internet based economy provides plenty of economic opportunities, and Australians have been quick to take advantage of such opportunities. According to the Department of Home Affairs, the internet based economy contributed $79 billion or 5.1% of GDP to the Australian economy in 2014.[81] This number is expected to grow to $139 billion by 2020.[82] The number may further increase given the shift of both work and business online during the pandemic.

However, malicious actors have also been quick to exploit these opportunities. Almost one in three Australians were victims of cybercrime in 2018.[83] Cyber incidences are estimated to cost Australian businesses up to $29

---

[76] Department of Foreign Affairs and Trade & Australian Cyber Security Centre, 'Unacceptable Malicious Cyber Activity' (Joint Statement, 20 May 2020) <https://www.cyber.gov.au/news/unacceptable-malicious-cyber-activity>.
[77] Department of Defence, *2016 Defence White Paper*, February 2016.
[78] Ibid 16.
[79] See, e.g., *Criminal Code Act 1995* (Cth) pt 10.7 div 477.
[80] 'Australia: accession to Budapest Convention', *Council of Europe* (Web Page, 30 November 2012) <https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/australia-accession-to-budapest-convention?inheritRedirect=false>.
[81] 'Cyber Landscape', *Department of Home Affairs* (Web Page) <https://cybersecuritystrategy.homeaffairs.gov.au/cyber-landscape>.
[82] Ibid.
[83] National Cyber Resilience: Is Australia ready for a computer COVID-19?', *Tim Watts*, 15 May 2020, 4 <https://www.timwatts.net.au/media/186428/ncr_discussion_paper.pdf>.

billion per year.[84] The Australia Cyber Security Centre (**ACSC**) has seen a significant increase in COVID-19 themed malicious cyber activity in Australia since March 2020.[85]

Additionally, cyber attacks can harm an economy in a number of other ways. These include cyber attacks against our country's financial institutions, such as banks and stock markets. Though such attacks have yet to occur in Australia, they have occurred in other countries. For example, in 2011, the Hong Kong stock exchange was suspended after it was the target of a cyber attack.[86] In another example, in 2016, hackers attempted to transfer around US$1 billion from the Federal Reserve Bank of New York account belonging to Bangladesh Bank, Bangladesh's central bank. The hackers were successful in transferring around US$81 million out of the account.[87]

This shows that whilst malicious cyber activity is having a sizeable impact on the Australian economy, there is a lot of room for that impact to worsen and damage Australia's ability to pursue its economic objectives.

Strategic objectives

Part of Australia's national security objectives during the pandemic have focused on curbing the spread of COVID-19 as well as to find a safe and effective way to prevent and treat COVID-19. These objectives have been a common goal of governments worldwide. However, the objectives have come under attack by malicious actors online.

In Australia, the transition of key staff of critical infrastructure providers to working remotely during the pandemic has increased the risk that these critical infrastructure facilities may become potential targets of cyber attacks.[88] Australian health sector organisations and COVID-19 essential services have already been targeted by malicious actors online.[89]

The increase in attacks on critical or COVID-19 related organisations has also occurred overseas. For example, the United Kingdom's National Cyber Security Centre and the United States' Cybersecurity and Infrastructure Security Agency issued a joint advisory about an increase in cyber campaigns targeting healthcare organisations in both countries.[90] Since then the United States' Federal Bureau of Investigations has issued a statement stating that it was investigating cyber attacks on COVID-19 research organisations which were linked to Chinese-affiliated cyber actors.[91]

---

[84] Department of Home Affairs, *Australia's 2020 Cyber Security Strategy – A Call for Views*, 5 September 2019, 4 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf>.
[85] 'Safeguarding Australia's Critical Infrastructure from Cyber Attack', *Australian Cyber Security Centre* (Web Page, 22 May 2020) <https://www.cyber.gov.au/news/safeguarding-australias-critical-infrastructure-from-cyber-attack>.
[86] 'Hong Kong share trading hit by hackers, *British Broadcasting Corporation* (online, 11 August 2011) <https://www.bbc.com/news/technology-14489077>.
[87] Michael Corkery, 'Hackers' $81 Million Sneak Attack on World Banking', *The New York Times* (online, 30 April 2016) <https://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html>.
[88] 'Threat update: COVID-19 malicious cyber activity', *Australian Cyber Security Centre* (Web Page, 27 March 2020) <https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity>.
[89] 'Advisory 2020-009: Advanced Persistent Threat (APT) actors targeting Australian health sector organisations and COVID-19 essential services', *Australian Cyber Security Centre* (Web Page, 8 May 2020) <https://www.cyber.gov.au/threats/advisory-2020-009-advanced-persistent-threat-apt-actors-targeting-australian-health-sector-organisations-and-covid-19-essential-services>.
[90] National Cyber Security Centre, 'Cyber warning issued for key healthcare organisations in UK and USA' (Joint Advisory, 5 May 2020) <https://www.ncsc.gov.uk/news/apt-groups-target-healthcare-essential-services-advisory>.
[91] Federal Bureau of Investigations, 'People's Republic of China (PRC) Targeting of COVID-19 Research Organizations' (Press Release, 13 May 2020) <https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations>.

Cyber attacks also have the capacity to threaten or damage Australia's broader strategic objectives. In its comments on the initial "Pre-draft" of a report by the OEWG, the Department of Foreign Affairs and Trade considered that the OEWG's statement that the "*use of ICTs in future conflict is becoming more likely*" should be revised to state that it is "*likely*".[92] Past cyber attacks which appear to have targeted information or systems involved in Australia's pursuit of its strategic objectives include:

(i) installation of malicious software on the Australian Bureau of Meteorology's computer system in order to steal sensitive documents and compromise other government networks in 2016;[93]

(ii) infiltration of malicious software into the parliamentary computer network in 2019;[94] and

(iii) hacking of the Australian National University's computer systems in order to access 19 years' worth of personal information of staff and students.[95]

Australia's governmental agencies are also ill equipped to fend off malicious cyber activity. In 2013, the Australian Signals Directorate (**ASD**) made it mandatory for all non-corporate Commonwealth entities to implement four strategies to mitigate cybersecurity incidents.[96] In March 2020, the ACSC produced a report assessing the Commonwealth's cybersecurity posture in 2019.[97] The report concluded that in its assessment of 25 Commonwealth entities, none had fully implemented the four mandated strategies.[98]

Australia's cyber resilience must be improved

Both academic and governmental experts have found that Australia's cyber resilience is inadequate. In 2018, former head of ASIO, David Irvine, said of Australia's cyber resilience:

> "*Australia's national capacity to counter threats and criminal activity using cyber investigative tools is relatively weak, uncoordinated, and dispersed across a range of agencies in both Commonwealth and state jurisdictions*".[99]

Similarly, a report completed by the National Security College at the Australian National University in June 2019 found that Australia is ill prepared for a cyber conflict. The report was commissioned by the Department

---

[92] Department of Foreign Affairs and Trade, *Australia's comments on the Initial "Pre-draft" of the report of the UN Open Ended Working Group in the field of information and telecommunications in the context of international security (OEWG)*, 16 April 2020, 2 <https://www.dfat.gov.au/sites/default/files/australias-response-to-the-oewg-pre-draft-report-april-2020.pdf>.
[93] Andrew Greene, 'Bureau of Meteorology hacked by foreign spies in massive malware attack, report shows', *Australian Broadcasting Corporation* (online, 12 October 2016) <https://www.abc.net.au/news/2016-10-12/bureau-of-meteorology-bom-cyber-hacked-by-foreign-spies/7923770>.
[94] Amy Remeikis, 'Australian security services investigate attempted cyber attack on parliament', *The Guardian* (online, 8 February 2019) <https://www.theguardian.com/australia-news/2019/feb/08/asio-australian-security-services-hack-data-breach-investigate-attempted-cyber-attack-parliament>.
[95] Stephanie Borys, 'The ANU hack came down to a single email – here's what we know', *Australian Broadcasting Corporation* (online, 2 October 2019) <https://www.abc.net.au/news/2019-10-02/the-sophisticated-anu-hack-that-compromised-private-details/11566540>.
[96] National Cyber Resilience: Is Australia ready for a computer COVID-19?', *Tim Watts*, 15 May 2020, 5 <https://www.timwatts.net.au/media/186428/ncr_discussion_paper.pdf>.
[97] Australian Cyber Security Centre, *The Commonwealth Cyber Security Posture in 2019*, March 2020 <https://www.cyber.gov.au/sites/default/files/2020-04/Commonwealth-Cyber-Security-Posture-2019.pdf>.
[98] Ibid 10.
[99] Andrew Greene, 'Australia's cyber defences 'relatively weak, uncoordinated', former ASIO boss David Irvine warns', *Australian Broadcasting Corporation* (online, 19 January 2018) <https://www.abc.net.au/news/2018-01-19/australias-cyber-defences-relatively-weak-irvine-warns/9341342>.

of Defence and included input from at least 17 senior officials.[100] Professor Rory Medcalf, Head of the National Security College, stated that:

> "*We plotted out plausible futures just a few years from now to look at whether our systems could in any way stand up to the kinds of cyber attacks that an actor like China, Russia, North Korea or maybe even organised crime could throw at Australia … The report found that Australia is certainly underprepared, in some ways unprepared, for full-scale cyber attack*" (emphasis added).[101]

As such, the Committee considers it important that the Australian Government focus on implementing measures to protect Australia from these increasingly likely threats.

Recommendations to bolster Australia's cyber resilience

The Committee welcomes the release of the 2020 Defence Strategic Update, detailing the Australian Government's adjustments to the plans in the 2016 Defence White Paper. These changes include strengthening Australia's capability to respond to "grey zone"[102] activities, including cyber capabilities, electronic warfare and information operations.[103] Whilst these changes focus on building offensive capabilities, there is a lack of focus on also building defensive or protective capabilities to increase Australia's cyber resilience in a balanced manner. In order the increase Australia's cyber resilience against cyber threats, the Committee makes three recommendations below.

Legislation or regulations for a minimum standard of cybersecurity

The growing number of cyber attacks against Australian businesses highlights the need for Australia to develop a better culture around cybersecurity. In particular, the transition to working from home has increased vulnerability to these attacks, whilst the increase of cyber attacks during the pandemic indicates that malicious actors are exploiting these vulnerabilities.[104]

In order to increase the protection of Australian businesses from cyber attacks, the Australian Government should consider enacting laws or regulations which set a minimum standard of cybersecurity measures that Australian businesses are required to implement. Whilst specific laws already regulate how critical infrastructure providers must secure their assets (for example under the Australian Privacy Principles contained in the *Privacy Act 1988* (Cth)), it is clear that further laws or regulations should be considered.

Cybersecurity requirements for government entities

As discussed above, cyber attacks have already successfully infiltrated our governmental agencies in the past. Those attacks ranged from stealing sensitive information to infiltrating other networks. Furthermore, other countries' experiences show that these attacks have the potential to be far more wide-reaching in their capacity to undermine economic and strategic objectives.

Following the 2019 report by the ACSC which found that none of the ASD's four mandatory cybersecurity strategies had been implemented by the Commonwealth government agencies studied, the Committee

---

[100] Sean Rubinsztein-Dunlop, 'Defence has imagined modern warfare and Australia is not prepared' (online, 15 May 2020) <https://www.abc.net.au/news/2020-05-15/australia-unprepared-for-security-threats-warns-review/12248332>.
[101] Ibid.
[102] The 2020 Defence Strategy Update uses the term "grey zone" to describe activities designed to coerce countries in ways that seek to avoid military conflict. See Department of Defence, *2020 Defence Strategic Update*, 1 July 2020, 12.
[103] Ibid 33.
[104] See 'Protecting small business against cyber attacks during COVID-19', *Australian Cyber Security Centre* (Web Page, 7 April 2020) <https://www.cyber.gov.au/news/protecting-small-business-against-cyber-attacks-during-covid-19>.

recommends that the Australian Government quickly act to implement those strategies in order to stem these critical vulnerabilities. Whilst the strategies are not mandatory for state and territory agencies, such agencies should consider implementation to ensure effective security of government entities across the nation.

Ministerial portfolio for cyber affairs

Following the implementation of the Australian Government's 2016 Cyber Security Strategy, the Australian Government created a dedicated ministerial portfolio for cyber affairs as well as appointing an "Australian Cyber Ambassador" (now known as the Australian Ambassador for Cyber Affairs).[105] In 2018, the ministerial position was scrapped, whilst the Australian Ambassador for Cyber Affairs position remains. The Australian Ambassador for Cyber Affairs currently leads the Australian Government's international engagement to advance and protect Australia's interests in the internet and cyberspace.[106]

However, without a dedicated ministerial portfolio on cyber affairs, there cannot be an effective coordination and implementation of cyber policies within Australia. This lack of coordination of Australia's domestic cyber policies may have contributed to its vulnerability to cyber threats. In order to oversee the implementation of relevant recommendations, as well as coordinate Australia's cyber policy, the Committee recommends that the Australian Government create or reinstate a dedicated ministerial portfolio for cyber affairs.

Concluding Comments

NSW Young Lawyers and the Committee thank you for the opportunity to make this submission. If you have any queries or require further submissions please contact the undersigned at your convenience.

Contact:

David Edney

President

NSW Young Lawyers

Email: president@younglawyers.com.au

Alternate Contact:

Katlyn Kraus

Chair

NSW Young Lawyers International Law Committee

Email: intlaw.chair@younglawyers.com.au

[105] Australian Government, *Australia's Cyber Security Strategy*, April 2016, 3-8 <https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf>.
[106] 'Australian Ambassador for Cyber Affairs', *Department of Foreign Affairs and Trade* (Web Page) <https://www.dfat.gov.au/about-us/our-people/homs/Pages/ambassador-for-cyber-affairs>.