CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

COMMENTS TO THE AUSTRALIAN DEPARTMENT OF FOREIGN AFFAIRS AND TRADE'S PUBLIC CONSULTATION ON RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE IN THE CONTEXT OF INTERNATIONAL SECURITY AT THE UNITED NATIONS

AUTHORED BY

Gunjan Chawla, Programme Manager, Technology and National Security, Centre for Communication Governance at National Law University Delhi

and

Sharngan Aravindakshan, Programme Officer, Technology and National Security, Centre for Communication Governance at National Law University Delhi

REVIEW AND EDITING ASSISTANCE

Sarvjeet Singh, Executive Director, Centre for Communication Governance at National Law University Delhi

Contact:

e: sarvjeet.singh@nludelhi.ac.in; gunjan.chawla@nludelhi.ac.in

m: +91-9990232298

TERMS OF REFERENCE

The Australian Department of Foreign Affairs and Trade (DFAT) in November 2019, called for submissions to inform Australia's engagement in two United Nations (UN) processes on responsible state behaviour in cyberspace.

In December 2018, the United National General Assembly (UNGA) established two processes: an inaugural *Open Ended Working Group on developments in the field of information and telecommunications in the context of international security* (OEWG) (A/Res/73/27); and, a sixth *Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security* (GGE) (A/Res/73/266).

The Centre for Communication Governance at National Law University Delhi (CCG) is an academic research centre that seeks to embed good governance within communication law and policy through rigorous academic research and capacity building. We are dedicated to working on information law and policy in India, with a focus on issues that arise at the intersection of national security law and policy, and existing and emerging technologies.

We thank the DFAT for inviting comments to inform Australia's engagement in the evolution of norms of responsible State behavior in cyberspace. We agree with the DFAT's view that the GGE and OEWG processes present an important opportunity to promote a peaceful and stable online environment and enhance international security. Additionally, as strategic partners since 2009, Australia and India enjoy strong political, economic and community ties.[1] Accordingly, through the submission of these comments, we hope to meaningfully contribute to the existing law and policy making underway at the international level in an open and transparent manner, with a view to strengthening bilateral relations between the India and Australia.

[1] Australian Government, Department of Foreign Affairs and Trade, India Country Brief, https://dfat.gov.au/geo/india/Pages/india-country-brief.aspx.

This submission responds to three of six questions indicated in the DFAT's Call for Comments. These are, namely:

2. Are there any specific areas of the Framework for Responsible State Behaviour in Cyberspace (international law, norms, confidence building measures and capacity building) that, from your perspective, should be further developed in the OEWG/GGE? If so, how would you like to see these areas addressed in any OEWG and/or GGE report(s)?

4. The mandate of the GGE invites members to annex to the GGE report "*national contributions...on the subject of how international law applies to the use of information and communications technologies by States*". Through the International Cyber Engagement Strategy, Australia has published its positions on the application of international law to cyberspace in 2017 and 2019. Are there any relevant areas of international law that that, from your perspective, should be addressed in any Australian contribution to the international law annex to the GGE report? If so, how would you like to see these areas addressed?

5. Another key Australian objective is for any report of the OEWG and/or GGE to make recommendations on better coordinating global cyber capacity building. We welcome suggestions on how coordination of global cyber capacity building might be improved, as well as how you would like this to be addressed in any OEWG and/or GGE report(s).

A. Are there any specific areas of the Framework for Responsible State Behaviour in Cyberspace (international law, norms, confidence building measures and capacity building) that, from your perspective, should be further developed in the OEWG/GGE? If so, how would you like to see these areas addressed in any OEWG and/or GGE report(s)?

Both India and Australia's engagement in the development of norms for responsible state behaviour in cyberspace is chiefly in two forums in the United Nations—the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security ("**GGE**") and the Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security ("**OEWG**").

Australia has previously been a member of the GGE in the 2012-13 and 2016-17 sessions and is also a member in the 2019-2021 session that is currently underway. India has previously been a member in all the sessions barring the 2014-15 session and is also a member of the current 2019-2021 session. Both India and Australia are members of the OEWG.

The Centre for Communication Governance at National Law University Delhi (CCG) notes that Australia has affirmed the GGE's 2013 and 2015 Reports acknowledging and confirming the applicability of international law to cyberspace.[2] CCG further notes that Australia's submission to the OEWG ("**Australia's OEWG Position Paper**") has also reaffirmed that it is "guided in its use of ICTs by the UNGGE Reports".[3]

Australia's OEWG Position Paper makes it clear that in Australia's view, the OEWG mainly serves as enabling other states particularly those that were not part of the GGE process to better understand the existing normative framework for responsible

[2] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Annex A: Australia's Position On How International Law Applies To State Conduct In Cyberspace*, *Australia's International Cyber Engagement Strategy*, October 2017, at https://www.un.org/disarmament/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf.

[3] Ibid, Para 2.3.

behaviour that was developed by the GGE, as well as to define the capacity building needs of states and other stakeholders in order to implement existing norms and confidence building measures (CBMs).[4]

Australia's OEWG Position Paper states that both the OEWG and the UNGGE should "build on the UNGGE Reports which it terms as the product of "effective work and consensus".[5] It also states that the OEWG should harness its membership of all 193 states in the UN to (a) seek views on existing and emerging threats, (b) seek an update from all member states on steps taken to implement the 2015 UNGGE report and any barriers to the same and (c) make recommendations on how best to coordinate capacity building to implement the 2015 UNGGE report.[6]

It leaves to the UNGGE to determine (a) how international law applies to cyberspace, (b) develop practical guidance to implement the 11 norms for responsible state behaviour identified in the 2015 UNGGE Report as well as (c) practical guidance to implement the CBMs identified in the 2015 UNGGE Report.[7]

Emphasizing on the need for the OEWG and GGE processes to be complementary to each other[8], Australia further states that the practical guidance from the UNGGE report

[4] Digital Watch Observatory, *Roles of the GGE and the OEWG*, at https://dig.watch/processes/un-gge.

[5] Commonwealth of Australia, Australian Mission to the United Nations, *Australian Paper – Open Ended Working Group On Developments In The Field Of Information And Telecommunications In The Context Of International Security*, September 2019, Para 4.1, at https://www.un.org/disarmament/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf.

[6] Commonwealth of Australia, Australian Mission to the United Nations, *Australian Paper – Open Ended Working Group On Developments In The Field Of Information And Telecommunications In The Context Of International Security*, September 2019, Para 4.4, at https://www.un.org/disarmament/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf.

[7] Commonwealth of Australia, Australian Mission to the United Nations, *Australian Paper – Open Ended Working Group On Developments In The Field Of Information And Telecommunications In The Context Of International Security*, September 2019, Para 4.5, at https://www.un.org/disarmament/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf.

[8] Commonwealth of Australia, Australian Mission to the United Nations, *Australian Paper – Open Ended Working Group On Developments In The Field Of Information And Telecommunications In The Context Of International Security*, September 2019, Para 4.6, at https://www.un.org/disarmament/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf.

could be drawn upon by states seeking to address gaps in implementation identified in the OEWG process. In Australia's view, this approach "respects the independent and separate mandates of the groups, while also encouraging complementary and mutually reinforcing outcomes."[9]

As far as India is concerned, it voted in favour of both the UNGGE as well as the OEWG. It must be noted that India has also affirmed its commitment to the UNGGE in its bilateral talks with other countries such as Russia[10] and also Australia.[11]

CCG believes that building consensus on the question of *how international law apples in cyberspace* is of utmost importance to encourage peace and stability in this realm. We suggest that interpretations of international law and the evolution of our understanding of the modalities of application of international law in cyberspace must be geared towards (1) discouraging the use of cyber operations by States for coercive policies through the stockpiling, proliferation and deployment of cyber weapons, (2) preventing the outbreak of hostilities between States in cyberspace and (3) where such hostilities have been resorted to, the international legal framework made applicable must encourage the adoption and execution of de-escalatory measures and policies to restore peace and stability in cyberspace. The following part of this submission focusses on one substantive issue that has a far-reaching impact on the achievement of these goals.

[9] Ibid.

[10] Staff Reporter, *Russia And India Confirm Readiness To Cooperate In Cyber Security*, Tass Russian News Agency, February 2018, https://tass.com/world/990504.

[11] Government of India, Ministry of External Affairs, *Joint Statement of Australia-India Cyber Policy Dialogue*, July 2017, at https://www.mea.gov.in/bilateral-documents.htm?dtl/28618/Joint_Statement_of_AustraliaIndia_Cyber_Policy_Dialogue.

B. The mandate of the GGE invites members to annex to the GGE report "*national contributions...on the subject of how international law applies to the use of information and communications technologies by States*". Through the International Cyber Engagement Strategy, Australia has published its positions on the application of international law to cyberspace in 2017 and 2019. Are there any relevant areas of international law that that, from your perspective, should be addressed in any Australian contribution to the international law annex to the GGE report? If so, how would you like to see these areas addressed?

CCG notes that Australia has affirmed the GGE's 2013 and 2015 Reports which acknowledge and confirm the applicability of international law to cyberspace[12] and also welcomes Australia's articulation of its position on how existing international law applies to cyberspace.[13]

CCG is aware that Australia's position is that international humanitarian law (IHL) (including the principles of humanity, necessity, proportionality and distinction) applies to cyber operations within an armed conflict.[14] This is in line with the view of the International Committee of the Red Cross ("**ICRC**"), which has also clarified that international humanitarian law limits (military) cyber capabilities that qualify as weapons, just as it limits the use of any other weapon, means and methods of warfare in an armed conflict, whether new or old.[15]

---

[12] Commonwealth of Australia, Australian Mission to the United Nations, *Australian Paper – Open Ended Working Group On Developments In The Field Of Information And Telecommunications In The Context Of International Security*, September 2019, Para 2.3, at https://www.un.org/disarmament/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf.

[13] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Annex A: Australia's Position On How International Law Applies To State Conduct In Cyberspace*, *Australia's International Cyber Engagement Strategy*, October 2017, p. 90, at https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/annexes.html#Annex-A.

[14] Ibid, Para 2.

[15] ICRC Position Paper, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, at https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

However, the issue what constitutes “cyber capabilities that qualify as weapons” (or ‘cyber weapons’) needs a deeper consideration and analysis. This is essential to ensure that the meaning supplied to international law concepts such as sovereignty, non-intervention, use of force and especially, ‘armed attack’ through the evolution of customary international law is not denuded to the detriment of those nations that are struggling to bridge the digital divide and acquire cyber capabilities for peaceful purposes, including and especially, greater integration with a globally networked economy.

To this end, CCG seeks to bring to the Australian Government’s certain interpretations of the law of armed that are in clear opposition to the interpretation of the law by the ICRC. In a recent paper, a principal author of the Tallinn Manual 1.0 and Tallinn Manual 2.0, in a reconsideration of his opinion expressed in these Manuals, argued that cyber capabilities cannot meet the definition of a weapon or means of warfare, but that cyber operations may qualify as methods of warfare.[16] Such an interpretation permits ‘cyber weapons’ to circumvent at least three obligations under IHL, including the requirement for legal review of weapons under Article 36 of the First Additional Protocol to the Geneva Conventions and taking precautions in attack.[17] Most importantly, the argument that cyber weapons cannot be classified as munitions also has the consequence of depriving neutral States of their sovereign right to refuse permission of their transportation (or in this case, transmission of weaponised cyber capabilities) through their territory.[18] In our view, such interpretations encourage the use of escalatory approaches and are more likely to catalyse conflict in cyberspace, than ensure peace and stability.

If the law presumes in line with such interpretations that cyber capabilities are neither weapons nor munitions, it will be very difficult, if not impossible, to classify any

[16] Jeffrey T Biller and Michael N Schmitt, *Classification of Cyber Capabilities and Operations as Weapons, Means or Methods of Warfare,* 95 INT‟L L. STUD. 179 (2019) at p. 219, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2462&context=ils.

[17] Ibid.

[18] Ibid.

instances of cyber attacks as “armed attacks”. As a direct consequence, those States that are victimized by the deployment of cyber weapons that may otherwise be illegal in international law, will not be able to legally exercise their inherent right of self-defence. This may engender a gradual erosion of the *de facto* sovereignty of many States, while retaining a *de jure* principle of sovereign equality in international law.

CCG recommends that this issue of defining what precisely constitutes ‘cyber weapons’ be taken up for further research and study, as well as be raised at both the GGE and the OEWG for serious consideration by nation states and relevant stakeholders. It is also relevant to highlight that CCG has made similar recommendations to the Indian Government in its Comments to the National Security Council Secretariat on India’s National Cyber Security Strategy 2020.[19]

[19] *Comments to the National Security Council Secretariat on the National Cyber Security Strategy 2020 (NCSS 2020)*, Centre for Communication Governance at National Law University Delhi, January 10, 2020, p. 24., https://drive.google.com/file/d/14XfyXu-5sAPgzAmEaKE78vphTTfH_Y5s/view.

C. Another key Australian objective is for any report of the OEWG and/or GGE to make recommendations on better coordinating global cyber capacity building. We welcome suggestions on how coordination of global cyber capacity building might be improved, as well as how you would like this to be addressed in any OEWG and/or GGE report(s).

CCG notes that India and Australia are strong partners in the Asia-Pacific region, with their relationship underpinned by shared commonalities such as pluralistic democracies, commonwealth traditions, expanding economic engagement and increasing high level interaction.[20] India's position in the Indian Ocean and Australia's position in the Pacific Ocean add strategic value to a partnership between the two nations.

In this regard, CCG seeks to highlight that this strong existing relationship between the two countries can be leveraged to promote cyber capacity building, thereby contributing to stability in cyberspace, at both bilateral and multilateral levels of engagement. Accordingly, we restrict the scope of our comments to addressing the question of coordinating cyber capacity building between India and Australia, in light of previous agreements and potential avenues for future cooperation in (1) bilateral and (2) regional and multilateral fora.

1. Bilateral Cooperation

Apart from their common commitments to promoting stability in cyberspace through multilateral and multi-stakeholder forums such as the GGE and the OEWG respectively, India and Australia have several ongoing bilateral engagements that are relevant to increasing and improving cyber capacity in the two nations. CCG has identified certain areas in the cyber domain as possible areas of bilateral cooperation between the two countries.

[20] Government of India, Ministry of External Affairs, *India-Australia Bilateral Relations*, p. 1, at https://mea.gov.in/Portal/ForeignRelation/Australia_05_09_2017.pdf.

(a) National Security and Cyber Security Enhancement

The Framework for Security Cooperation between India and Australia ("Framework"), agreed upon by the two countries in 2014 provides scope for cyber cooperation. It reflects "the deepening and expanding security and defence engagement between India and Australia"[21], aims "to intensify cooperation and consultation between Australia and India in areas of mutual interest."[22]

Although it primarily serves as an umbrella arrangement for security and defence cooperation, its Action Plan identifies "exchanges on cyber policy and cooperation between CERT-India and CERT-Australia" as part of efforts to counter terrorism and transnational crimes.[23] This makes it uniquely suited to enhance cooperation in the cyber domain.

Other areas for cooperation identified by the Framework's Action Plan include defence policy planning and coordination, counter-terrorism and other transnational crimes, border protection, coast guard and customs, disarmament, non-proliferation, civil nuclear energy and maritime security, disaster management and peacekeeping and cooperation in regional and multilateral fora.[24] The progress under this Action Plan is to be reviewed through institutional arrangements including the Foreign Ministers' Framework Dialogue and the Defence Ministers' Meeting.[25]

Given its wide ambit, CCG recommends that maximum engagement on issues in the cyber domain take place under the aegis of the Framework. Further, the India-Australia

[21] Government of India, Ministry of External Affairs, 'Framework for Security Cooperation between India and Australia', November 18, 2014, at https://mea.gov.in/bilateral-documents.htm?dtl/24268/Framework_for_Security_Cooperation_between_India_and_Australia.

[22] Ibid.

[23] Ibid at Para 3(g).

[24] Ibid.

[25] Ibid.

Cyber Policy Dialogue, which flows from the Framework for Security Cooperation, is also highly significant.[26] It has so far had three iterations, which are detailed below:

i. The First Iteration (2015)

The first iteration of the India - Australia Cyber Policy Dialogue was held in New Delhi in August 2015.[27] CERT-India and CERT-Australia signed a framework for operational cooperation on cyber security to promote greater cooperation in exchanging information on cyber threats and in responding to incidents.[28] The two countries were also able to identify opportunities to work together to exchange information on cybercrime and on law enforcement measures.[29] The two sides also acknowledged the work of regional bodies including the ASEAN Regional Forum on confidence building and the Asia-Pacific CERT community in supporting the development of regional CERT capacity.[30]

The participating agencies from India included the Joint Secretary (Policy Planning, Counter Terrorism and Global Cyber Issues) to the Ministry of External Affairs and representatives from CERT-India, the Ministry of Home Affairs, the National Security Council Secretariat, the Ministry of Defence, the Central Bureau of Investigation, the Department of Telecommunications as well as the Ministry of External Affairs.[31]

The participating agencies from Australia included the Assistant Secretary (Strategic Issues and Intelligence Branch) to the Department of Foreign Affairs and Trade and representatives from the Department of the Prime Minister and Cabinet, the Department

[26] Government of India, Ministry of External Affairs, *Joint Statement: Inaugural India-Australia Cyber Policy Dialogue*, August 31, 2015, at https://mea.gov.in/bilateral-documents.htm?dtl/25774/Joint+Statement+Inaugural+IndiaAustralia+Cyber+Policy+Dialogue.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Ibid.

of Communications, the Attorney-General's Department (CERT-Australia), and the Australian Federal Police.[32]

ii. The Second Iteration (2017)

The second iteration of the India - Australia Cyber Policy Dialogue was held in Canberra in July 2017.[33]

In this session, both countries reaffirmed (a) their commitment to an open, free, secure, stable, peaceful and accessible cyberspace enabling economic growth and innovation, (b) their commitment to act in accordance with the UNGGE's previous reports and, in particular, the 11 voluntary norms of state behaviour set out in the 2015 report, (c) the applicability of the Charter of the United Nations and existing international law to cyberspace as well as (d) which identified Points of Contact on various issues of mutual interest in the area of Cyberspace.[34] Both countries also affirmed the multi-stakeholder approach to norm building in cyberspace.[35]

The participating agencies from India included the Joint Secretary for Cyber Diplomacy from the Ministry of External Affairs, India's High Commissioner to Australia, as well as representatives from the Ministry of Home Affairs and India's National Security Council Secretariat.[36]

The participating agencies from Australia included Australia's Ambassador for Cyber Affairs and representatives from the Department of the Prime Minister and Cabinet, the Department of Communications and the Arts, and Australian Cyber Security Centre agencies (the Attorney-General's Department, including CERT Australia; the

[32] Ibid.

[33] Government of India, Ministry of External Affairs, *Joint Statement of Australia-India Cyber Policy Dialogue*, July 2017, at https://www.mea.gov.in/bilateral-documents.htm?dtl/28618/Joint_Statement_of_AustraliaIndia_Cyber_Policy_Dialogue.

[34] Ibid.

[35] Ibid.

[36] Ibid.

Department of Defence; the Australian Federal Police; and the Australian Criminal Intelligence Commission).[37]

iii. The Third Iteration (2019)

The third session of the India-Australia Cyber Policy Dialogue was held in New Delhi in September 2019.[38] This session saw both countries:

(a) Note their sustained concern with the increasing frequency and seriousness of cyber security incidents that have the potential to impact the national and economic security of respective countries and undermine international peace and security[39];

(b) Reaffirm their commitment to 2013 and 2015 GGE reports[40];

(c) Resolve to further enhance practical cyber security policy cooperation through reciprocal expert exchanges to share information on cyber security policy development, telecommunications, legislative developments, and engagement with the private sector (India and Australia agreed to commence in-country expert exchanges with Australia offering to host the first interaction)[41];

(d) Agree to work towards the establishment of a Joint Working Group on Cyber Security Cooperation and to commence negotiations for a Framework Agreement on Cyber Cooperation and acknowledge the importance of the Internet of Things ("**IoT**") and Security by Design.[42]

---

[37] Ibid.

[38] Government of India, Ministry of External Affairs, *3rd India-Australia Cyber Dialogue*, September 2019, at https://www.mea.gov.in/press-releases.htm?dtl/31794/3rd_IndiaAustralia_Cyber_Dialogue.

[39] Ibid.

[40] Ibid.

[41] Ibid.

[42] Ibid.

The participating agencies from India included Joint Secretary in charge of e-Governance, Information Technology and Cyber Diplomacy at the Indian Ministry of External Affairs as well as representatives from the National Security Council Secretariat, Ministry of Home Affairs, Ministry of Electronics and Information Technology, Department of Telecommunications, CERT-In and National Critical Information Infrastructure Protection Centre.[43]

The participating agencies form Australia included the Australian Ambassador for Cyber Affairs as well as representatives from the Department of Home Affairs, the Australian Signals Directorate's Australian Cyber Security Centre, and Australian Federal Police.[44]

CCG notes the successful completion of three editions of the India Australia Cyber Dialogue and hopes that both countries will continue to utilize this platform to engage meaningfully on matters of cybersecurity and cyber capacity building.

Separately, India and Australia are also part of the Quadrilateral Security Dialogue (QSD) which is a strategic dialogue between Japan, India, United States and Australia, initiated as a response to China's increasing economic and military power. After a period of dormancy between 2008 and 2016, the QSD was revived in 2017 and has met five times in since then.[45] It aims to promote a "free and open Indo-Pacific amid China's aggressive postures in the region". The QSD includes naval exercises and other joint operations. The QSD provides opportunities for transfer of cyber expertise and cooperation from a military perspective.

CCG also draws attention to the Comprehensive Economic Cooperation Agreement (CECA), currently being negotiated by both countries, which will provide greater market

[43] Ibid.

[44] Ibid.

[45] Dipanjan Roy Chaudhary, *India's fine balancing act with Quad and BRICS meet in New York*, The Economic Times, September 28, 2019, accessible at https://economictimes.indiatimes.com/news/defence/indias-fine-balancing-act-with-quad-and-brics-meet-in-new-york/articleshow/71338616.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

access to exporters of goods and services.[46] CCG is optimistic about the CECA's performance, and accordingly, we submit that issues pertaining to goods and services relevant to access and provision of products and services relevant for cybersecurity also be considered under it.

(b) Cyber Crime, Cyber Terrorism and Critical Infrastructure

CCG considers that cooperation on critical issues such as fighting cyber-crime, cyber terrorism and securing critical infrastructure can be pursued by both India and Australia through the Memorandum of Understanding for Combating International Terrorism and Transnational Organized Crime entered into by both nations in April 2017 ("**MoU on Terrorism**").[47]

CCG points out Paragraph 1(2)(o) of the MoU on Terrorism in this regard, which records the parties' agreement to cooperate in combating criminal acts, in particular, "cyber crimes and/or attack on critical infrastructure lying within the jurisdiction of [the two countries]".[48] Similarly, para 1(2)(a) records the countries' commitment to cooperate in combating terrorism and terrorism enabling capabilities including terrorism financing. CCG seeks to highlight these provisions specifically and the MoU generally for their potential for increased cooperation in these areas.

(c) Science and Technology Development and Transfer

CCG submits that earlier arrangements between India and Australia such as the Agreement on Cooperation in the Fields of Science and Technology, 1975, presented opportunities for building capabilities in cyberspace, in the form of technology transfers and contributions to scientific development. The Agreement has since expired (its term

[46] Government of India, Ministry of External Affairs, *India-Australia Bilateral Relations*, p. 3, accessible at https://mea.gov.in/Portal/ForeignRelation/Australia_05_09_2017.pdf.

[47] Government of India, Ministry of External Affairs, Memorandum of Understanding between the Government of the Republic of India and the Government of Australia on Cooperation in Combating International Terrorism and Transnational Organized Crime, at http://www.mea.gov.in/Portal/LegalTreatiesDoc/AU17B3005.pdf.

[48] Ibid, Para 1(2)(o).

was limited to one year), however, CCG hopes that both governments will consider reopening these avenues to promote cyber capacity building though cooperation in science and technology.

Ongoing cooperative efforts between the two nations in the cyber domain include Indian companies such as Tata Consultancy Services (TCS) participating in the Australian Government's Cyber Security Cooperative Research Centre, building innovation laboratories to foster cyber innovation and supporting Australian partners by providing access to its leading technology platforms.[49] Wipro, another India-based company, has set up a "Cyber Defence Centre" in Melbourne, which will reportedly offer protection from cyber-attacks to the organisations and will generate 100 new tech jobs for locals.[50] CCG appreciates such efforts and recommends that these measures be replicated and more such partnerships be built in the future to fully harness the benefits of both countries' expertise in the cyber domain.

Other initiatives such as the Indo-Australia Fund for Scientific and Technological Cooperation (currently ongoing) which act as platforms for bilateral collaboration in science and support collaborative, leading- edge research between scientists in India and Australia across a range of agreed priority areas[51], can prove equally beneficial to both nations by facilitating cutting edge research and development in emerging areas of cybersecurity, blockchain, cryptocurrency and artificial intelligence.

[49] Australian Government, Department of Foreign Affairs and Trade, *An India Economic Strategy to 2035. Navigating from Potential to Delivery- A Report to the Australian Government by Mr Peter N Varghese AO*, April 2018, p. 54, at https://dfat.gov.au/geo/india/ies/pdf/dfat-an-india-economic-strategy-to-2035.pdf.

[50] Staff Reporter, *Wipro To Establish Cyber Defence Centre In Melbourne*, The Economic Times, December 4, 2019, https://economictimes.indiatimes.com/news/defence/wipro-to-establish-cyber-defence-centre-in-melbourne/articleshow/72361893.cms?from=mdr.

[51] Government of India, Ministry of Science and Technology, Department of Science and Technology, Indo-Australia Fund for Scientific and Technological Cooperation (Indo-AISRF) Round 11, Call for Proposals- 2019, at https://dst.gov.in/sites/default/files/For%20Website%20DST-AISRF%20Call%20for%20proposals.pdf.

CCG also notes and appreciates the Australian Government's active interest in Indian cybersecurity, evidenced by the advisory issued by Australian Trade and Investment Commission to Australian cybersecurity firms to invest in the Indian market.[52]

Moreover, CCG also points to the presence of Indian diaspora in Australia that can be leveraged for development in cyber capacity, skilling and research. CCG understands that the Australian Government is already in the process of examining efforts to galvanize the Indian diaspora in this regard[53] and hopes such efforts fructify in mutual benefit to both nations. The Department of Foreign Affairs and Trade commissioned a report in this regard which identifies many areas relevant to the cyber domain, including tracking and improving retention of masters-and-above level Indian students in STEM courses in Australian universities[54] and notes other significant facts such as most Indian diaspora in Australia owning small and medium enterprises with potential for economic integration with India[55] and 'professional, technical and other services' constituting 30% of India's exports to Australia.[56]

CCG also notes and appreciates Australian efforts to cultivate the Indian diaspora community in Australia, evidenced by measures such as the announcement by the Victoria government of financial assistance of 3-million Australian dollars for an "infrastructure fund" meant to be used to renovate "Indian community facilities".[57]

---

[52] Government of Australia, Australian Trade and Investment Commission, *Insight – Bolstering India's Cyber Security Capabilities*, at https://www.austrade.gov.au/news/insights/insight-bolstering-india-s-cyber-security-capabilities.

[53] Australian Government, Department of Foreign Affairs and Trade, *An India Economic Strategy to 2035. Navigating from Potential to Delivery- A Report to the Australian Government by Mr Peter N Varghese AO*, April 2018, p. 357-373, at https://dfat.gov.au/geo/india/ies/pdf/dfat-an-india-economic-strategy-to-2035.pdf.

[54] Ibid, p. 368.

[55] Ibid, p. 357.

[56] Ibid, p. 370.

[57] Staff Report, *Australia's Victoria Govt Announces 3-Million Australian Dollar Assistance For Indian Diaspora*, The Economic Times, November 26, 2019, https://economictimes.indiatimes.com/nri/australias-victoria-govt-announces-3-million-australian-dollar-assistance-for-indian-diaspora/articleshow/72235432.cms?from=mdr.

(d) Education, Training and Research

In the field of education, training and research, India and Australia signed a Memorandum of Understanding (MoU) on 24 August 2015, with a view to encouraging the "development of cooperation between the educational institutions of the two countries based on their respective needs".[58] This MoU is due to expire this year[59], and CCG hopes that it will be renewed to ensure continued cooperation in the field of education, training and research, with additional provisions on training of cybersecurity professionals to meet anticipated shortages in both the countries' respective cyber workforce.

2. Regional and Multilateral Cooperation

India and Australia are both members of the following international regional fora:

(a) ASEAN Regional Forum;

(b) Commonwealth of Nations;

(c) G20 (areas- economic);

(d) East Asia Summit (areas - trade, energy);

The roles of the ASEAN Regional Forum in confidence building in the cyber domain and the Asia Pacific CERT Community on the development of regional CERT capacity have also been recognized in the India-Australia Cyber Dialogue.[60] CERT-In has also

[58] Memorandum of Understanding between the Government of the Republic of India and the Government of Australia on Cooperation in the Fields of Education, Training and Research dated 24 August 2015, https://mhrd.gov.in/sites/upload_files/mhrd/files/upload_document/EEP/AustraliaMOU.pdf.

[59] Article 8, Memorandum of Understanding between the Government of the Republic of India and the Government of Australia on Cooperation in the Fields of Education, Training and Research dated 24 August 2015.

[60] Government of India, Ministry of External Affairs, *Joint Statement: Inaugural India-Australia Cyber Policy Dialogue*, August 2015, at https://mea.gov.in/bilateral-documents.htm?dtl/25774/Joint+Statement+Inaugural+IndiaAustralia+Cyber+Policy+Dialogue.

participated in drills, exercises and other activities as part of the APCERT community, showcasing the importance of Asia-Pacific cyber cooperation to India.[61]

CCG also notes and appreciates the Australian Government's support to India's membership in the Asia Pacific Economic Cooperation ("**APEC**").[62] We hope that these additional engagements will provide more opportunities for mutual cooperation on cyber issues, especially capacity building.

[61] Annual Report (2018), Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & Information Technology, Government of India (CERT-In), p. 11-13, at https://www.cert-in.org.in.

[62] Australian Government, Department of Foreign Affairs and Trade, Government Response to An India Economic Strategy to 2035, November 22, 2018, at https://dfat.gov.au/about-us/publications/Pages/government-response-india-economic-strategy.aspx.