Australia welcomes the opportunity, in response to the invitation in General Assembly resolution 78/237, to provide its views on advancing responsible State behaviour in cyberspace in the context of international security and further regular institutional dialogue.

This submission builds upon submissions provided by Australia in response to resolutions 77/37 in 2023, 76/19 in 2022, 75/32 in 2021, 74/28 in 2020, 70/237 in 2016, 68/243 in 2014 and 65/41 in 2011 on developments in the field of information and telecommunications in the context of international security.

**Australian Cyber Security Strategy 2023-2030**

On 22 November 2023 Minister for Cyber Security Clare O’Neil launched Australia’s Cyber Security Strategy 2023-2030, which sets out Australia’s vision for domestic and international cyber security through a whole-of-nation approach to building cyber resilience.

The Strategy identified six shields to build stronger cyber defences and bounce back quickly following a cyber incident: (1) strong businesses and citizens; (2) safe technology; (3) world class threat sharing and blocking; (4) protected critical infrastructure; (5) sovereign capabilities; and (6) resilient region and global leadership.

The Strategy sets out Australia’s continuing commitment to shape, uphold, and defend international cyber rules, norms and standards, including by upholding international law and norms of responsible State behaviour in cyberspace, and deploying all arms of statecraft to deter and respond to malicious actors.

**Uphold international law and norms of responsible state behaviour in cyberspace:**

Australia will collaborate with our existing partners and build new partnerships to uphold international law and the agreed framework for responsible state behaviour that underwrites our stability, prosperity, independence and sovereignty in cyberspace.

All countries have agreed to a rules-based cyberspace, founded on existing international law and norms. International law, complemented by agreed voluntary norms of responsible state behaviour, confidence-building measures and capacity building, provides a robust framework for predictability and stability in cyberspace. When implemented and adhered to, this framework provides a toolkit to address threats posed by state-generated and state-sponsored malicious cyber activity.

Australia will work with our international partners in United Nations discussions to clarify how international law applies in cyberspace and strengthen implementation of the framework for responsible state behaviour in cyberspace. Such efforts will include enhancing cooperation through regional forums, including as part of the Pacific Islands Forum and through engagement with the ASEAN Regional Forum.
Deploy all arms of statecraft to deter and respond to malicious actors:
Australia will deploy all arms of statecraft to deter and respond to malicious cyber actors. Australia will work with our international partners to take action to impose costs on individuals and organisations that make cyberspace less safe and secure. This includes calling out instances where states act to undermine or breach international law and norms, and imposing sanctions on those who carry out or facilitate significant cyber incidents – when we have sufficient evidence and it is in our national interests to do so.

In all its actions, Australia will uphold existing international law and the agreed voluntary norms of responsible state behaviour in cyberspace.

Support a cyber resilient region:
Australia will continue to work with our neighbours in the Pacific and Southeast Asia to build a more cyber resilient region. Our cooperation and assistance will continue to be coordinated by Australia’s Ambassador for Cyber Affairs and Critical Technology.

Australia is refocusing Australia’s cyber cooperation and capacity building efforts to be more targeted, impactful and sustainable and to enable our neighbours to better prevent cyber incidents and recover quickly when they occur. Recognising that people engage with cyber security issues in different ways, our efforts will continue to consider gender equality, disability and social inclusion. This includes continuing support for the United Nations Women, Peace and Security agenda, as well as Australia’s National Action Plan on Women, Peace and Security 2021–2031.

When severe cyber incidents occur in our region, Australia will be better positioned to respond to requests for assistance. Australia is establishing a regional cyber crisis response team in the Department of Foreign Affairs and Trade, drawing on expertise from government, industry, and the technical community. In response to government requests following significant cyber incidents in the region, the team will help contain the spread and impact of cyber incidents and restore critical services and infrastructure.

Regular institutional dialogue

Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security (POA)
Australia supports the establishment of a single, permanent, flexible, inclusive, transparent, and action-oriented mechanism, under the auspices of the UN First Committee, to discuss, implement and advance the Framework of Responsible State Behaviour in Cyberspace (the Framework), agreed and reaffirmed by consensus by the General Assembly. The Framework consists of international law, norms, confidence building measures, and supported by coordinated capacity building. The POA should provide a forum where all 193 Member States can meaningfully engage in both discussion and action, on a regular and ongoing basis. The POA should be able to grow, pivot and develop – it should support implementation of the existing agreed Framework and allow for potential further development of the Framework, by consensus, as new threats and challenges arise.

General Assembly Resolution 77/37 welcomed the proposal to establish the POA and requested the Secretary-General seek the views of Member States on the scope, structure and content for the programme of action. That report (A/78/76) recommended that States continue to discuss the potential scope, structure, principles, content, functions and follow-up mechanism of the programme of action proposal under the auspices of the 2021-2025 Open-Ended Working Group (OEWG),
drawing on the views expressed in the report while also taking into consideration the regional and subregional consultations organized by the Office for Disarmament Affairs pursuant to General Assembly resolution 77/37.

The OEWG plays a key role in the elaboration and preparatory work for the POA. The POA should build on the hard-fought consensus gains and cumulative discussions of the past six successive Groups of Governmental Experts (GGEs) and the inaugural and current OEWGs. A permanent mechanism represents the next phase or evolution in UN cyber architecture that builds upon what has come before and guarantees that these issues are accorded the attention and importance they merit going forward.

General Assembly Resolution 78/16 decided to establish a mechanism under the auspices of the United Nations, upon the conclusion of the 2021-2025 OEWG and no later than 2026, that will be permanent, inclusive and action-oriented, with the specific objectives affirmed in UNGA resolution 77/37 and with the common elements for future regular institutional dialogue agreed by consensus in the 2023 annual progress report of the 2021-2025 OEWG.

Australia supports the proposal for an international conference to be convened, in 2025, to adopt the founding document of the POA, on the basis of the preparatory work done in the 2021-2025 OEWG.

Australia supports a founding document for the POA setting out the commitments of States, and providing a mechanism that could be endorsed by an UNGA Resolution. The founding document, which could be set out as a Political Declaration, should:

- endorse and reaffirm States’ political commitment to the Framework (including the application of existing international law in cyberspace) as agreed in GGE reports\(^1\) and the OEWG report\(^2\);
- recall existing and emerging threats to international security related to the malicious use of ICTs, building on the threat assessments contained in the GGE and OEWG reports;
- establish a permanent institutional mechanism to advance implementation of this Framework (including supporting States’ capacities to do so) and the relevant modalities;
- allow for further development and updates to the Framework as appropriate to include consensus principles, recommendations and commitments in the event that UNGA, by consensus, endorses a report of the OEWG, GGE or other UN processes, or by consensus agreement at a POA Review Conference;
- set out focus areas of work for the POA based upon issues the international community agrees to discuss and address; and
- clearly foster and encourage engagement with relevant members of the multistakeholder community in relevant areas.

In relation to rules of procedure, Australia reiterates that the POA should require agreement on all issues by consensus (including reports, recommendations, and declarations).

To ensure POA activities are evidence based and data driven, the POA should emphasise supporting implementation efforts, including through specific, targeted, coordinated capacity building. Measures for dedicated capacity building should be elaborated clearly within the POA. To promote targeted capacity building which is based upon need and founded upon an evidence base, the POA might

\(^1\) A/65/201 (2010); A/68/98 (2013); A/70/174 (2015); A/76/135 (2021).
\(^2\) A/AC.290/2021/CRP.2.
encourage Member States to survey and self-report on their implementation of the Framework periodically (for example, every three years, or otherwise in line with the review conference cycle) using a standardised reporting mechanism, the Survey of National implementation of UN General Assembly Resolution 70/237: https://nationalcybersurvey.cyberpolicyportal.org/.

Australia recognises the importance of the multi-stakeholder community, including civil society, the private sector, academia and the technical community, in contributing to a free, open, secure, stable accessible and peaceful cyberspace. Australia proposes the POA allow for regular and institutionalised consultation with relevant stakeholders.

In summary, Australia emphasises that the POA should have a clear mandate that builds upon and reaffirms the agreed Framework; be flexible, both substantively in that the Framework may be further developed by consensus and procedurally; support implementation efforts through voluntary reporting and in implementing the Framework through capacity building; and be inclusive in that decisions on matters related to international security remain the prerogative of States, yet discussions and working groups be open to the multistakeholder community.

Australia looks forward to continuing to work with the Secretary-General, Office of Disarmament Affairs, and Member States to develop an effective, flexible and inclusive POA.