Ad Hoc Committee to elaborate a comprehensive international Convention on Cybercrime
Australian submission on scope, objectives, and structure

29 October 2021

Australia welcomes the opportunity to submit its views on the scope, structure, and objectives of a new international Convention on cybercrime. The new Convention offers an unrivalled opportunity to secure widespread consensus on international cooperation to counter cybercrime, enabling states to better combat this pervasive and constantly evolving threat.

A new Convention will only be valuable if it can secure widespread support among the majority of UN Member States, based on consensus agreement obtained from good faith discussions under the auspices of the Ad Hoc Committee (AHC) established by General Assembly Resolutions 74/247 and 75/282. To this end, Australia is committed to an open, inclusive, transparent, and multi-stakeholder process, which offers the best chance of ensuring States can arrive at an outcome acceptable to the broadest number of States. This is in line with the principles set out in Australia's past national submissions to the AHC, and joint submissions which Australia has joined. Australia takes this opportunity to reiterate the points made in those submissions.

Cybercrime threatens all States, but it poses particular challenges for small States. Effective international cooperation on cybercrime is especially important for Small Island Developing States (SIDS), to help enhance their domestic capacity to combat transnational cybercrime operations. It is imperative that SIDS are able to engage meaningfully in the work of the AHC. Australia is committed to ensuring there are adequate opportunities for Pacific Island Countries to participate in the work of the AHC. Australia welcomes the decision to support hybrid participation for AHC sessions and emphasises the importance of ensuring adequate preparation and participation time for smaller delegations.

Private sector entities play a unique and invaluable role in addressing cybercrime. To succeed, the work of the AHC must therefore take account of the valuable expertise provided by industry stakeholders. States should also be responsive to the vast insight and expertise that other non-state actors, such as civil society organisations, academics and intergovernmental bodies, can contribute to the discussion on how best to combat cybercrime. To ensure well-informed discussions and effective outcomes, the AHC should afford these groups as many opportunities as possible to contribute.

Scope

Given the short timeframe for negotiations, States have limited time to reach agreement on the many issues that comprise a new Convention. The scope of the Convention must be clearly defined and should focus closely on the criminal justice response to cybercrime. It should not address broader cyber security issues that are addressed in other fora.

To accelerate our work, States should focus their attention on areas where common approaches to cybercrime are needed. The AHC's work should adopt concepts and terminology related to cybercrime and international cooperation on criminal justice that are already well-understood by the international community. We do not need to 'reinvent the wheel' nor do we wish to create ambiguity.

The new Convention should therefore draw heavily from the UN Convention against Transnational Organised Crime (UNTOC) and the UN Convention against Corruption (UNCAC), as well as from other concepts that have been agreed by consensus at UN Crime Congresses and in other UN fora, as appropriate. It should be informed by effective existing international instruments that States have already adopted at the international and regional level – such as the Council of Europe Convention on Cybercrime (the Budapest Convention) – and must avoid undermining existing norms established in

those agreements. This is in line with the mandate provided by Resolution 74/247, which urges the AHC's work to take 'into full consideration existing international instruments and efforts at the national, regional and international levels'.

In particular, the Convention should continue to use the term 'cybercrime'. This term reflects a widely understood concept that has been used in countless UN documents, including the outcome documents of the twelfth, thirteenth and fourteenth UN Crime Congress, as well as in UNGA resolutions (most notably resolution 65/230) and many other resolutions and reports of the Commission on Crime Prevention and Criminal Justice and the ECOSOC.

Treaty elements (Structure and Objectives)

Criminalisation

The new Convention offers the opportunity to substantially improve international cooperation in relation to cybercrime. Harmonised standards for a core set of cybercrime offences will increase States' ability to respond to cybercrime on a global, regional, and domestic level.

To this end, Australia considers that the Convention should take a focussed approach to those types of criminal conduct that have been substantially altered by cybercrime. States' domestic criminal laws are typically more than adequate to define familiar crimes, like trespass, vandalism, theft, narcotics-related and violent crimes. The Convention does not need to reimagine these crimes, simply because a computer or information system was involved in their commission.

The new Convention must include new standards for criminalisation of offences which can only be committed by use of information and communications system – known variously as 'pure cybercrime' or 'cyber-dependent crime'. These crimes did not exist before the advent of information and communications networks, and States' domestic criminal laws are often insufficient or inconsistent in their application to these crimes. In this realm, harmonised standards for criminalisation will offer considerable benefits for States, both in terms of their own domestic efforts to combat cybercrime, and in facilitating greater international cooperation.

Similarly, 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 are sometimes 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' as to 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 or scope of the criminalised conduct is not significantly altered by that element.

Australia considers there are two obvious candidates for the category of 'cyber-enabled' crimes which should be included in the Convention: the severe threat posed by child sexual exploitation and abuse online, and the widespread and significant increase in cyber-enabled fraud and theft, including ransomware-related extortion. Australia is open to hearing arguments in support of other 'cyber-enabled' crimes, but, for the reasons outlined above, the Convention should adopt a restrained approach to including any new crime category.

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. Given the role of technology in facilitating

cybercrime, the Convention should also consider a harmonised criminal standard for offences involving the production, procurement or provision of technology and software adapted solely or primarily for the commission of cybercrimes.

Cybercrime is a rapidly evolving area, and cybercriminals consistently look to deploy new technologies and methodologies to expand their activities and evade law enforcement. To counter this, the Convention must ensure criminalisation standards are drafted in a 'technology and methodology neutral' fashion, to ensure the treaty remains relevant and effective into the future.

Procedural measures to combat cybercrime

Procedural law is a critical element of 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. The scope of any 'procedural measures' framework should support clear domestic laws, which are robust enough to allow for law enforcement or other relevant authorities to combat the challenges of cybercrime, including detection, disruption, prevention, investigation and prosecution.

Procedural measures should also account for the nature of electronic data, ensuring that 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. Types of procedural measures could include search and seizure powers, production of data powers (such as access to stored communications and interception activities), and emergency or urgent requests or orders for the disclosure of such data. Procedural measures must be underpinned by robust safeguards and limitations that adequately protect human rights and the rule of law.

States will likely need to consider how state practice relating to the collection of electronic data across jurisdictions will be captured within a new Convention.

International cooperation and technical assistance

Cybercrime is overwhelmingly transnational. International cooperation, supported by harmonised criminalisation, is crucial to States' ability to effectively investigate and prosecute cybercriminals.

The international community has made significant progress on international cooperation on criminal justice in past decades, developing effective tools across a range of existing international treaties governing mutual legal assistance, extradition, and other forms of international cooperation. The provisions of the UNTOC and UNCAC, for example, provide an excellent basis for such cooperation, and have been almost universally adopted.

The new Convention should draw as much as possible from similar UNTOC and UNCAC provisions in relation to mutual legal assistance, extradition, transfer of prisoners and recovery of proceeds of crime. These provisions have proven effective and enjoy broad international support. In line with the mandate provided by Resolution 74/247, the new Convention should also ensure it complements and does not undermine other existing mechanisms for international cooperation on criminal justice.

Other international and regional regimes provide effective frameworks for international cooperation to counter cybercrime, underpinned by robust safeguards and limitations. The new Convention should draw from these as much as possible. Chief among these is the Budapest Convention, which continues to provide an effective basis for international cooperation among a large number of States from all regions of the world.

In addition to international cooperation, the new Convention should provide a meaningful boost to efforts to improve international capacity to combat cybercrime. This language should reaffirm the UNODC's principal role in providing technical assistance and capacity building, including as the convenor of the Global Programme on Cybercrime.

Safeguards to protect and promote human rights

State access to individuals' electronic and telecommunications data, by its very nature, impacts individual rights. The Convention must reaffirm the responsibility of States to promote and protect individuals' human rights in their efforts to combat cybercrime, consistent with international human rights law.

Individuals' rights to privacy and to freedom of opinion, expression and association must all continue to be adequately protected, in line with existing international standards. Other rights that must also be protected include the right to a fair trial, including equality before the law, as well as freedoms from torture and inhuman or degrading treatment or punishment, arbitrary detention, and discrimination. The international community has repeatedly reaffirmed that these rights apply online just as they do offline, and the Convention should reiterate States' existing responsibilities to uphold these rights in the course of their counter-cybercrime operations.

Structure and method of work

Once States have had the opportunity to express their views in relation to the scope of the Convention at the first negotiating session in January 2022, Australia anticipates a consensus on the structure for the Convention will emerge quickly.

After States have expressed their views as to scope, structure and objectives of the new Convention in January, Australia proposes that States be invited to submit proposals on clauses to be included under each structural element of the new Convention (for example, proposals on 'criminalisation', on 'international cooperation', etc.). The Chair, in consultation with the Bureau as necessary, should then work to synthesise these various proposals into a draft, which States can then negotiate, with each set of clauses to be considered in turn according to a workplan established by the AHC at its first meeting.

Following initial negotiations on each element of the structure, the Convention can be further negotiated as a whole, again according to a workplan established by the AHC at its first meeting and managed by the Chair thereafter.