Australia Cybersecurity and Critical Technology International Engagement Strategy (CCTIES) Consultation

Dear Ambassador Feakin,

Microsoft welcomes the opportunity to provide input into the update of Australia's Cybersecurity and Critical Technology International Engagement Strategy (CCTIES). Cybersecurity plays a key role in a number of topics central to both our digital and analogue environments, including international peace and stability, cybercrime, trade, human rights and democracy. It is also a challenge that transcends territorial boundaries, and we were pleased to see Australia embrace that fact early with the development of the first international cybersecurity strategy, and by establishing it firmly as a priority in its foreign policy. Its implementation has wielded clear results, securing Australia's objectives in international discussions, but also demonstrably increased cybersecurity resilience in countries benefiting from its capacity building initiatives.

Nevertheless, much has changed since the initial International Cyber Engagement Strategy was unveiled in 2017. While the pace of adoption of new technologies has been increasing for some time, and geopolitical shifts have likewise been occurring, the world was also suddenly and dramatically altered this year by the pandemic in ways that have accelerated both of those trends. In a matter of weeks, the importance of technology for work and production, learning and education, communication and diplomacy, and healthcare provision and research was laid bare. The significance of strong established relationships and allies to ensure supply chains remain uninterrupted was similarly underlined.

At the same time as the criticality of technology is adding a layer of complexity to security, governments continue to invest in greater offensive capabilities in cyberspace, and nation-state attacks on civilians are on the rise. It is therefore more important than ever that states invest in the international aspects of cybersecurity, and work together to address the growing range of cybersecurity threats. Given the speed of development in the technology industry, each country also needs to look across the horizon in addition to addressing the challenges here today. To that end, we particularly welcome the approach taken by the Australian government here and hope that our contributions prove useful.

In our response we highlight:

- How **critical technologies** will shape the geopolitical environment in this decade and the opportunities and risks of these technologies to Australia and the Indo-Pacific;
- **Proposed objectives** for the CCTIES;
- The **role of multistakeholder cooperation** in international cybersecurity strategy.

We expand on these recommendations below and remain available for further contributions and discussion.

What should Australia's key international cybersecurity and critical technology objectives be? What are the values and principles Australia should promote regarding cyberspace and critical technology?

We are at a critical juncture for international cybersecurity, and it is important that governments clearly make a case for a free, open, and secure internet. This is critical not only to ensure that we are able to continue to enjoy the many benefits cyberspace has afforded us, but also to ensure that these opportunities are extended to an ever greater number of people as global connectivity is strengthened.

These objectives were of course already highlighted in the original 2017 strategy and pursued by the Australian government since. We recommend a high degree of continuity with this approach, but urge the government to take a step further and clearly make the case for its value with a series of highly visible initiatives, including:

- Model its commitments to human rights online domestically, ensuring that any international cybersecurity discussion includes a human rights dimension and actively combatting ideas that suggest otherwise.
- Act as a regional leader and global advocate in promoting and investing in cybersecurity policy approaches that are interoperable internationally, leveraging international standards to the greatest extent practicable and facilitating global trade and cooperation through alignment of baseline security requirements.
- Demonstrate how to achieve assurance of the protection and continuity of critical technologies while also recognizing the global nature of the technology ecosystem and the need for approaches that could be reciprocated without undermining confidence in other jurisdictions.
- Promote the peaceful use of technology in line with the government's social and security interests, building on defensive and deterrence frameworks rather than leaning into the offensive space.
- Double down on investments in international legal, regulatory, governance and diplomatic efforts to shape global cybersecurity norms and their implementation, in particular when it comes to critical technology protection, such as in healthcare or elections.
- Lead efforts to clarify disputed areas of international law, adding more detail on how existing rules apply to cyberspace, and building coalitions of supporters around those interpretations.
- Encourage frameworks that deter private sector actors from engaging offensively, by limiting government mandates, and regulating the sale of offensive technologies.
- Contribute to research into attribution from policy, legal, and technical perspectives and support other nations in this space to drive norms adherence.
- Build a broader coalition that aligns with the values and objectives of the Australian government in this space, breaking old models and alliances, and innovating by incorporating the multistakeholder community.

How will cyberspace and critical technology shape the international strategic/geopolitical environment out to 2030?

The intersection of cybersecurity and critical technology will continue to impact global security and international relations for many years to come. Technological advantages resulting from increasingly powerful capabilities in interconnectivity, processing power, cognition, and autonomy may exacerbate competition, strengthen ally coordination, and amplify the importance of cybersecurity. Moreover, there will likely continue to be opportunities for international cooperation and friction across efforts to develop standards, protect intellectual property, increase confidence in supply chains, access talent and innovation, develop and implement international law and norms, and raise the costs of cybercrime.

Without thoughtful and focused investment, the geopolitical environment also may be impacted by a widening digital divide. Connectivity and the ability to extract insights from information now firmly underpin social, economic, and political institutions, and will continue to shift the balance of power in favor of those with the greatest ability to leverage these critical technology capabilities. The potential scale of advancement in critical technologies in the coming years risks creating disproportionate gaps in economic opportunity and overall security between countries and deepening inequality, resulting in potential division, instability, and conflict.

Access to, use of, or manipulation of enablers of critical technologies and digital platforms will also impact the geopolitical environment. In regions with greater connectivity and access to technology, there may be competition over enablers of transformational capabilities like AI, including access to quality data, strong supply chains, energy, and computing power. There will also continue to be efforts to control and manipulate information, which risks eroding public trust, including through disinformation campaigns. It will be critical for the international community to act together to support democratic institutions.

The complexity of critical technologies and their connection to security and economic and political power will also challenge the creation of norms in the international community. Calls for restraint on activity or behavior may be viewed as a threat to technological development or information dominance. Norms for responsible behavior in cyberspace will be a critical tool for geopolitical stability and management of systemic risk. First, states must come to consensus on the applicability of national and international law to cyberspace. This work is already being tackled at the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Without this effort, it will be a difficult task to apply or build further norms for the security of critical technologies.

What technological developments and applications present the greatest risk and/or opportunities for Australia and the Indo-Pacific? How do we balance these risks and opportunities?

Technology is at once becoming rapidly more complex and more ubiquitous, and so too are techniques to secure and promote trust in these evolving technologies. The past few months have underlined our reliance on technology for everything from work, to learning, communicating and healthcare. It has also shown how vulnerable we are to cyberattacks. The rapid adoption we experienced during the COVID-19 pandemic is therefore a perfect metaphor for how technology generates risks and opportunities in equal measure. With that in mind, rather than focusing on a particular groundbreaking technology that is likely to impact the region in the coming years, such as artificial intelligence or 5G, Microsoft would like to underline the importance of risk management and prioritization for all of the country's technology adoption.

For security approaches to be effective, they must enable organizations to prioritize among the risks and capabilities that are most critical in their environments. Risk-based approaches enable enterprises to have sufficient flexibility as they implement guidance or requirements, allowing their unique infrastructure, operating environment, and business priorities to inform decision-making. In turn, such flexibility means that enterprises can innovate, integrating both security and productivity advancements into products and services that benefit and better protect governments, enterprise customers, and consumers.

In addition to developing risk-based approaches, governments should focus on the most important risks first. While there is value in being comprehensive, doing so can also obfuscate important details, potentially leading to overlooked risks. An all-encompassing approach is also impossible to manage, as it is likely to result in confusion both when organizations attempt to demonstrate compliance and when governments try to assess it. Risk prioritization, by way of contrast, not only helps to ensure that the greatest threats are mitigated, but also focuses attention and increases efficiency in demonstrating security practices and assessing compliance.

Finally, we encourage the Australian government to retain room for maneuver and ability to keep up with dynamic technology development, by ensuring its regulatory solutions focus on the desired outcomes (on what they want to achieve) rather than specific mechanisms (how they want to achieve it). This is particularly important in cybersecurity. As technological innovation accelerates and threat actors continue to rapidly evolve offensive techniques and strategies, governments and enterprises must also be able to improve their defenses quickly. Rather than being locked in to using technologies or capabilities that were state of the art when a particular control was introduced, governments and enterprises must be able to deploy more secure or convenient solutions as they become available, without the control having to be revised continuously. Outcomes-focused approaches enable such agility.

How should Australia pursue our cybersecurity and critical technology interests internationally?

Pursuing Australia's cybersecurity and critical technology interests will inevitably rely upon robust international engagement with a diverse set of stakeholders. This is due to the rapidly increasing levels of connectivity around the world, as nations everywhere proceed through this tumultuous and exciting period of digital transformation. Unlike other areas of statecraft, the digital ecosystem is not, in general, a space of zero-sum gains. In most cases, technological advancements, or improvements for one nation or region, have cascading benefits across the board. Improvements in connectivity and ICT infrastructure result in access to new markets for goods and services, as well as new innovations. Meanwhile, improvements in security are nearly always shared benefits, as any vulnerabilities in one part of a networked ecosystem inherently put others at risk.

With these opportunities for shared benefits and prosperity in mind, Microsoft would encourage Australia to pursue four overarching objectives as it seeks to achieve its cybersecurity and critical technology interests internationally – i) policy transparency and leadership, ii) regulatory harmonization, iii) multistakeholder engagement, and iv) capacity building.

Policy transparency and leadership

Australia has long been a leader when it comes to transparency in its cybersecurity policies. Such transparency is invaluable both as an example and a learning opportunity for other nations, as well as a method of easing potential tensions or conflict in cyberspace. By publishing materials like a national cybersecurity strategy or an international cybersecurity engagement strategy, Australia helps illustrate how other countries can also take charge of their digital destinies. Moreover, by publishing more traditionally sensitive materials, including a vulnerability equities process and a clear explanation of how international law applies to and guides Australia's actions in cyberspace, allies and potential adversaries alike can have a better understanding of the boundaries Australia has set for its own behavior in cyberspace and how to behave in a way that respects those boundaries.

While some of the information surrounding a national cybersecurity policy and its implementation may understandably need to remain confidential, additional transparency in implementation would be uniquely beneficial in reinforcing norms and expectations vis-à-vis other states. This might include, for example, explaining how attribution decisions are made following a cybersecurity incident, what laws and/or expectations have been violated by such incidents, and what types of response options would likely be employed. While such information would likely involve sensitive intelligence at the time of, or immediately following, an attack, it would be helpful to even provide retrospective explanations of how previous attacks were attributed and how they specifically violated international expectations.

Australia's transparency and leadership in this space serves as an invaluable example for others. By this same token, however, we would encourage Australia to also consider the broader implications of its policy decisions in light of that same leading role it plays on the international stage. In late 2018, Australia passed legislation

that would allow government authorities to insist upon access to encrypted communications in certain circumstances, potentially requiring private companies to create "backdoors" or other ways around their own encryption in some cases in order to comply. While such policies may be properly motivated to try and legally intercept criminal and other nefarious communications, they also threaten to critically damage the encryption which underpins so much of our shared digital ecosystem. In addition to giving private industry pause about their ability to comply with these requirements and do business in Australia, however, we also worry that such policies inevitably set a troubling example for other countries to follow. Even if there were a responsible way for Australia to exercise such authorities, it seemingly unavoidably sets a dangerous precedent for abuse if these policies become the norm across the globe, including among less responsible governments.

Regulatory harmonization

The threats to cyberspace do not stop at national borders. It is therefore essential that governments adopt approaches for tackling cybercrime and encouraging cybersecurity that acknowledge that reality. The ability to have technology products and services adhere to recognized standards across countries and regions improves security and allows for ease of adoption, driving economic growth and further technological innovation. Meanwhile, international cooperation to identify best practices, yields standards that prioritize and optimize for security as well.

Australia should therefore integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind wherever possible. We also encourage Australia to continue its participation in international standards bodies such as the International Organisation for Standardisation (ISO) and promoting the adoption of harmonized approaches in their capacity building efforts.

Multistakeholder engagement

Through its Cybersecurity Affairs office in the Department of Foreign Affairs and Trade (DFAT), Australia is already actively engaged in key forums on the digital economy around the world. This includes participation in the ongoing UN dialogues on information security – the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE). While such multilateral dialogues have a unique and exclusive role to play in establishing peace and security online, they have limitations in that they are only open to governments. The challenges posed by our ever-growing digital ecosystem and the online world it enables require ongoing and regular collaboration with a broader set of stakeholders than governments alone – including industry and civil society. This is in part because our shared cyberspace is largely owned and operated by private industry, which has unique insights in how best to support and protect a robust digital ecosystem.

Australia's Cybersecurity Affairs office has already played a significant and helpful role in supporting this multistakeholder collaboration by actively and consistently seeking input from industry and other non-state stakeholders throughout the duration of the twin UN dialogues referenced above, as well as in other venues. Microsoft has been glad to provide direct contributions to those consultations. We appreciate and encourage Australia's continued advocacy for greater multistakeholder inclusion in all UN dialogues on technology issues.

Moreover, we appreciate Australia's decision to endorse and support the 2018 Paris Call for Trust and Security in cyberspace. With more than 75 government endorsements, as well as hundreds of other industry and civil society supporters from across the globe, the agreement is now the largest such multistakeholder commitment to cybersecurity principles in the world. More than just a statement of principles, however, the Paris Call seeks to empower its community of supporters to promote trust and security in cyberspace and to discourage reckless and irresponsible behavior. We hope that Australia will continue to support this effort to develop an important and regular global multistakeholder dialogue on how to advance peace and security online.

Finally, the government could invest in strengthening its multistakeholder engagement domestically as well. In particular, it could build on the example this consultation provides, by creating a standing industry advisory

panel to CCTIES, which would allow Australia to take the pulse on the implementation of CCTIES regularly and not just at the end of each process.

Capacity building

As mentioned earlier, the digital domain is unique in that improvements and advancements can be shared – indeed, it is often best for all involved when they are. While there remain areas for strategic competition, in general the gains achieved in cyberspace are not zero-sum. Improvements in connectivity and digital capacities in one country can open new economic opportunities and lead to further innovations which benefit others elsewhere. While this is true across the digital domain, it is especially true when it comes to issues of cybersecurity – improvements in the cybersecurity defenses of one country benefit all others in a connected world. With that in mind, Microsoft encourages Australia, as a leading nation in the digital space, to support robust capacity building efforts, which rely on the following principles:

- Utilize existing mechanisms. Numerous states, foundations, and private actors have dedicated funding and resources to capacity building initiatives. Instead of replicating the efforts, Microsoft encourages governments to pool resources to generate greater impact, and participate in fora, such as the Global Forum on Cyber Expertise (GFCE), which can act as match-making mechanisms between needs and expertise.
- Understand the need. Capacity building efforts can only succeed if they are responding to a real need. They therefore need to begin with the participant's understanding of what issues matter to them and why, as well as an understanding of where they have gaps in capacity or capability that need to be addressed.
- Develop an all of government approach. All too often, capacity building efforts strictly focus on enhancing technical capabilities at the expense of others – including diplomatic, judicial, etc. Against the background of the increasing number of venues for diplomatic engagement on digital technology issues, such as the UN and beyond, Microsoft believes cybersecurity-diplomacy for the foreign service should be prioritized to ensure all countries are equipped to participate in these conversations on an equal footing.
- Be inclusive of all stakeholders. When developing and implementing capacity building efforts, it is worth remembering that digital technologies can impact all parts of a society. It is therefore critical that capacity building focus not just on government stakeholders, but industry and civil society as well. Moreover, it is important that diverse perspectives are included in the development and delivery of trainings.
- Maintain relevance. Technology is evolving rapidly, and it is important to ensure that capacity building efforts move with the times. Trainings and development projects should therefore strive to incorporate understandings of the latest technologies to ensure participating entities are equipped to leapfrog their counterparts, rather than stagnate. Even more importantly, capacity building needs to be treated as a continuous and recursive process, rather than a series of one-off engagements.

How can government, industry, civil society and academia cooperate to achieve Australia's international cybersecurity and critical technology interests?

As underlined earlier in the document, Microsoft strongly believes that robust multistakeholder dialogue is essential to addressing issues across the broad spectrum of policy challenges effecting the digital ecosystem. As with many other areas we have highlighted in this response, Australia has already been leading the way in pioneering these kinds of partnerships, both at domestic and international levels. This includes the Australian government cooperating with industry and academia in designing and implementing advanced degree programs to address the growing global cybersecurity skills shortage, as well as developing some of the

world's leading graduate programs training researchers in emerging technologies. This very process of developing an international cybersecurity engagement strategy, and actively seeking multistakeholder input in doing so, speaks to Australia's commitment to cooperation across stakeholder groups.

In addition, however, there are particular international dialogues and processes related to digital technology that Microsoft would encourage Australia's diplomatic efforts to focus on, including the **Internet Governance Forum (IGF)**[1]. Established by the UN, the IGF facilitates multistakeholder discussion of issues critical to the governance of the digital ecosystem through its annual convening and ongoing working groups. The IGF is unparalleled in coordinating authentic multistakeholder engagement on a wide range of internet governance issues, helping to set and influence the international agenda. Unfortunately, however, government participation in the IGF has historically been limited, which curtails the potential for discussion and cooperation. To this end, we would encourage Australia to participate more robustly in the annual event, and to participate as well in the respective "Best Practice Forums," which serve as ongoing multistakeholder working groups on different topics of internet governance that produce research and reports for review and presentation, and to build consensus and understanding, with the broader IGF community.

In addition to participating in the IGF as it currently stands, we also are in agreement with the UN's 2019 High Level Panel on Digital Cooperation[2] on the need for more regularized and formalized institutional dialogue between UN Member States and a multistakeholder community on issues relating to the impact of digital technologies. To that end, we support the recommendation included in that body's final report for the establishment of an "**IGF Plus" model**, to leverage and further build on the strengths and successes of the current IGF structure while expanding its impact by empowering it with additional authority and decision making responsibilities. We encourage Australia to support efforts to evolve the current IGF through exploring and implementing the various IGF Plus mechanisms outlined in the High Level Panel's report, linking the IGF Plus Secretariat to the Office of the UN Secretary-General, and providing it with additional resources as necessary to support this transition and fulfil an expanded mandate moving forward.

Finally, we would encourage the Australian government to **not be limited by existing frameworks**, but to pursue its international cybersecurity objectives through new forms of cooperation. The fast-moving pace of technological innovation requires governments to re-assess their decision-making models, which can move slowly, in particular at the international level, where the challenges can be compounded by the differing geostrategic objectives. We therefore urge the government to participate, and potentially stand up new frameworks that bring together new allies – across the stakeholder community – that could make progress on a particular objective. The Paris Call for Trust and Security in Cyberspace[3], referenced above, is a great example of a new way of agreeing principles in this space, and we hope that the Australian government will be able to participate more fully in its implementation, as well as to identify new opportunities for engagement. In addition, we recommend the government assess whether there would be interest in developing a Track 1.5 dialogue series with key nation states to ensure continued communication and cooperation.

What policies and frameworks exist in other countries that demonstrate best practice approach to international cybersecurity and technology policy issues?

---

[1] Internet Governance Forum: https://www.intgovforum.org/multilingual/

[2] Report of the UN High Level Panel on Digital Cooperation: https://digitalcooperation.org/report/

[3] Paris Call for Trust and Security in Cyberspace https://pariscall.international/en/

Microsoft believes that, at the heart of international engagement on cybersecurity and technology issues, lie open communication and a commitment to a goal that is supported at multiple levels in government and society. Lessons from cooperation in cybersecurity can be brought forward to critical technologies. Because critical technologies and cybersecurity both have social, political, and economic dimensions, governments should take a holistic, multistakeholder approach to implement and demonstrate their commitments and create public awareness that will support their cooperation and investment at the international level.

Several countries provide examples of a "whole of society" approach that has resulted in greater awareness and cybersecurity hygiene at the citizen level, supported digital transformation, and created demonstrable accountability to the international community to uphold norms of responsible behavior. Many of these activities can translate directly into supporting policy and strategy for critical technologies, such as creating bodies of coordination between government, civil society, and industry. Here, we highlight the longstanding programs of the Netherlands and the United Kingdom as strong examples of cybersecurity commitment. Notably, these countries have a strong base of public awareness of cybersecurity that enable them to pursue strategic-level objectives for cybersecurity.

The Netherlands

The Netherlands' approach to cybersecurity is unique in that it takes a keen interest in establishing itself as a cybersecurity business hub. The Dutch government has successfully identified and pursued the development of what is now the largest cybersecurity cluster in Europe, with the Hague Security Delta[4]. Similarly, the government has funded and attracted a number of international and non-profit institutions that deal with cybersecurity, such as the Global Forum for cybersecurity Expertise[5], Europol's European Cyber Crime Center (EC3)[6] and the NATO Communications and Information (NCI) Agency[7].

United Kingdom

The United Kingdom similarly recognizes that international cooperation on cybersecurity is critical to its national wellbeing and economic growth, and it assigns cybersecurity the highest category of threat to its national security. What is particularly worth emulating is the country's approach to metrics. In each part of its National Cybersecurity Strategy for 2016-2021[8], the UK government identifies its objectives, approaches, and importantly, metrics of success. These are an accountability mechanism to achieving its strategy and signal its intent to lead in the international arena. Further, the government recognizes that the cybersecurity capacity of its peers will affect its security, and has hinged one of its own metrics of success on the increased cybersecurity resilience of the international community.

---

[4] The Hague Security Delta: https://www.thehaguesecuritydelta.com/?gclid=CjwKCAjwyo36BRAXEiwA24CwGbB1xxNr9nt_TlOOkVnlZ7f8rEu5-22f4knvyTpClWoz7QS8VcogzBoCA5kQAvD_BwE

[5] GFCE: https://thegfce.org/

[6] Europol EC3: https://www.europol.europa.eu/about-europol/european- cybersecuritycrime-centre-ec3

[7] NCI Agency: https://www.ncia.nato.int/

[8] United Kingdom National Cybersecurity Strategy 2016-2021: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cybersecurity_security_strategy_2016.pdf

One useful way to think about creating strategic change is by being able to demonstrate quantifiable progress against a certain set of indicators. In fact, the ITU's Global Cybersecurity Index (GCI)[9] measures a country's cybersecurity commitment through indicators in five pillars: legal, technical, organizational, capacity building, as well as cooperation. In 2018, Australia ranked 11th in the GCI, with cooperation (including bilateral, multilateral, and public-private partnerships) being its lowest performing category. We hope that Australia will be able to climb through the ranks in the coming years, and able to publicly document its progress, so that others can emulate its efforts.

Conclusion

Finally, Microsoft would once again like to underline how much we appreciate the opportunity to comment on Australia's Cybersecurity and Critical Technology International Engagement Strategy. The rapid pace of change we are experiencing currently will only serve to exacerbate existing cybersecurity challenges. However, increased public awareness of these challenges can help spark international policy action to promote peace in cyberspace, and cooperation in critical areas over the next decade.

Australia can set a distinct precedent for international engagement on cybersecurity through a strategy grounded in multistakeholder cooperation that can bring greater value for peace, security, and prosperity over the longer term than short-term competition. We commend the Australian government's long-term vision for international cooperation on cybersecurity and critical technologies and we welcome the opportunity to work with Australia to find and implement best practice approaches over the next decade.

[9] ITU Global Cybersecurity Index, 2018: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf