13 April 2022

Ad Hoc Committee to elaborate a comprehensive international Convention on Cybercrime

Australian submission on criminalisation, procedural measures, and general 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 second session in Vienna (30 May – 10 June 2022).

Australia remains committed to an open, inclusive, transparent, and multi-stakeholder process, and to arriving at an outcome acceptable to the broadest number of states. Australia takes this opportunity to reiterate and expand upon previous national submissions to the AHC, in relation to criminalisation, procedural measures and general provisions.

Criminalisation

The new Convention offers the opportunity to improve international cooperation in relation to cybercrime, while at the same time ensuring consistency with, and avoiding unnecessary duplication of, existing international crime conventions and other relevant instruments. Criminalisation articles should be consistent with existing international instruments and avoid conflicts between such instruments. Criminalisation articles should also be appropriately balanced with respect for the rule of law, human rights and fundamental freedoms.

Australia considers that the new Convention offers an opportunity to increase global harmonisation of cybercrime offences. This will in turn reduce safe havens for cybercriminals and enhance the ability for law enforcement to be able to combat cybercriminal activity online.

The new Conventions' substantive criminal law provisions should be specific and clearly articulate the underlying criminal conduct. The Convention should also give due consideration to predicate offences and ancillary liability for cyber-dependent and cyber-enabled crimes. This should include the standard extensions of criminal liability included in instruments such as the UNTOC and UNCAC.

- Cyber-dependant crimes

Australia considers that the new Convention should include standards for criminalisation of offences directed at computer systems ('cyber-dependent crimes'). Australia proposes the following cyber-dependant criminal offences should be included in the new Convention:

- illegal access to any part of a computer system (including computer data) without right;
- illegal interception of transmissions of computer data without right;
- illegal interference with computer data (including deletion, deterioration, alteration or suppression of computer data) without right; and
- illegal interference with the functioning of a computer system or network; and
- producing, supplying, distributing or obtaining malicious software for the purposes of committing another cybercrime.

- Cyber-enabled crimes

Almost all States' existing domestic criminal laws are adequate to capture familiar crimes, inter alia trespass, vandalism, theft, narcotics-related and other violent crimes.

The Convention does not need to reimagine these crimes simply because a computer system or digital technology was involved in their commission, if the use of a computer system in the commission of the offence doesn't change the character or seriousness of the offending behaviour.

However, Australia considers there are some 'traditional' crimes whose scope, scale and ease of commission have all been drastically increased by the speed, anonymity, and widespread reach that information and communications networks provide. These crimes can be described as 'cyber-enabled' crimes. The Convention should address these crimes judiciously, by developing a clear framework for identifying why certain crimes are so significantly altered by a 'cyber element' they require a new harmonised international standard that elevates this conduct above 'traditional' crimes. The Convention does not need to create new categories of offences for every existing crime which may incorporate a 'cyber element', particularly where the severity, scale, scope or ease of commission of the criminalised conduct is not significantly altered by that element.

While Australia believes the Convention should adopt a restrained approach to including any new crime category, Australia is open to hearing arguments in support of broadening the Convention beyond cyber-dependent crimes to 'cyber-enabled crimes'.

To this end, Australia noted with appreciation the many calls to address the severe threat posed by online child sexual exploitation and abuse during the first session of the AHC. Australia considers this an issue where countries can constructively reach consensus. In recognition of this serious criminality, Australia has separately made a proposal. for offences covering online child abuse, including online grooming and livestreaming.

Australia also sees the significant increase in cyber-enabled fraud and theft, including ransomware related extortion, as a widespread issue where States may reach consensus to criminalise this conduct for the purposes of Convention.

- The link between criminalisation and procedural powers

Australia recognises States may wish to ensure the Convention improves international cooperation for familiar crimes with or without a cyber dimension (such as trespass or murder), by providing a framework for requests and access to electronic evidence located in another jurisdiction, in relation to the commission of such crimes.

The procedural powers, investigative powers, and international cooperation frameworks of the Convention to detect, investigate and prosecute cybercrime should apply to the offences listed in the Convention, but should not be restricted to apply only to those offences.

Procedural powers (expanded upon below) under the Convention should apply to other criminal offences committed by means of a computer system or digital technology, as well as the collection of electronic evidence required to detect, investigate and prosecute criminal offences that do not involve a computer system in their commission, that meets the required conditions and thresholds for those procedural powers.

Similarly, the framework for international cooperation under this Convention should apply not only to the criminal offences created by the convention, but, where appropriate, to other criminal

offences committed by means of a computer, as well as the collection of electronic evidence required to detect, investigate and prosecute a kinetic criminal offence.

Therefore, the purpose of the criminalisation chapter is not to restrict the operation of other chapters of the Convention, but, rather, to establish a common standard for a relatively new crime type – cybercrime – across all States.

Procedural measures to combat cybercrime

Procedural law is a critical element for investigating and prosecuting cybercrime. The Convention should provide a clear framework of procedural measures to ensure law enforcement authorities can obtain the evidence needed to combat cybercrime, underpinned by robust procedural safeguards and limitations that uphold the rule of law, and protections for human rights and fundamental freedoms. The Convention's articles on procedural measures should also respect existing frameworks, and avoid fragmentation of existing international instruments.

Procedural measures should apply to the substantive criminal offences within the Convention, and, consistent with states' domestic legal frameworks, to other criminal offences committed by means of a computer system or digital technology, as well as the collection of electronic evidence required to detect, investigate and prosecute a kinetic criminal offence, that meets the required conditions and thresholds for those procedural powers.

Australia Proposes the following procedural measures should be included in the new Convention:

- Orders for the preservation of electronic data (including stored content data, subscriber information, and traffic data);
- Orders for the production of electronic data;
- Search and seizure of electronic data;
- Real-time collection of electronic data (including traffic data and live interception of content data); and
- Orders for emergency / expedited preservation and production of data

Procedural measures should account for the nature of electronic data, ensuring that data is preserved quickly and effectively, and law enforcement and other relevant authorities can obtain such data quickly and effectively to ensure criminal methodologies and practices in cyberspace do not disrupt authorities' collection efforts.

- Conditions, requirements, and safeguards for procedural measures

Procedural measures for detecting, investigating, and prosecuting cybercrime can engage obligations with respect to human rights and freedoms under relevant international human rights instruments, including the International Covenant on Civil and Political Rights (1976). These may include, inter alia:

: Fair trial and fair hearing rights (ICCPR Article 14)

Article 14 of the ICCPR contains fair trial and fair hearing rights, including procedural guarantees, the rule of law and the presumption of innocence. The United Nations Human Rights Committee has stated that 'article 14 of the Covenant aims at ensuring the proper administration of justice and to this end guarantees a series of specific rights'.

Article 14 is not an absolute right, it is subject to permissible restrictions provided those restrictions are prescribed by law and are reasonable, necessary and proportionate means for pursuit of a legitimate objective.

: Freedom from interference with privacy (ICCPR Article 17):

Article 17 of the ICCPR establishes the right to freedom from interference with privacy and provides that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence'.

The content of this right is outlined in greater detail by General Comment No. 16 of the Human Rights Committee. It states that such protections 'are required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons'. Paragraph 3 of General Comment No. 16 states that the 'term 'unlawful' means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.'

: The right to freedom of expression (ICCPR Article 19(2))

Article 19 of the ICCPR provides for the right to freedom of expression. Article 19(2) of the ICCPR recognises the right to seek, receive and impart information and ideas through any medium, including written and oral communication, the media, broadcasting and commercial advertising.

The right to freedom of expression is not an absolute right. Under article 19(3) freedom of expression may be limited as provided for by law and when necessary to protect the rights or reputations of others, national security, public order, or public health or morals. Limitations must be prescribed by legislation necessary to achieve the desired purpose and proportionate to the need on which the limitation is predicated.

The objective of the Convention and its procedural measures is to reduce the threat, impact, and damage of cybercrime – which may provide a permissible basis for restricting human rights and freedoms when lawful, reasonable, necessary and proportionate.

It will be imperative for the procedural measures set out in the Convention to be established, implemented, and applied subject to the conditions and safeguards provided for under the ICCPR and other applicable human rights instruments.

Such conditions and safeguards should include, inter alia and as appropriate for each procedural measure:

- judicial or other independent supervision / oversight;
- grounds justifying the application of the procedural measure;
- limitations on the scope and duration of the procedural measure; and
- consideration of the impact of procedural measures upon the rights, responsibilities and legitimate interests of third parties.

General provisions

General provisions should include:

- a statement of purpose that is clearly focused on combatting cybercrime
- scope of application that is targeted and clearly defines
- agreed definitions, which should be discussed and agreed only after the substantive articles of the Convention are settled

The nature of cyberspace, as distinguished from physical space, adds complexities to the application and interpretation of international law rules and principles, including the principle of state

sovereignty, and to the application of territorial jurisdiction. Australia suggests that discussions on how these legal issues might be addressed in the Convention continue in parallel to the elaboration of substantive provisions.