Ad Hoc Committee to elaborate a comprehensive international Convention on Cybercrime

Australian submission on international cooperation, technical assistance, prevention measures, mechanism of implementation and final provisions

Australia welcomes the opportunity to submit its views for the consideration of the Ad Hoc Committee to elaborate a comprehensive international Convention on Cybercrime (AHC) at its third session in New York (29 August – 9 September 2022).

The new Convention offers an unrivalled opportunity to secure widespread consensus to broaden international cooperation to counter cybercrime, while respecting existing commitments, and protecting existing processes that have proven effective.

International cooperation, collaboration, information sharing, discussion and capacity building are vital to any meaningful response to the threat posed by cybercrime.

Australia takes this opportunity to reiterate and expand upon previous national submissions to the AHC (29 May 2020; 29 October 2021; 13 April 2022), in relation to international cooperation, technical assistance, prevention measures and mechanism of implementation and final provisions.

International cooperation

Technology continues to expand the cybercrime threat landscape, and in turn, produce increasingly challenging circumstances in which to carry out criminal investigations. The growth of global connectivity and increased reliance on cloud computing means that data is often stored in other jurisdictions and can be owned or controlled by service providers across multiple jurisdictions. Lawful access to this data is vital for the effective investigation of cyber-dependent and cyber-enabled crimes.

Australia recognises the utility of the Convention establishing a framework for requests, consent and access to electronic evidence in another jurisdiction, in relation to the commission of crimes with and without a cyber dimension.

The Convention's international cooperation provisions should apply to offences set out in substantive criminalisation articles within the Convention. The Convention's mutual legal assistance provisions for collection of evidence in electronic form, where consistent with states' domestic legal frameworks and with sufficient conditions and safeguards, could apply to other criminal offences, including offences committed by means of a computer system.

International cooperation for the exchange of information and/or electronic evidence must be clearly limited in the Convention so that it can only be used for the purpose for which it was provided, and should not be used for other purposes without reverting to the providing state.

International cooperation under the new Convention cannot be considered in isolation. The depth and breadth of the international cooperation provisions appropriate for inclusion in the Convention will be determined by the scope of the new Convention, and the robustness of the procedural and

human rights safeguards (including essential interest protections) underpinning the powers set out in the Convention to detect, investigate and prosecute cybercrime.

In order to protect the proper function of existing frameworks and avoid duplication of efforts, States Parties should not be obliged to use this UN Convention as the basis for their international cooperation where they already have existing bilateral or multilateral agreements.

Cooperation through central authorities

States continue to rely on traditional international cooperation mechanisms (such as mutual legal assistance) though central authorities to obtain electronic evidence and other records in combating all manner of crime, including cybercrime. This also extends to other mechanisms, such as extradition.

In line with the mandate provided by Resolution 74/247, the new Convention should ensure it complements and does not undermine existing mechanisms for international cooperation on criminal justice (*inter alia* Chapter III of the Budapest Convention; and Articles 16-18 of UNTOC; Chapter IV of UNCAC.

Broadly, these conventions allow States to provide cooperation subject to the conditions and safeguards under their domestic laws. This includes domestic laws which ensure compliance with States' obligations under the *International Covenant on Civil and Political Rights*, the *Second Optional Protocol to the ICCPR aiming at the abolition of the death penalty*, and the *Convention Against Torture*. The Convention's international cooperation provisions should be similarly framed.

These provisions should also be subject to safeguards within the new Convention – for example, the new Convention could include a provision that references the protection of human rights and States' international legal obligations.

- Mutual assistance to request and access electronic evidence

Mutual assistance under the Convention should facilitate States to cooperate, including to request electronic data and evidence in another jurisdiction, while preserving certain safeguards. In particular, mutual assistance under the Convention should be subject to the requested State's domestic laws and other applicable treaties, including for any grounds of refusal. The Convention may also include further safeguards that will apply in addition to any grounds of refusal and safeguards under the requested State's domestic law and other treaties, including the ability to refuse a mutual assistance request:

- : in circumstances relating to any matter where a person has been arrested, detained, charged or convicted in relation to a death penalty offence, recognising that in some circumstances it may be appropriate to grant the assistance requested, having regard to any 'special circumstances' of the case (e.g. the requesting State provides a sufficient undertaking that the death penalty will not be sought, imposed or carried out, or where the requested assistance is considered exculpatory evidence)
- : where the request relates to the investigation, prosecution or punishment of a person for a political offence, or on account of inter alia a person's race, sex, sexual orientation, religion, nationality or political opinions
- : where there are substantial grounds for believing that a person would be in danger of being subjected to torture if the request was granted; and
- : where the granting of the request would prejudice the sovereignty, security or national interest of the State.

- Extradition

Extradition under the Convention should be subject to the requested State's domestic laws and applicable treaties, including for any grounds of refusal, requirements to establish dual criminality, and minimum penalty requirements. This will ensure that the provisions preserve existing safeguards for human rights and the rule of law, and operate consistently with the existing international legal extradition framework. The Convention should also include further safeguards that will apply in addition to any grounds of refusal and safeguards under the requested State's domestic law and other treaties, including:

: that extradited persons be guaranteed fair treatment
: that nothing in the Convention be interpreted as imposing an obligation to extradite where the requested state has substantial grounds for believing extradition was made for the purposes of discrimination on basis of a person's race, sex, sexual orientation, religion, nationality or political opinions
: prohibition of extradition of a person for an offence which attracts the death penalty, unless a sufficient undertaking is provided that the death penalty will not be imposed, or if imposed, will not be carried out; and
: prohibition of extradition of a person if there are substantial grounds for believing they would be in danger of being subjected to torture.

Cooperation through law enforcement agencies

There are additional forms of international cooperation which represent immense value to law enforcement and criminal justice outcomes and sit outside of mechanisms traditionally overseen by central authorities, such as police-to-police cooperation. The new Convention should facilitate police-to-police cooperation to the widest extent possible and complement other international cooperation, including mutual legal assistance. Certain key principles should underpin how the new Convention incorporates international frameworks that support law enforcement access to electronic evidence, such as:

: streamlining government-to-government cooperation, particularly in emergency circumstances
: importance of interoperability to facilitate international cooperation requests, including through agreed language, with additional languages to be agreed between States Parties, preventing unnecessary delays due to translation issues; and
: the importance of clear requirements to facilitate international cooperation requests upfront, including minimum information requirements and format of a request to another State Party.

The new Convention could also provide a facilitation framework for cooperation with/between States Parties that do not have readily accessible points of contacts or international frameworks in place, and which, as a result, can be taken advantage of by cybercriminals.

- Cooperation through law enforcement: 24/7 networks

24/7 networks are key enablers for rapid and effective international cooperation, by providing for agreed channels through which law enforcement agencies can directly seek assistance or be referred to the correct agency within a State's domestic framework. The new Convention should consider agreed points of contact for each State Party to facilitate this cooperation, including by referring priority requests to the relevant competent authority. Such contact points should leverage and complement existing, functioning 24/7 networks – such as the Interpol National Central Bureau

Network or the 24/7 network established under the Budapest Convention – rather than create new networks. However, the designation of a 24/7 contact should ultimately be determined by each State Party.

Under Article 35 of Budapest Convention, Parties themselves determine where the 24/7 point of contact is best placed, providing flexibility to implement the arrangement that is most effective in each Party's respective domestic framework to ensure quick and effective cooperation. For example, this may be a specialised cybercrime police unit, or staff within a central authority for mutual assistance with expertise in cybercrime matters. Where that point of contact is not a Party's authority for mutual assistance, the point of contact must be able to coordinate with that authority in a timely manner.

For example, Australia's 24/7 point of contact is the Australian Federal Police's National Operations State Service Centre (NOSSC), which provides a 24/7 single point of entry for domestic and foreign law enforcement agencies to request assistance for criminal investigations and prosecutions. Australia's INTERPOL National Central Bureau also sits within the AFP.

Asset recovery and proceeds of crime

Law enforcement agencies across jurisdictions are seeing an increase in criminals' use of digital assets to facilitate their offending and to hold and distribute the benefits derived from their offending, including in the context of ransomware, money-laundering and other predicate offending.

Australia supports the inclusion of provisions on recovery of proceeds of crimes in the Convention, provided those provisions are consistent with the existing international framework contained within UNTOC, UNCAC and the Financial Action Task Force (FATF) standards: it is important that legal frameworks continue to support an overarching policy objective of depriving criminals of the benefits of their crimes. Australia is in favour of adopting the UNTOC model for any provisions on recovery of proceeds of crime, noting that it covers a broader range of offending than UNCAC, and Australia considers the UNTOC model to be better adapted to the scope of the new Convention. The transfer of proceeds of crime should also be underpinned by robust safeguards and due regard for the rule of law.

It is important that legal frameworks continue to support an overarching policy objective of depriving criminals of the benefits of their crimes. In order to be consistent with the existing robust international framework, this Convention's provisions on asset recovery should be appropriately defined and limited with reference to existing standards contained within UNCAC and the Financial Action Task Force (FATF). The transfer of proceeds of crime should also be underpinned by robust safeguards and due regard for the rule of law.

Technical assistance

Criminals look to exploit gaps in State's legislative, policy, law enforcement and technical capacity. Technical assistance and capacity building is therefore an essential part of our collective response to cybercrime. Cyber capacity building should be multi-disciplinary, multi-stakeholder, modular and measurable. Capacity building should be supported by subject matter expertise focused on building resilience to cybercrime.

Australia supports provisions in the Convention that are specifically focused on encouraging and providing mechanisms and technical assistance for effective implementation of the Convention

itself, and assessment of Convention implementation. This can be achieved by working with the UN and also other global, regional and subregional bodies, alongside relevant stakeholders. Technical assistance under the Convention should encourage transparency and information sharing on effectiveness.

Provisions in the Convention addressing technical assistance should be responsive to States' Parties needs, while also drawing on and supplementing existing work underway. Australia supports multistakeholder involvement in the design and delivery of technical assistance and capacity building. These measures will ensure the Convention does not duplicate or disrupt existing efforts, and is a useful, practical and future-proof instrument.

Fortunately, we are not starting from scratch. Significant work is either underway or has been completed to assist States to respond to cybercrime, including:

- The UNODC's Global Programme on Cybercrime
- Australia's Cyber and Critical Tech Cooperation Program, through which Australia provides targeted and multifaceted capacity building to support ASEAN and Pacific countries to respond to the challenges posed by cybercrime
- The exchange of technical expertise, information and best practice between States, through the open-ended intergovernmental expert group on cybercrime (IEG)
  - : where experts emphasised, *inter alia*, countries' needs and existing technical assistance activities, including capacity-building for law enforcement and criminal justice systems in handling electronic evidence
- The Council of Europe's Global Action on Cybercrime (GLACY+), supporting countries across Africa, Asia-Pacific, Latin America and the Caribbean.

Prevention

While an adequate criminal justice response is critical to responding to the occurrence of cybercrime, States should consider the importance of prevention of cybercrime, and in particular, how States can prepare and educate their communities, civil society, private sector and government that reduce the occurrence and risk of cybercrime threats. Preventive measures are important to holistically responding to cybercrime and are as important as ensuring strong criminal justice responses to cybercrime. Prevention measures should be gender- and age-responsive; acknowledge and account for diversity and intersecting inequalities; and address the particular impacts of cybercrime on different groups, including women, children, the elderly and persons with disabilities.

The Convention should therefore contain language (including in the Preamble) encouraging States to promote best practices and policies aimed at the prevention of cybercrime. This could include measures such as:

- research on cybercrime issues, trends and responses
- tailored education programs and resources, including information for victims on how to report cybercrime
- raising awareness by providing evidence-based information
- encouraging States Parties to cooperate and share best practice and expertise, where appropriate and practicable; and
- encouraging States Parties to create, and keep updated, targeted national plans to address and prevent cybercrime domestically. These should employ:

- targeted approaches which take into consideration the specific needs of populations which are particularly vulnerable to cybercrime; and
- monitoring and evaluation.

Australia recognises the important role the private sector plays in preventing cybercrime. However, while the Convention should encourage private sector cooperation, regulation of the private sector should not be included in this Convention, and only occur through domestic frameworks (as contained within UNCAC Article 39.1, for example).

Implementation and final provisions

Implementation mechanisms should leverage, but not duplicate, existing UN bodies, such as the Commission on Crime Prevention and Criminal Justice and the UN Office for Drugs and Crime. The mechanism should promote and review implementation of the Convention, and engage experts to exchange information on best practices, challenges, integration of cross-cutting issues, responses and trends in cybercrime.

Australia recognises that reservations and declarations may be necessary in certain circumstances to facilitate the broadest possible membership to the Convention. However, as a general principle, Australia considers that the inclusion of reservations and declarations should be limited, and not undermine the Convention's objectives and safeguards, including for human rights.