GLOBAL COALITION TO FIGHT FINANCIAL CRIME

United Nations Cybercrime Convention
Comment Letter by GCFFC

1. Background and Context

The UN secretary-general was tasked in 2019 with collecting views of member states on the challenges that they faced in countering the use of information and communications technologies for criminal purposes. Common concerns regarding investigative co-operation, emerged from the report[1], namely:

- access to cross-border data and cloud storage
- slow mutual legal assistance processes
- the challenge of obtaining evidence, in particular working with the private sector
- differing legal statutes and definitions of crimes.

Some 5 years later and after many difficult negotiations a new UN Convention on Cybercrime[2] was announced as a response to these concerns. It is a triumph of international negotiation, and is long overdue. It is the first anti crime Convention passed at the UN in over 20 years so it's significance is obvious, especially when there is less international support for multilateralism these days. The Treaty was passed by the UN General Assembly in December 2024[3], without requiring a vote but has received support from the governments of the USA[4], the EU, the UK as well as from Russia, China and Iran. It will come into force 90 days after being ratified by the 40th Signatory, which is possible in 2025.

The Treaty[5] when implemented by countries, provides new opportunities for tackling all manner of cyber crimes by seeking to criminalise activity on a consistent basis and so to allow and enable increased international law enforcement co-operation, in the investigation and prosecution of cybercrimes. The Treaty takes much from the existing Council of Europe Budapest Convention[6] passed in 2001 and with 76 parties has been the "standard", which has informed this new UN Convention, but which has the potential for increased country adoption and participation.

Whilst the Convention will need 40 States to sign up before it comes into force[7], it can only be amended after 5 years have passed[8] (with a two thirds voting majority), the adoption of supplementary protocols[9] are possible with the support of 60 Signatory States and requires a two thirds voting majority of States Parties to pass.

Existing international law enforcement approaches to tackle traditional types of crimes offline and or via money laundering channels have struggled to reach the scale needed to address the problems of transnational organised crime so far, due to legal, technical and capacity challenges, which are likely to apply just as much if not more to online criminal cases.

2. Public Commentary

The Convention has received significant policy support, including from UN Secretary General Antonio Guterres who stated[10] that:

> *"This Treaty is a demonstration of multilateralism succeeding during difficult times and reflect the collective will of Member States to promote international co-operation, to prevent and combat cybercrime. The Convention creates an unprecedented platform for collaboration", in the exchange of electronic evidence, protection for victims, and prevention, while safeguarding human rights online".*

And from INTERPOL Secretary General, **Valdecy Urquiza** who stated[11] that :

> *"Cybercrime as a uniquely borderless threat that is increasing at a dramatic rate. Cyber attacks destroy businesses, undermine public institutions and endanger lives. Only by moving forward together in lockstep can countries effectively combat cybercrime. The UN Cybercrime Convention provides a basis for a new cross sector level of international co-operation, we desperately need*".

And from UNODC Executive Director **Guada Waly** who stated[12] that:

> *"Technology has created opportunities for a greater scale, speed, and scope of crimes, from terrorism to drug trafficking to trafficking in persons, migrant smuggling, firearms trafficking and more. The Convention provides tools that will enhance international co-operation,, law enforcement efforts, technical assistance and capacity building related to cybercrime".*

Whilst law enforcement, for example INTERPOL and the UNODC have come out in strong support of the Treaty, and others in the technology sector[13] and in civil society, including Human Rights Watch and Amnesty International[14] have raised genuine and legitimate concerns, overall UN Member States, including some considered more democratic and others considered more autocratic have weighed up the pros and cons and decided to support the Treaty.

The Chair of the GCFFC, **John Cusack** has stated that:

> *"The GCCFC offers its conditional support to the UN Cybercrime Convention recognising the need for criminalising all forms of Cybercrime globally and more and better international co-operation in preventing and combatting Cybercrime. Nevertheless, States will and must differ on when and with whom to co-operate, which will limit increasing co-operation even in legitimate cases, and supporting countries should reflect that the aims of the Treaty to prevent and combat cybercrime is more likely to be achieved with more than international law enforcement co-operation, which includes involving the private sector and requires legal cross border information sharing gateways, with privacy safeguards to be expressly promoted, which are not yet provided for in the Convention but must find their way into subsequent protocols".*

3. The Treaty & its Aims

The Treaty was proposed in 2019 by 29 countries[15] and led by Russia.

The new Treaty's aims are to

- *"prevent and combat cybercrime more efficiently and effectively"*
- "*strengthen international co operation*" and
- *"support technical assistance and capacity building".*

According to the UN[16], *"The Treaty recognises that in 2023, 67.4% of the world's population accessed the internet, according to the World Bank, with people relying on connectivity for tasks ranging from communication and shopping to advances in research and innovation. However this connectivity also exposes more than two thirds of the global population to the dangers of cybercrime. Cybercriminals exploit digital systems using malware, ransomware, and hacking to steal money, data, and other valuable information. Information and communication technology (ICT) are also used to facilitate crimes such as drug trafficking, arms smuggling, human trafficking, money laundering and fraud. Until now there has been no globally negotiated convention in cybercrime. The new convention against cybercrime will enable faster, better coordinated, and more effective responses, making both digital and physical worlds safer".*

4. Benefits:

Their are real positives to the Treaty.

- Firstly, reaching an agreement to internationally **criminalise** a broad swathe of cyber enabled crimes (expressly including sharing sexual images without consent, sextortion, grooming minors and child online sexual exploitation) will provide fewer safe havens for criminals involved in these activities and cyber dependent crimes (Internationally via signatories) is no small feat.
- Secondly, on providing gateways to improve **law enforcement cooperation**, where agreement has been reached with protocols on how to request, who to request from and how to obtain crucial electronic evidence which is key to investigating and prosecuting cyber criminals and targeting their proceeds and monies laundered. Existing law enforcement co-operation protocols exist which extend to requesting and providing evidence of many cyber and other crimes under the Council of Europe's Budapest Convention[17] but this Treaty has just 76 signatories and in most cases include traditional supporters of human rights and so are prepared to co operate and exchange information with each other, on this basis. These countries are also the places that are home to much information on servers in data centres, including e-mail address and social media data and are subject to data protection safeguards. The UN Treaty provides a mechanism for third countries to benefit from co-operation from these countries which are likely to become signatories and other countries that may not qualify or feel comfortable signing up to the Budapest Treaty.
- Thirdly, on securing **legal and human rights** protections, the Treaty provisions are designed to prevent States from benefiting from the provisions of the Treaty if their activities, in requesting and or investigating or prosecuting cases flout legal and other human rights.
- Fourthly on **awareness and training,** the Treaty emphasises prevention and urges Countries to invest in training for public and private sectors as well as initiatives to raise awareness about cyber crime risks.
- Fifthly on **victim support,** the Convention also prioritises justice for victims and encourages Member States to provide support services, compensation and legal restitution.

5. Concerns:

Whilst the GCFFC conditionally support the new Treaty, there are concerns which need to be addressed and or monitored as the Treaty is implemented in order for it to overall generate positive outcomes. For example:

- Firstly, whilst the **criminalisation** of many types of activities that represent problematic cyber crimes is welcome, and will help to ensure no country is a safe haven for cybercriminals, passing domestic laws criminalising these activities is just a first step. In countries where, for example State support for cyber criminality exists, passing laws alone will have little impact, and in countries where state embedded organised crime and or corruption are at elevated levels, again the impact of these actions will be very limited.
- Secondly, countries accessing co-operation internationally may have the benefit of improved procedures and processes, but substantive cooperation including the exchange of actual information may well remain limited, particularly from countries where most of the important data is stored. Democracies and other signatory countries already have the ability to request and receive much of the data and electronic evidence from other democracies, under the Council of Europe Budapest Convention, which requires **legal & human rights (freedom of expression and privacy rights)** safeguards to be in place prior to acceding to any request. If countries that have poor legal and human rights records request information from countries with better legal and human rights

records then they may find their requests are unsuccessful. This may not be limited to investigations that target foreign critical journalists, researchers, think tanks, NGOs etc where their freedom of expression should be protected and any request should be rejected if the Treaty provisions are being applied properly, but also to requests from countries where investigations are conducted without fair independent judicial authorisation and oversight and or where prosecutions are carried out where the accused is unlikely to receive a fair trial. There may be a role for an intermediary such as INTERPOL who could act as both a clearing house and independent initial arbiter of such matters if appropriate protocols could be agreed.

- Thirdly, upholding **privacy rights** are also important. By extending the ability of law enforcement in one country potentially to be able to in effect intercept and surveil and to coordinate investigation and enforcement actions against foreign persons presents obvious concerns in terms of privacy. Electronic data can provide many personal details about people's lives, including their health, economic and financial activity, private relations including sexual preferences and political and social opinions. When collecting electronic data about a possible cybercrime, investigators often have to sift through much more information which is irrelevant to the crime in order to find any actual relevant evidence, and much more than when carrying out a traditional offline investigation. The risks of privacy infringements in such cases is obviously much greater as a result and investigators by their nature operate in secret and are subject to little independent oversight or obligation to provide transparency as to their actions. Whilst the EUs European Data Protection Supervisor (EDPS) Wojciech Wiewiórowski, referring to the proposed UN Cybercrime Convention stated[18] that: *"Exchanging personal data between EU countries and non-EU countries to combat cybercrime comes with great responsibility. Strong safeguards must be put in place to ensure that the protection of individuals' personal data in a non-EU country is not undermined, especially when sharing sensitive data related to alleged criminal activities", this* is not particularly helpful and is just a restatement of the current legal obligations. What would be more helpful is if the EDPS, EDPB and EU provided specific support and interpretation of the existing EU GDPR which would help facilitate compliant sharing of data i.e. how to navigate and interpret articles 9 (sensitive data) and article 10 (criminal data) and article 6 (purposes of processing including lawful measures, legitimate interests and public interest) of GDPR.
- Fourthly, the **awareness and victim support** provisions are just warm words with no specific measurable actions and will depend on decisions taken domestically, including making available resources for these purposes. The provision for **technical support** also needs strengthening[19] with technology transfers an important element of future support[20]. Funding commitments from leading Member States to agencies such as INTERPOL to drive this forward should be considered.
- Fifthly, the approach taken by the UN to **monitor implementation** of the terms of its Treaties by signatory States, through a Conference of the Parties process, the first to be held after 5 years and to be supported by the UNODC has shown to be largely ineffective for many financial crime related Treaty's. Compare this to the approach to tackle money laundering where FATF as an independent well resourced inter governmental body is able to hold signatory's States more to account and to have measures that can be taken to penalise non compliance.
- Sixthly, the Treaty doesn't go far enough to tackle the size and scale of cybercrime. This is not least because it is over relying on an **international legal and judicial law enforcement** approach to tackle cybercrime, which includes the online activities of criminals involved in all serious crimes, including drugs, arms, people, wildlife trafficking, fraud and scams and money laundering. Existing international law enforcement approaches to tackle these types of crimes offline and or via money

laundering has not achieved its aims, despite the effort and it is unlikely that approaching this in a similar way because it is online is likely to have any greater success. It is now well recognised that it takes international leadership and co ordination of both public and private sectors with collaboration, intelligence and information sharing and the use of technology to improve effectiveness. Within the private sector, the designers and operators of much of the digital world as well as other stakeholders such as those involved in combatting money laundering will need to take responsibility, supported by civil society. The UN Cybercrime Convention refers to *"strengthening co-operation, between law enforcement agencies or prosecutors and relevant individuals and entities outside the public sector… and private sector entities*" to prevent and combat cybercrime[21]. It also "*encourages service providers to take effective measures…to strengthen the security of the service providers products, services and customers*"[22]. These provisions fail to address this shortfall. One of the most prevalent and harmful types of cybercrime is represented by fraud and scams, where the digital world is exploited in order to exploit victims. For 40 recommendations to tackle fraud and scams, particularly cyber related fraud and scams see the work of the GCFFC APAC Chapter on Scams in East Asia[23], where service providers, for example telcos, technology companies, search, e-mail, social media, online platforms etc should be regulated and be required to have robust anti cybercrime programme in place to mitigate the risks from online harms. A supplemental protocol should be urgently considered to address the role and responsibilities of non public bodies, to ensure coverage, consistency and to provide legal gateways with safeguards for increased public to private, private to public and private to private information sharing, in particular not just domestically but also cross border.

6. Conclusion

The GCFFC which represents many fighting financial crime stakeholders including those fighting cybercrime, is conditionally supportive of the Treaty. Whilst recognising the many benefits that may come from the Treaty, and are needed, we also recognise the legal and human rights challenges facing countries in making this Treaty work fairly. The GCFFC believes the Treaty is necessary and overdue, but implementation should be closely monitored to ensure it is implemented and used in line with its terms including ensuring legal and human rights safeguards are fully respected. The Treaty has the ability to make cyber criminality more difficult and more risky, provided law enforcement has the knowledge, skills, capabilities and resources and willingness to co-operate internationally. Still a law enforcement approach is unlikely to prevent and combat cybercrime alone.

We call on all State Parties that ratify the Treaty to quickly start work on both implementing it and working on a supplementary protocol. This supplementary protocol should include provisions which help to address the concerns raised above, but in particular to agree the roles and responsibilities of non public bodies, to ensure coverage, consistency and provide legal gateways with safeguards for increased public to private, private to public and private to private information sharing, in particular not just domestically but also cross border.

GCFFC - February, 2025

Acknowledgements: The GCFFC wishes to thank its Members for contributing to and in supporting the publication of this comment letter. In particular the GCFFC would like to recognise the expert contributions of Vivienne Artz, Samantha Beesley, John Cusack, Julia Chin, Louis De Koker, Sean Doyle, Oleksiy Feshchenko, Pawee Jenweeranon, Xolisilie Khanyile, Nick Maxwell & Yulia Murat.

Endnotes:

[1] United Nations General Assembly, Countering the use of information and communications technologies for criminal purposes: Report of the Secretary-General, United Nations, 30 July 2019, See: https://www.unodc.org/documents/ Cybercrime/SG_report/V1908182_E.pdf. In addition GI-TOC previously outlined the challenges in accessing data for investigations, which included *"a reluctance among states to share data; the multi jurisdictional nature of possible offences; and a lack of cooperation from private companies.both private tech companies and governments are integral partners in gaining access to data in investigations"* See: https://globalinitiative.net/wp-content/uploads/2021/12/UN-Cybercrime-PB-22Dec-web.pdf

[2] See: https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf

[3] See: https://news.un.org/en/story/2024/12/1158521

[4] Whilst the former Biden administration supported the Treaty, it is far from clear whether the Trump Administration will do so. At the time of writing, the new US Administration's position on the Treaty is not clear. The USA is an important actor in its own right, but is also the home to where many of the worlds tech giants are based and where much of the data that might be requested from third parties is stored or could be accessed. Technology companies, including from the US have been critical of the Treaty, throughout its journey and throughout advocated for a more focussed and balanced approach that safeguards human rights, ensures data privacy and supports the essential work of cybersecurity professionals.

[5] See: https://documents.un.org/doc/undoc/ltd/v24/055/06/pdf/v2405506.pdf

[6] See: https://www.coe.int/en/web/cybercrime/the-budapest-convention-old#:~:text=It serves as a guideline,Racism committed through computer systems. The signatories are: Albania, Andorra, Argentina, Armenia, Australia, Austria, Azerbaijan, Belgium, Benin, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Cameroon, Chile, Colombia, Costa Rica, Côte d'Ivoire, Croatia, Cyprus, Czechia, Denmark, Dominican Republic, Ecuador, Estonia, Finland, Fiji, France, Georgia, Germany, Ghana, Greece, Grenada, Hungary, Iceland, Israel, Italy, Japan, Kiribati, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Monaco, Montenegro, Morocco, Netherlands, Nigeria, North Macedonia, Norway, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Moldova (Republic of), Romania, Rwanda, San Marino, Senegal, Serbia, Sierra Leone, Slovakia, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Tunisia, Türkiye (Republic of), Ukraine, United Kingdom & United States of America

[7] See Article 65

[8] See Article 66

[9] See Article 62

[10] See: https://www.un.org/sg/en/content/sg/statement/2024-12-24/statement-attributable-the-spokesperson-for-the-secretary-general-the-adoption-of-the-united-nations-convention-against-cybercrime?_gl=1*zi1fvd*_ga*MTQ5ODczODU4My4xNzM2MDY3MTU1*_ga_S5EKZKSB78*MTczNjA2NzE1NC4xLjAuMTczNjA2NzE1NC42MC4wLjA.*_ga_TK9BQL5X7Z*MTczNjA2NzE1NC4xLjAuMTczNjA2NzE1NC4wLjAuMA

[11] See: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-welcomes-adoption-of-UN-convention-against-cybercrime

[12] See: https://news.un.org/en/story/2024/12/1158521

[13] See: https://www.cyberdaily.au/security/10895-tech-companies-call-for-changes-to-draft-un-cybercrime-convention

[14] See: https://www.hrw.org/news/2024/10/21/eu-member-states-should-vote-no-un-cybercrime-treaty

[15] Russia led the effort at the UN for a global Treaty, and by 2019 had secured the support of many of the worlds leading autocracies, for example, the following States were then supporting a draft Convention: Algeria, Angola, Azerbaijan, Belarus, Bolivia, Burundi, Cambodia, China, Cuba, North Korea, Egypt, Eritrea, Iran, Kazakhstan, Laos, Libya, Madagascar, Myanmar, Nicaragua, Russia, Sudan, Suriname, Syria, Tajikistan, Uzbekistan, Venezuela and Zimbabwe.

[16] See: https://news.un.org/en/story/2024/12/1158526

[17] See: https://rm.coe.int/1680081561

[18] See: https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/new-united-nations-convention-cybercrime_en

[19] See for example Jamaica's position statement In January 2022 which sums up an expectation of technical support: "*It is crucial that technical assistance is made available to build capacities to strengthen States' abilities to contribute more to the global framework to fight cybercrime. In this regard, capacity building should be sustainable, have a clear purpose, correspond to domestic needs, and meet the objective of human resource development in this specialised area. Consideration should also be given to establishing a funding mechanism to support the capacity building for the implementation of the Cybercrime Convention*". See: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.

[20] See for example Jamaica's position statement In January 2022 which sums up an expectation of technical support: "*It is crucial that technical assistance is made available to build capacities to strengthen States' abilities to contribute more to the global framework to fight cybercrime. In this regard, capacity building should be sustainable, have a clear purpose, correspond to domestic needs, and meet the objective of human resource development in this specialised area. Consideration should also be given to establishing a funding mechanism to support the capacity building for the implementation of the Cybercrime Convention*". See: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.

[21] See Article 53. 3) a) *"Strengthening co operation between law-enforcement agencies or prosecutors and relevant individuals and entities outside the public sector, such as non-governmental organisations, civil society, organisations, academic institutions and private sector entities for the purpose of addressing relevant aspects of preventing and combatting the offences established in accordance with this convention".*

[22] See: Article 53. 3) d) "*Encouraging service providers to take effective measures, where feasible in the light of national circumstances and the extent permitted by domestic law, to strengthen the security of the service providers products, services and customers".*

[23] See: https://www.gcffc.org/an-assessment-of-scams-in-east-asia/