Annex to ICC Cybersecurity Issue Brief #2

Substantive considerations on an international instrument on cybercrime

Acts of cybercrime cross borders more often than not. Therefore, international cooperation is at the core of effective prosecution. However, this kind of cooperation requires that the offences are commonly understood and clearly recognised by all parties involved. Henceforth, building a comprehensive and robust international regulatory framework that will define the scope, set the objectives and describe the mechanisms of tackling cybercrime, is essential. An international framework would not only facilitate international cooperation but also bring a common understanding to developing national legislations in harmony, that collectively tackle cybercrime. In this Annex, the International Chamber of Commerce (ICC) describes a set of considerations to bring such an instrument into force.

1. Purpose and desired outcomes

A globally agreed convention on cybercrime has the potential to reach shared understanding on matters related to cybercrime, set common ground for action and inspire international cooperation to ensure a more stable, secure and trusted digital environment. At the same time, it runs the risk of bringing further complexity and confusion into this space if its provisions duplicate or contradict existing frameworks, or of being operationally deficient if it fails to take account of the complexity of practical international cooperation on crime of this kind.

A global convention should intend to supplement other existing instruments in the field and be based on existing frameworks, such as the Council of Europe Convention on Cybercrime (Budapest Convention)[1] and its additional protocols, the United Nations Convention against Transnational Organized Crime[2] (UNTOC) or the United Nations Convention against Corruption[3]

[1] The Budapest Convention, a criminal justice treaty developed by the Council of Europe and opened for signatures in 2001 is, to date, the most relevant international agreement on cybercrime and electronic evidence. It aims to provide states with (i) the criminalisation of a list of attacks against and by means of computers; (ii) procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards; and (iii) international police and judicial cooperation on cybercrime and e-evidence. It is complemented by two additional protocols, one concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems that entered into force in 2006 and one on enhanced cooperation and disclosure of electronic evidence, developed with the support of business and opened for signatures in 2022.

[2] United Nations, 2004, United Nations Convention Against Transnational Organized Crime and the Protocols Thereto, (https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html)

[3] United Nations, 2004, United Nations Convention Against Corruption, (https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf)

(UNCAC). Further, it should avoid duplicating or including provisions that conflict with instruments already in place.

The convention's priority should be **increasing effective international cooperation between national law enforcement and prosecutorial agencies to reduce the incidence of major cyber-dependent criminal activity** as well as to protect the victims of such crimes.

To that end, the scope of the future convention should be

- clearly and narrowly defined,
- include appropriate safeguards to ensure robust independent oversight and effective redress mechanisms,
- minimise and avoid conflicts with existing laws,
- create mechanisms to prevent conflicts
- and resolve disputes that arise.

If national frameworks can develop in harmony to address cybercrimes in a domestic context then this will also help to create the foundation for effective international cooperation. Failing that, the convention could run the risk of undermining and fracturing existing efforts to fight cybercrime and could also produce unintended negative consequences for legitimate commercial and non-commercial activity of all kinds and gravely impact human rights.

In addition, a new convention provides an opportunity for **greater collaboration between governments and experts from the private sector, civil society and the technical community**. Such collaboration would help ensure the convention's provisions are future proof and technology neutral, and will enable continuous exchange of views on new and emerging threats and potential mitigations, thus adding to the security and stability of the online environment.

A new convention could also provide a legal framework for **capacity building to enable the effective investigation and prosecution of cybercrime globally**. Today, countries are at vastly different levels of readiness when it comes to cybercrime investigation and prosecution. Work is needed to empower authorities to prevent and counter cybercrime irrespective of where they are in the world, as criminals continuously evolve and adapt their tactics. A new convention could provide a framework for training programmes in this area as well as technical assistance to support the implementation of the convention.

2. Defining cybercrime and the scope of a global convention

Given the globally accepted principle that a person shall face penalties only when their actions constitute a violation of the law, one's conduct can only be determined as a crime in accordance with the legal rules.

The convention should provide a definition and scope of each crime it covers, including descriptions of what types of activities/conduct are regarded as illegal conduct. As these definitions form the base for the establishment of penalties and compliance requirements once the convention is transposed into national law and implemented, it is imperative these definitions are clear, narrow, precise and carefully written to avoid unintended interpretation.

1) **The convention should focus on serious crimes that are cyber-dependent**[4], such as illegal access. Far too often, even very serious cyber-dependent crimes do not attract punishment that fits the act, and that problem is growing. The convention will be considered a success only if it effectively addresses this situation. A focus on serious crime, such as illegal access, will also help streamline the processes and procedures related to transboundary enforcement as well as raise the prospect of reaching consensus between states which, consequently, could increase the number of signatories to the convention. Furthermore, to ensure a clear scope of application, all provisions, including procedural and law enforcement measures, should only relate to a precisely defined set of crimes covered by the convention and not be expanded to other ICT-related crimes.

2) **The provisions on criminalisation should, in principle, align with those in the Budapest Convention[5] and include offenses against the confidentiality, integrity and availability of computer data and systems[6]**. Examples include access, interception, data and systems interference and misuse of devices. These could include elements such as, but not limited to, the following:

   a) Unauthorised access (e.g., hacking): breaking into others' computer or related equipment by, for example, entering another's account code and password without authorisation, breaking into a protection measure or taking advantage of a loophole of such system.

   b) Unauthorised system interference (e.g., denial-of-service attacks): interfering with the computer or related equipment of another person and causing injury to the public or another through the use of computer programmes or other electromagnetic methods.

   c) Unauthorised data interference (e.g., phishing): obtaining, deleting or altering information of another's computer or related equipment without authorisation, causing injury to the public or others.

3) **Inclusion of provisions on offences covered by other conventions, simply because those offences leverage ICTs, should be avoided**, as this would create unnecessary duplication. Such offences may include, *inter alia*, corruption, trafficking, terrorism or drugs. Duplication raises the real risk of causing confusion, contradicting or conflict of laws during implementation and risks losing focus on a targeted, practical, effective instrument to tackle cybercrime effectively. When mentioning such crimes in the context of this convention is essential, due reference should be made to the other convention(s), clearly noting any amendments or accompanying obligations proposed to the source instrument. The convention should avoid giving rise to potentially conflicting interpretations where (elements of) the crime fall under the purview of several conventions. In such cases, the convention should seek to offer clarity on which of the convention's provisions take priority.

---

[4] International Criminal Police Organization – INTERPOL, 2021, National Cybercrime Handbook, (https://www.interpol.int/content/download/16455/file/Cyber%20Strategy%20Guidebook.pdf)

[5] Council of Europe, March 2022, Convention on Cybercrime: Special edition dedicated to the drafters of the Convention (1997-2001), (https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e)

[6] The Budapest Convention refers to *"computer systems"*, however we recommend using the term *"ICT systems or devices"* to ensure that the Convention reflects the evolving nature of cybercrime and current technology.

4) **Dual criminality must be the basis for defining crimes under the scope of the convention.** This will be important for states and service providers alike, who need to understand the instances in which states can be expected to legally request information. Without this standard, certain conduct may not be understood to be the same or similar enough of a crime in all relevant jurisdictions. Such understanding is a necessary prerequisite for cooperation in this space. Where it is necessary to establish dual criminality, the future convention should also **leverage agreed-upon language as much as possible**. Existing instruments, such as the UNTOC, UNCAC, and other widely accepted instruments, such as the Budapest Convention, can provide guidance and help in this regard. Therefore, the exact text of these conventions should be used, whenever possible, since such provisions have already been transposed into national legislation across the world. Introducing differences in similar provisions across instruments could result in unintended negative consequences and create confusion which can produce delays, increase costs or in some cases even frustrate cooperation entirely.

5) **Novel cyber technologies and criminal activities, such as intentionally developing, spreading and using malicious computer code, to attack government systems, critical infrastructures or ICT supply chains should be considered for inclusion in the convention**. These are all ultimately aimed at facilitating cyber attacks by deploying, selling and/or spreading (making available/ hosting) malicious cyber tools. The evolving criminal Access-as-a-Service (AaaS) ecosystem provides various tools and methods to ultimately orchestrate cyber attacks for profit. ICC encourages the Ad Hoc Committee to consider what the convention can do to thwart the proliferation of offensive cyber capabilities (OCCs) done for malicious or criminal purposes.

   The proliferation, i.e., the distribution, sale or offering for sale of hardware, software or other criminal tools used to commit cybercrime, was criminalised in some countries. Further discussion shall be conducted to determine whether in the international convention "proliferation" shall be defined as a crime.

6) **The convention should not treat traditional crimes as cybercrime merely because a computer was involved in the planning or execution of the crime.** It is important to remember that these types of activities can be and are adequately covered by other statutes. For example, terrorism-related offenses, arms trafficking or counterfeit medical products should not be addressed by these new treaties as these activities are already covered by other existing treaties. Including these topics raises the risk of creating confusion and contradiction, and will not help deliver a targeted, practical instrument that can improve our collective ability to tackle cybercrime.

   The new convention should only include illegal activity that is cyber dependent, except if the offenses are of the scale, scope or speed that they would not be feasible without ICTs. If necessary, such cyber-enabled crimes should be addressed through a subsequent protocol attached to the convention.

7) **The convention should not attempt to regulate content, given the different legal practices and cultural approaches to this area across the world.** There is simply not enough coherence in the definition of criminal acts involving content to find a common denominator that would be both specific enough to facilitate international cooperation and general enough to take account of the lack of compatibility of defining such acts. Similarly, the convention should specifically

avoid any commitments that would result in preventive content take downs, particularly if they could lead to hampering journalistic freedom or harming freedom of expression.

8) **When criminalising various actions, the convention should explicitly mention intentionality for each act.** For example, security and vulnerability research and disclosure, when appropriately coordinated with affected vendors and relevant authorities, should not be criminalised by the convention, since that would have the opposite effect and make the cyber ecosystem less secure, rather than more secure. In this respect, it would be useful to consider both the intent and effect of an action, where an act would be considered criminal when it leads to a certain effect, such as the interception, damaging, deletion, deterioration, alteration or suppression without right of computer data as per Arts. 3, 4 and 5 of the Budapest Convention.

   Furthermore, failure to include a threshold of "criminal intent" and effect allows other clearly lawful activities to attract an unknown level of liability. For example, if the convention addresses misuse of ICT devices without this threshold, a user could technically be accused of a crime subject to international enforcement when downloading an app that, unbeknownst to the user, has a flaw allowing it to be used as part of a botnet. The vendor of the app and potentially even the app store may also be implicated even though neither has the ability to know of the underlying problem.

9) **The convention should include specific measures to adequately protect, *inter alia*, security researchers or penetration testers**, who perform essential work to continuously test and improve our cyber defences. The convention should also recognise legitimate exceptions for what would otherwise be considered unlawful behaviour.

10) To facilitate countries' increasing international efforts to combat cybercrimes, **the definition and categorisation of these crimes should take into account the following factors: actors, conduct, rights/benefits intended to be protected by recognition of an act as a crime and the effect of the actions and subject of the crimes**.

In sum, given the rapid evolution of technologies and the need to ensure protection of human rights when it comes to criminal penalties, the following principles should be considered when defining cybercrimes:

- Clarity: The language shall provide sufficient clarity to help the implementation process, especially for the purposes of imposing criminal liabilities as well as providing a compliance baseline, and to ensure that the crimes in the convention are recognised similarly enough across all jurisdictions to facilitate enforcement;
- Precision: The description of the activities subject to criminalisation shall be precise and universally understandable;
- Intentionality and effect: The description of the activities to be criminalised should explicitly refer to intent and be based on the harmful effect that the activities may cause;
- Avoiding overlaps: The cybercrimes being targeted should not overlap with existing criminal sanctions covered by existing treaties;

In addition to the definition of cybercrime, all terms and provisions used throughout the convention should be aligned with established and agreed upon definitions, particularly those included in the Budapest Convention, as one of the most widely referenced statutes in this area.

The convention should not seek to introduce new definitions of widely applied concepts, such as obstruction of justice, liability and negligence. These types of acts may not always imply criminal responsibility and are not limited to cybercrime or to the online environment as such. Liability for securing data in particular is primarily addressed via data protection regulators and civil litigation across a number of jurisdictions rather than through criminal prosecution.

We further recommend for the convention to use precise terminology and clearly defined terms (e.g. avoid the unqualified use of terms such as "wrongful" and "lawful"). This would also include criminalising serious cybercrime offences where "clear criminal intent" can be established, rather than relying on terms such as "dishonesty" and "illegitimacy", which can carry various meanings across different jurisdictions.

Similarly, we would recommend for the convention to use precise terms such as "unauthorised access", "electronic data", and "ICT system or device" rather than broad terms such as "avoiding security measures", "access to information" and a "computer system".

While definitions must strive to be as precise as possible, they should remain technology neutral and flexible enough to ensure the convention is future-proof and adaptable to the rapid development of technology.

3. Procedural measures and safeguards of a treaty

To safeguard end-users against potential abuse of executive authority, the scope of application of all procedural measures set forth in a future treaty needs to be exclusively limited to crimes set forth in the convention. We would in particular recommend this section to refer to specific articles in the criminalisation section and would caution states against including general references to "ICT crimes" or "any other crimes".

Such references might inadvertently obligate one state to apply the treaty's law enforcement provisions to investigations or prosecutions of ICT acts considered to be criminal by another state even if (a) such crime is not part of the agreed set of crimes in this text or (b) such crime is criminalised in only one of the two jurisdictions.

Furthermore, the convention should not contain any provisions that could potentially open the door to expansive claims of extraterritorial jurisdiction by establishing jurisdiction over a crime committed in one country due to services being offered elsewhere. The same applies to potential demands for data that would conflict with existing legal obligations (e.g. blocking statutes) or that would prevent/hinder effective international cooperation.

To protect rights of end-users, purpose and reach of government access to data needs to be narrowly tailored to meet specific public safety and national security needs.

1) **Existing international regulations on cybercrime should serve as inspiration for a relevant framework on procedural measures**. There is a common perception that procedural powers are necessary in order to adequately respond to cyber-related crimes, and that these include:[7]

   a) preservation, collection and disclosure of different kinds of data;

   b) search, seizure and transfer of stored data;

   c) production orders.

2) **In addition to the criminalisation of substantive offenses, the convention should address the need for domestic legal authorities to preserve, collect and share electronic evidence**, where possible, bearing the potential costs that it entails, consistent with due process and the protection of human rights and fundamental freedoms. The issues around access to data for crime prevention and enforcement are extremely complex and as a result present considerable risks of unanticipated negative consequences. Here are just a few of the issues which the convention should address around this topic:

   a) The convention should **clearly identify the types and categories of data subject to government access** and the specific authorities required to fulfil data safety and national security needs.

   b) The convention should require strict and transparent data minimisation, retention and dissemination limits**,** and impose custodial obligations on the entities that will hold any data provided - and ensure it is not subject to undetected unauthorised modification.

      The convention should recognize that real-time access to data will not always be technically possible, that data retention requirements mean that many types of data cannot be retained for long periods – and that providers may be legally prevented from doing so even when it is technically possible.

      Additionally, the convention should not be used to indefinitely extend retention periods by deferring to domestic laws. Instead, it should provide a specific limit, as the Budapest Convention does (ninety-day limit). The convention should not allow for bulk collection of information. Demands should include specific account identifiers and should be limited to seeking data that is necessary and proportionate to the particulars of the specific case.

   c) The convention should allow technology providers an opportunity to challenge government demands for data on behalf of their customers, including those based on potential conflicts of law, to ensure that governments are acting within the law and are respecting the rights of the providers and their users. It should contain provisions to address conflicts of law and mechanisms to resolve such conflicts that will inevitably arise. Providers cannot be asked to break the law in one jurisdiction to provide data to another.

   d) The convention should not negatively impact data protection, privacy, freedom of expression or other human rights of natural persons. In particular, the convention's

[7] See Articles 23–29 of the Arab Convention on Combating Information Technology Offences, Article 31 of the African Union Convention on Cyber Security and Personal Data Protection, Articles 16–21 of the Budapest Convention and Articles 33–38 of the Russian UN draft Convention on cybercrime.

provisions related to the real-time collection of traffic or content data need to be carefully evaluated against existing data protection obligations to avoid potential conflicts of laws.The convention should contain a provision which introduces conditions for prior approval of an access request to be obtained from an independent judicial or administrative body. This would allow for a preliminary review of the reasoning behind the compelled access and help prevent violations of private rights by potentially non-compliant requests

e) Legally binding remedies should be available to data subjects in the event of a breach by the government of the access, use and retention rules. If the information obtained through obliged access is later used in a criminal prosecution, those being prosecuted should have the right to obtain and challenge it. Furthermore, the convention should include the right to redress for any individual whose rights were violated through the exercise of powers set forth in this convention.

f) The convention should explicitly recognise that the public has a right to know how governments may access their information and under what circumstances third parties may be obliged to provide it to public authorities. This could be achieved by explicitly recognising the right for service providers to give users notice of government requests to access information, thereby preserving the rights of those users to object to certain uses or disclosures of their data, especially where doing so does not interfere with or otherwise compromise an ongoing investigation or prosecution.

3) **An expansion of procedural powers inevitably calls for the considerations of third parties**, i.e. that when adopting new procedural powers or instruments, the rights, responsibilities and legitimate interests of third parties need to be weighed. Businesses are routinely requested to cooperate in criminal investigations. Taking their views into account will mean that the rules of today will adapt to the evolution of technology. In addition, the private sector is well suited to understand where and when cybercrimes might be planned and how they may be committed (e.g. through various incremental steps in a supply chain). They are, therefore, essential partners when defining cybercrime and establishing what kind of procedural mechanisms are needed to detect and investigate such crimes.

4) **Safeguards**. The intrinsic tension between effective investigation by law enforcement and the protection of fundamental human rights needs to be legally addressed and asserted through safeguards. An umbrella provision establishing the core principles under which all procedural rules and powers are to be applied and, by extension, the rules to be imposed, is necessary. In the context of international law, enforcing such minimum guarantees is not unusual.[8]

5) **Protecting fundamental human rights**. Provisions of this convention should not give ground to misinterpretation that might serve to limit fundamental human rights, such as the right to freedom of speech or the right to privacy. The protection of fundamental human rights needs to be equally considered when developing procedural measures.

[8] See for example Article 33 of the African Union Convention on Cyber Security and Personal Data Protection, Article 15 of the Budapest Convention, Article 32 of the Russian UN Draft Convention on Cybercrime and Article 9 of the UN Convention Against Transnational Organized Crime.

6) **Procedural measures aimed at combating crime can interfere with fundamental human rights and freedoms**. Therefore, an international framework needs to highlight that fundamental human rights and freedoms should be equally ensured within the entire jurisdiction – both offline and online and regardless of national borders and legal systems. Human rights and rule of law benchmarks could limit the use (or abuse) of procedural powers and foster closer integration of telecommunication operations between countries with different types of governance structures (predictable legal frameworks for private parties operating in different types of jurisdictions).

   The convention should reflect that, except in narrowly defined circumstances, the public has a right to know how, when and why governments seek access to their data. Transparency in the conduct of law enforcement authorities is needed, with obligations in place to provide notice to impacted individuals, provided that does not compromise an investigation. Overall, however, secrecy should be the exception rather than the rule to ensure that users are able to assert their rights and privileges. This is necessary to preserve trust in the online ecosystem as well as in the rule of law.

7) **Liability/responsibility of third parties**: As a default, the convention should not create liability for third parties, but encourage and permit the production of timely mitigation measures in case ICT vulnerabilities are detected. Liability/responsibility regulation in the different jurisdictions should be honoured. Definitions of third party liability differ across jurisdictions for good reason. Disturbing these arrangements through international obligations in one area is very likely to lead to unanticipated negative consequences in other areas. The example used above, with respect to criminalisation of device use without careful limitations also applies here. Such an approach could create an unknown level of liability for hardware and software vendors and third parties which commercialise both. Any new procedural rules need to be drafted to ensure that third parties can cooperate with legal certainty based on clearly defined procedures including protection of end-users' fundamental rights. Furthermore, any requests must be proportionate to achieve well-targeted and clearly defined objectives while ensuring that parties' liability risk exposure is deliberately minimised.

8) **The convention should not seek to increase cyber resilience through the introduction of industry regulation.** Other means of regulating industry exist, but these should not be conflated with cybercrime policy, and thus, should not be included in this convention. The convention should focus on empowering public authorities in the prevention and investigation of cybercrime and the prosecution of cyber criminals. For the convention to remain an effective criminal justice instrument, it should also not seek to introduce measures in the area of data and consumer protection. Such provisions would likely come into conflict with existing laws and would at any rate fall outside the scope of criminal justice domain.

9) **The convention should explicitly protect whistleblowers, journalists, victims and witnesses**, reiterating and building upon the relevant provisions of the United Nations Convention against Transnational Organized Crime (UNTOC), particularly Articles 24 and 25.

4. Implementation and international cooperation

The possibility of further fostering international coordination and cooperation on cybercrime is important. Finding common ground on procedural issues to allow for expedited and efficient investigations should be an important objective of this convention. However, the rules on coordination and cooperation must be carefully crafted as parties will need to maintain sovereignty when, for example, they are asked to hand over data or extradite persons charged for cybercrimes conducted in another party's territory.

Taking the example of the Budapest Convention, common cybercrime regulations have been implemented in several jurisdictions. Costa Rica, Croatia, Finland, France, Germany and Spain are just a few examples.[9] This enabled successful investigative cooperation in a number of cases. For example, the convention served as an important tool for Georgia in its multinational investigations with non-European partners. By relying on the information shared by the U.S. Department of Justice's Office of International Affairs on the basis of Article 26 of the Convention, Georgia was able to prosecute the leader of a transnational organised cybercrime network which had used GozNym malware to target victims from multiple different countries and cause hundreds of millions of dollars worth of damage.[10]

As noted earlier, ICC sees the primary scope of this convention to enable, increase and strengthen international cooperation to reduce the incidenceof major cyber-dependent criminal activity in particular, and to protect the victims of such crimes. To achieve this scope, the drafting of the convention should take into account the following considerations:

1) The convention should **include a straight-forward provision highlighting that international cooperation is critical to effective cybercrime prosecution**. In contrast, it should **not contain provisions or language that opens the door to expansive claims of extraterritorial jurisdiction** and subsequent demands for data that would be at odds with existing legal obligations (e.g. blocking statutes) or that would hinder effective international cooperation.

2) As referenced above, **dual criminality must be the starting place for international cooperation on cybercrime**. Experience shows that transboundary crime cooperation is much more likely to be effective if all jurisdictions recognise the act as criminal.

   In the same vein, the convention should build on commonalities across jurisdictions. The scope of the agreement's measures should focus on widely understood criminal acts which have common, clear and compatible definitions in many different legal jurisdictions. This is fundamental as many elements of cross-border crime cooperation are greatly limited or rendered ineffective if the acts are not similarly understood in all concerned jurisdictions. Focusing on elements that are defined and understood similarly not only facilitates consensus in discussions and incentivizes cooperation, but also helps ensure that the convention is implementable.

---

[9] Cybercrime Convention Committee, The Budapest Convention on Cybercrime: benefits and impact in practice, 13 July 2020, p. 6–8 (https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac).
[10] Ibid, p. 15. (More information here, here and here.)

3) The convention should **avoid overly prescriptive provisions and establishing conflicting rules that raise barriers to international criminal cooperation**. Given the global nature of data flows, there is significant risk of conflicting national rules which represent substantial compliance costs. The convention should strive towards maximum flexibility and creating the least risk of conflict.

4) **A standing body, such as a Conference of the Parties, should be established to oversee the operation and effectiveness of the convention.** The convention should delimit particular roles and responsibilities for such a body. These rules should address, among other things, whether unanimous approval is required in order for the body to agree upon documents and decisions and if such documents and decisions are legally binding on parties. At the same time, it will be important not to constrain the body from performing future unforeseen functions necessary to ensure the convention's effective operation in line with its object and purpose.

   Given the role the technology industry has in this space, the convention should **ensure the meaningful participation of ICT companies in meetings of the Conference of the Parties**. Previous experience from regional bodies, such as the Council of Europe's Cybercrime Committee, has shown the value of public-private cooperation in this area. Such cooperation would be especially valuable to parties who have less experience with transboundary cybercrime cooperation, and would help all parties to work with concerned third parties on the complexities of data access and other requests, as well as the conflict of laws situations that will inevitably arise.

   Having said that, the creation of any new permanent commission or similar organisation, or the expansion of the existing organisations' scope of work to this space should be avoided as it might lead to conflation of other treaty commitments with those assumed under the present convention.

5) As a related matter, it will not be enough to simply come to a political agreement around text. **The convention's text needs to be reviewed before it is finalised to determine whether it will actually produce the intended results and do so without serious human rights violations or other unanticipated consequences**. That review should include organisations like EUROPOL and INTERPOL, the experts in the Council of Europe and UNODC, those in the private sector who work daily with law enforcement, other NGOs as well as law enforcement officials themselves. Only after this is done, and any advice is reviewed, should the convention be finally adopted by the General Assembly and opened for signature.

6) Any future revisions or amendments to the convention should take place through the same process as the treaty negotiations and be adopted through consensus.