POLICY BRIEF

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

CONTROL, ALT, OR DELETE?

The UN cybercrime debate enters a new phase

Summer Walker | Ian Tennant

DECEMBER 2021

ACKNOWLEDGEMENTS

Special thanks to Mark Shaw for his thoughtful review and to The Global Initiative Against Transnational Organized Crime (GI-TOC)'s Publications team.

ABOUT THE AUTHORS

Summer Walker is the GI-TOC's New York representative and a senior analyst. She focuses on global criminal justice agendas, analyzing a range of issues from cybercrime to drug policy. She engages with the United Nations community and government missions to bring the research, analysis and innovative approaches of the GI-TOC and its Network of Experts to multilateral policy debates.

Ian Tennant is based in Vienna, where he leads GI-TOC engagement with the UN Office on Drugs and Crime and the wider diplomatic and civil society community in Vienna. He manages the GI-TOC Resilience Fund, a multi-donor initiative that supports civil society individuals and organizations working to counter the damaging effects of organized crime around the world.

Cover: © Markus Spiske, Christian Wiediger/Unsplash.com
Design: Ink Design Publishing Solutions

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

CONTENTS

SUMMARY

A potentially significant shift in the UN response to cybercrime is underway. Since the adoption of the UN Convention against Transnational Organized Crime (UNTOC) in 2000, and the subsequent adoption of the Council of Europe's Budapest Convention in 2001, the internet and the scope of its use have changed beyond recognition. Although this evolution of the internet and technology is considered a 'great accelerator' of transnational organized crime,[1] there has not been a similar acceleration in UN action on cybercrime since the beginning of the millennium.

Following periods of inertia, intense political disagreement, lack of trust over the governance of cyberspace and limited shared understanding of cybercrime, with widely varying associated responses, the UN membership will finally enter a formal negotiation process in 2022 to outline a global legal instrument to deal with cybercrime. This will have major implications for setting standards, international cooperation, human rights and freedom of expression.

This brief outlines the substantive issues that impair the creation of a shared understanding of cybercrime cooperation and offers insights into the history of the geopolitical tensions, how they manifest, and what conclusions we can draw for the outcome of these negotiations.

The process could produce something very similar to the Budapest Convention, i.e. its UN alter ego (ALT); or one based on proposals submitted by the Russian government (CONTROL); or a consensus position between the two (CONTROL/ALT) – or nothing at all (DELETE). Taken together, the arguments and process so far have shown significant political, ideological and substantive obstacles to the creation of a new treaty on cybercrime. The geopolitics does not lend itself to building trust in these times of declining multilateralism, with the cybersphere as a key battleground.

Will governments find a way to produce an instrument that improves cooperation across a range of competing interests, or will lack of consensus and trust be too difficult to overcome?

ACRONYMS AND ABBREVIATIONS

CARICOM	Caribbean Community
CCPCJ	Commission on Crime Prevention and Criminal Justice
EGM	Expert Group Meeting
GDPR	General Data Protection Regulation
ICT	information communication technology
OECD	Organisation for Economic Co-operation and Development
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention against Transnational Organized Crime

© Kirill Kudryavtsev/AFP via Getty Images

INTRODUCTION

At a time when lives are increasingly lived online – from health appointments and schooling to debating politics in the digital civic squares of social media – everything about information communication technology (ICT) and internet policy is political. The upcoming UN cybercrime treaty debate is no different. Politics – and geopolitics – permeates this agenda: from how the process should be run to what should be in the treaty.

In January 2022, governments will begin a process to expand a global cybercrime instrument at the UN – the first to tackle this pervasive and complex phenomenon. While there is a near universal belief that *something* should be done to increase global cooperation and create a shared understanding of the issues, this process is hampered by a deep mistrust among member states. From the outset, Western states, including EU member states, the United States, the United Kingdom and Canada, resisted a UN process to develop a cybercrime instrument. The agenda was led by Russia during the 2019 General Assembly, and a resolution to start the process was taken to a vote. The vote passed with 79 states in favour and 60 against – and with 33 abstentions. Viewed collectively, it passed with minority support: 79 to 93.

States have very different priorities for what this instrument may offer. Some expect that it will help build domestic technical capacities to counter cybercrime; some foresee improved cooperation in investigations into crimes such as ransomware attacks. Either way, beyond particular interests, as a UN instrument, it will have normative significance for understanding what constitutes cybercrime and outlining corresponding state responsibilities.

Ahead of the formal process, this brief details why states are entering into these negotiations in such a deeply divided fashion. It outlines the major substantive issues that remain unresolved and which will weigh in on the negotiations from the beginning: digital sovereignty; defining criminal offences (including content-related offences); international cooperation and access to data; and technical cooperation and capacity building.

The brief then turns to the events that led to the new negotiations process, offering insights into the history of geopolitical tensions, how they present in this context and what it indicates for future negotiations.

The UN General Assembly discusses countering the use of information and communications technologies for criminal purposes, New York, May 2021. *© UN Photo/ Eskinder Debebe*

© Donat Sorokin\TASS via Getty Images

STARTING POSITIONS: THE UNDERLYING DEBATES HEADING INTO NEGOTIATIONS

In 2019, the The Global Initiative Against Transnational Organized Crime (GI-TOC) published a guide to the UN cybercrime debates that outlined how the system addresses cybercrime and the obstacles that inhibit cooperation. One of the main underlying disagreements was around the need for a universal instrument negotiated through the UN. This process is now advancing, despite some hesitancy.

Other concerns related to regulating cyberspace, the definition of cybercrime, regulating online content and access to data.[2] At their core, these concerns boil down to issues of state control – both as involves other states and with regard to countries' own citizens. It will be a challenge to set out terms for international cooperation in an environment where key global powers still do not effectively cooperate in cybercrime investigations.[3] Finally, the issue of capacity building remains high on the list of priorities of many member states leading into this process, and is one of the few issues achieving a certain level of consensus across the political divide.

The need for a new instrument

Arguments for a universal treaty: A group of states, including China, Russia and a number of developing countries, would like to see a global instrument on cybercrime, arguing that a newly negotiated legal document with global inputs is necessary. This argument stems from these states not having been involved in the drafting process of the Budapest Convention.[4] Many claim the convention does not reflect their concerns, in particular national sovereignty concerns over transborder access to information and electronic evidence, even if many of those issues are now being attended to.

Arguments against a universal treaty: Most EU and OECD member states believe the Budapest Convention already provides a basis for a universal treaty, arguing that it fosters multilateral cooperation on cybercrime and includes many signatories from other global regions. Having entered into force in 2004, the convention has 66 states parties, including a number of countries outside the Council of Europe, such as the US, Japan, Canada, Senegal, Sri Lanka, the Philippines, Turkey, Morocco and the Dominican Republic, and is open to ratification by other states. Observer countries include South Africa and Mexico.[5]

Digital sovereignty

In the past couple of years, states have – for different reasons – grown closer together on the 'digital sovereignty' agenda, a drive to control and regulate digital data and the associated infrastructure in their own territory. Historically, Russia and China were the primary champions of this, but others, including EU countries, have since come on board.

Although an earlier brief reported that Western states favoured 'a multi-stakeholder [internet governance] model, which includes private-sector actors, such as technology companies',[6] it is increasingly clear that states want to increase their authority with regard to these companies, particularly when they are based outside of the state's territory. Senators in the US demanded a response from TikTok after it was revealed that the platform intended to 'collect biometric identifiers and biometric information' from users' content, such as 'faceprints and voiceprints'.[7] Tech companies have had to comply with the EU's General Data Protection Regulation (GDPR)[8] since 2018 when operating across the EU, as the EU is actively strategizing on how to maintain stronger protections for citizens' data. Yet, the EU also wants to become more competitive in providing infrastructure for ICT, cybersecurity and cloud storage amid US and Asian companies dominating the market.[9] The US president, Joe Biden, has placed critics of big tech in high-level positions of multiple relevant agencies, including the Federal Trade Commission, the National Economic Council and the Department of Justice's anti-trust division. However, the US remains one of the most permissive regulatory environments: while government hearings with tech leaders take place, the federal government has resisted most regulation on data protection and privacy.

Some countries are taking more direct action than is possible in the West. For example, Russian authorities recently arrested the chief executive of Group-IB, a cybersecurity firm, on treason charges,[10] and Chinese regulators have been constraining the power of tech companies by imposing fines and restructuring on major firms, and reportedly causing a mysterious three-month disappearance of prominent Chinese tech billionaire Jack Ma.[11]

Global tech companies are increasingly meeting the demands of the governments where they operate. © *VCG via Getty Images*

In recent years, global tech companies have also increasingly met the demands of the governments where they operate, reducing the perceived leverage of the private sector against government. In China, Apple now stores the personal data of its customers on Chinese government servers inside the country, and does not use its encryption technology in the country.[12] TikTok, owned by Beijing-based ByteDance, claims it stores all US-generated data within the US (although it has been reported that ByteDance has access to the data).[13] In September 2021, Russia successfully lobbied Apple and Google to remove an app used by the opposition in the lead-up to the elections.[14]

Governments now also control more elements of ICT or have capabilities that allow them to implement measures such as internet shutdowns, regardless of compliance by tech companies. A joint investigation by Google's Jigsaw project, Access Now and Censored Planet found that of the nearly 850 shutdowns documented over the last 10 years, 768 happened in 63 countries since 2016.[15] In 2020 alone, when most of the world was in COVID-19-induced lockdowns and reliant on the internet for basic communication and needs, there were a reported 155 internet shutdowns in 29 countries.[16] Government control has clearly escalated across the board.

States may be more favourable to government intervention, but the underlying reasons continue to differ and this will impact negotiations. Objectives for stricter oversight and regulation of tech companies exist along a continuum ranging from prioritizing citizen protection to state control and surveillance. This feeds into cybercrime debates around obtaining data across borders, justifications for data requests or trying to force private tech companies to provide information.

In the upcoming negotiations, large private-sector tech companies will most likely have a role in providing inputs to the treaty through access to government delegations. Protection of private-sector autonomy, citizens' rights and protection, and assertion of state power will continue to shape this debate.

Outlining criminal offences

Another complication is that markets such as cryptocurrency have different levels of regulation and consumer protection across countries.

A universal treaty will have to contend with outlining offences. As noted in the 2019 GI-TOC report, there is no shared definition of cybercrime. *Cyber-dependent* crimes threaten the confidentiality, integrity and availability of data and systems; *cyber-enabled* crimes refers to offences that also occur offline, but in which criminals may deploy technology to achieve their ends. Although there are a growing number of online criminal markets, from arms to antiquities, and which employ both the surface web and the darknet, practitioners rarely need new legally defined offences, because they are already able to act given that the activity is illegal offline. What they do need are new tools for detection, investigation and cooperation with private companies, which is where hold-ups often occur. In many cases (such as the use of messenger apps and social media sites to sell women by extremist groups), it has taken media coverage, public awareness and public outrage to spur action from private companies, not legal definitions. Another complication is that markets such as cryptocurrency have different levels of regulation and consumer protection across countries, and thus the framework for redress following hacks or loss of property is often ad hoc and, at times, driven by the platforms and investors.

As states advance a UN instrument, it is worth noting that earlier crime-related conventions have avoided setting out strict definitions. The UN Convention against Transnational Organized Crime (UNTOC) does not define 'transnational organized crime' and sets an extremely low threshold for defining an organized criminal group,[17] nor does the UN Convention on Corruption define 'corruption'.[18] Although cybercrime is a complex and evolving phenomenon, leaving the definitional boundaries of cybercrime open to interpretation in a universal instrument is a risk.

States will be more likely to find common ground on setting out terminology for cyber-dependent crime than cyber-enabled crime, as existing regional conventions share similar language on cyber-dependent crimes. For instance, ahead of January 2022, Japan submitted a position statement that says offences in the new convention should 'foremost cover cyber-dependent crimes, and cyber-enabled crimes should be covered only where it is necessary and there is broad consensus among Member States'.[19] However, as crimes online expand, the approaches taken by different bodies show the potential need to reconcile differences:

- In its 2018 report, the open-ended Intergovernmental Expert Group Meeting on Cybercrime (EGM) listed 25 offences that states should consider criminalizing.[20]
- A draft Russian treaty for this process, submitted in July 2021, notes an array of crimes, including separate articles for issues such as illicit drug trafficking online and illicit distribution of counterfeit medicines and medical products.[21]
- The Budapest Convention focuses primarily on cyber-dependent crimes and outlines specific content-related crimes, noted below.
- Article 29 of the African Union's convention on cybercrime includes attacks on computer systems, data breaches and similar content-related crimes to Budapest; however, it also specifies that gambling should not 'be exercised freely' through 'e-commerce activity'.[22]
- In the Arab League's (draft) law, gambling is listed as an offence related to pornography (article 13).[23]

How will content-related offences be addressed?

Over-reach threatening online freedoms and which puts individuals' civic and political rights at risk has been cited as a key obstacle to a universal treaty.[24] Indeed, at the UN General Assembly vote in 2019, concerns over maintaining online freedoms in a universal instrument were a key reason for many governments not voting for the resolution.

Worldwide, governments have dramatically different legislation on online content. Freedom House found that people were arrested or convicted for online speech in 56 countries (out of 70 covered in the report) in 2021. It also found, that 'officials suspended internet access in at least 20 countries, and 21 states blocked access to social media platforms'.[25] In a number of countries, cyber laws are applied to arrest and penalize journalists and activists when they use online platforms to voice an opinion or share content.

In the West, platforms are increasingly pressured to rein in misinformation, hate speech and extremist content. Recently, President Biden vented his frustration with Facebook during the pandemic, calling on them 'to do something about [...] the outrageous misinformation about the vaccine',[26] yet regulation remains weak in the US. In the UK, a new online safety bill, moving through Parliament during late 2021, is designed to include criminal sanctions for those posting 'foul content'. The opposition Labour Party is calling for directors of tech companies to be held liable for the content of messages posted on their platforms, with the Labour leader, Sir Keir Starmer QC (a former director of public prosecutions), referring to online extremism as a 'cesspit'.[27]

The four existing regional instruments on cybercrime offer some insights into how content-related offences have been addressed previously.

Activists protest Nigeria's Twitter ban, Lagos, June 2021. Governments across the world have dramatically different legislation on online content. *© Pius Utomi Ekpei/ AFP via Getty Images*

The 2001 Budapest Convention only addresses child pornography under content-related offences.[28] A 2003 protocol on 'criminalisation of acts of a racist and xenophobic nature committed through computer systems' calls for states to criminalize dissemination of racist and xenophobic material through computer systems as well as motivated threats or insults through computer systems.[29]

The African Union Convention on Cyber Security and Personal Data Protection shares similar parameters for online content, limiting it to child pornography and racist and xenophobic content. The African Union's treaty establishes content-related offences as relating to acts involving or facilitating child pornography, creating or disseminating racist content or threatening people owing to their race or ethnicity, and denying or justifying genocide or crimes against humanity,[30]

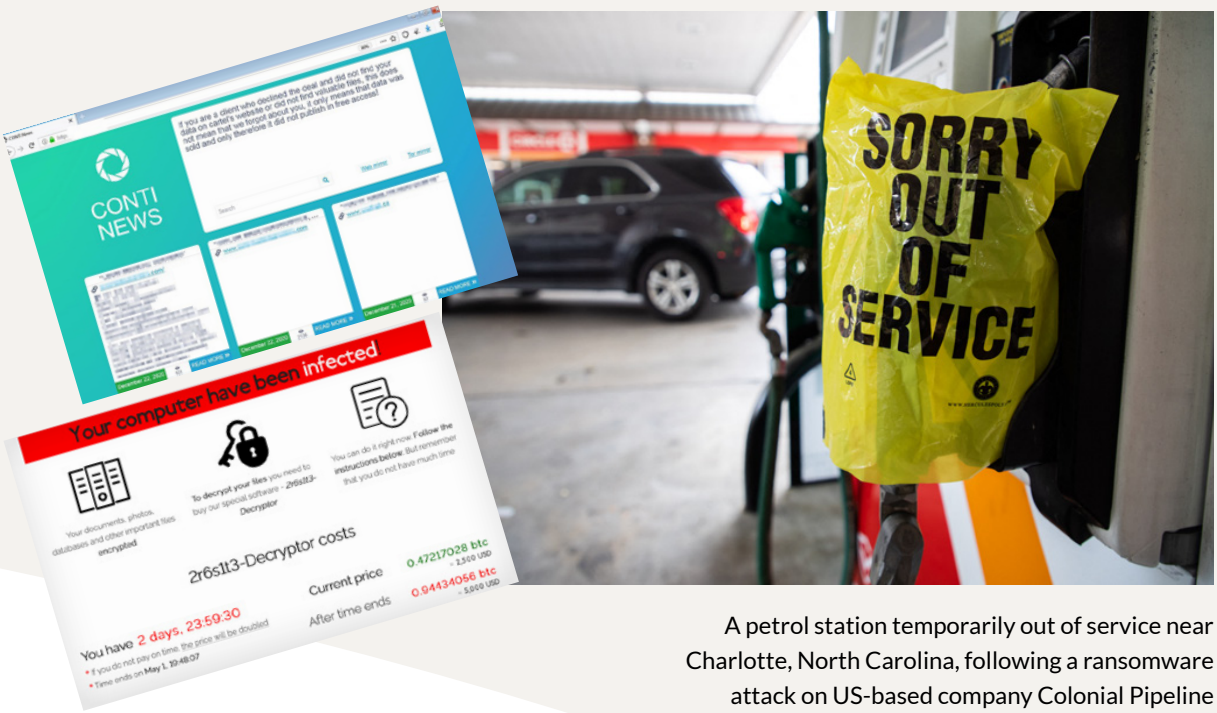
In the League of Arab States' Arab Convention on Combating Information Technology Offences, content-related offences cover 'pornographic material or material that constitutes outrage of modesty through information technology', with greater penalties levied for child pornography. It also criminalizes 'dissemination and advocacy of the ideas and principles of terrorist groups'.[31]

The Shanghai Cooperation Organization has a cooperative agreement on 'international information security', which includes cybercrime as a key risk to information security but is not considered solely a cybercrime treaty. In the 2009 Agreement on Cooperation in Ensuring International Information Security, cybercrime – defined as 'using information resources and/or influencing them in the information space for illegal purposes' – is listed as a major challenge addressed by the agreement. The agreement does not list content-related offences or delineate cybercrimes, but it does list cybercrime alongside risks such as 'information terrorism' and 'use of a dominant position in the information space to the detriment of the interests and security of other States'.[32]

Russia's draft treaty submitted for consideration in the upcoming negotiations includes provisions on child pornography, racial or ethnicity-based incitement and crimes against humanity, similar to what is included in the Budapest and African Union treaties. However, it further includes incitement to suicide (article 16) and a loosely defined article on 'offences related to the involvement of minors in the commission of unlawful acts that endanger their life or health'.[33] Under its extremism-related offences (article 21), the draft treaty includes a 'Pandora's box' clause:

> Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other unlawful act under its domestic law distribution by means of ICT of materials that call for unlawful acts motivated by *political*, *ideological*, *social*, racial, ethnic, or religious hatred or enmity, advocacy and justification of such actions or the provision of access to them.[34]

In the General Assembly Third Committee's debate on crime and ICT in October 2021, both the EU and the US stated their expectation for an instrument that will preserve human rights obligations and maintain an open internet, and Mexico submitted a position paper that includes an expectation that the 'violation of freedom of speech' should be listed as a general offence in the treaty.[35] States' differing basic perspectives on what constitutes offences are expected to be a key area of friction during the drafting process.



A petrol station temporarily out of service near Charlotte, North Carolina, following a ransomware attack on US-based company Colonial Pipeline that prompted fuel shortages, May 2021.
© Logan Cyrus/AFP via Getty Images

International cooperation and access to data

In 2019, the UN secretary-general was tasked 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 cooperation emerged from the report, 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.[36]

The GI-TOC previously outlined the challenges in accessing data for investigations, which include a reluctance among states to share data; the multijurisdictional nature of possible offences;[37] and a lack of cooperation from private companies. Both private tech companies and governments are integral partners in gaining access to data in investigations.

There are regional cybercrime agreements that help to facilitate cooperation during investigations, and lessons learned from these can contribute to a stronger international instrument. But real-world examples illustrate the dichotomy with which many states are entering into these negotiations: a desire for access and cooperation when they need it, and a hesitancy to cooperate when asked by another country. The tactic of using criminal proxies for state-led attacks further complicates cooperation. Even if attacks are not sponsored by a state, destabilization through cyber attacks is an established and growing tool in geopolitical struggles, therefore limiting an interest in cooperation.

Recent ransomware attacks illustrate these difficulties, specifically a series of high-profile attacks by allegedly Russian-speaking groups based in Russia and Eastern Europe, such as the:

- attack on the Irish healthcare system by the Conti ransomware group;[38]
- REvil attack on software company Kaseya, affecting 1 500 companies;[39] and
- Darkside attack on US-based company Colonial Pipeline.

Responses to these attacks are opaque and it is unclear what level of cooperation between states occurs below the surface. Addressing the issue at the executive level, Biden has warned his Russian counterpart, President Vladimir Putin, to cooperate in ransomware investigations and said he would escalate the issue to be treated as a national security threat rather than a criminal offence.[40] In the case of Darkside, the group seemingly shut down after losing access to its servers and having its crypto-currency wallets emptied, which some researchers speculate was the work of the US government.[41] The development of a universal decryption key to restore information in the Kaseya attack has led some to speculate that either the Russian state stepped in to help or the US hacked REvil.[42]

Although the impetus for the treaty should be to increase international cooperation, realities on the ground show that cross-border investigations are plagued by political power struggles, bilateral disputes, a lack of transparency in responses and differences on human rights issues, further complicated by other difficulties such as a lack of resources or networks. The added political difficulties associated with drafting cyber policies do not bode well for a new age in international cybercrime cooperation and cross-border investigations.

Technical cooperation and capacity building

A consistent and more consensual view expressed by states in the UN secretary-general's 2019 report is the need for training and capacity building. The need for training law enforcement officials, judiciary, investigators and others involved in combating cybercrime was raised by both those who sought capacity building and those with more advanced tech capacity and who can provide support. The COVID-19 pandemic highlighted how pervasive and necessary the use of ICT is in every aspect of life – from civic engagement to healthcare and education. As this dependence on ICT increases, many countries feel underprepared to deal with security breaches and criminal activity online, especially in light of increasing attacks on critical infrastructure such as hospital computer systems or gas pipelines. As in other UN tech agendas and in keeping with the UN crime prevention and criminal justice agenda, many states will lobby for this treaty to deliver technical capacity building as part of international cooperation, with high-income countries expected to provide financial support.

Jamaica's position statement ahead of January 2022 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 specialized area.
- Consideration should also be given to establishing a funding mechanism to support the capacity building for the implementation of the Cybercrime Convention.[43]

A number of capacity-building programmes already exist, at both the regional and international level. For example, the Organization of American States' training programme on cybercrime covers investigation, prosecution, and evaluation and analysis.[44] There are also multiple programmes and projects on cybercrime at the UN level. For example, the United Nations Office on Drugs and Crime (UNODC)'s Global Programme on Cybercrime provides technical assistance to states and offers tools such as a case-law repository and e-learning courses on digital forensics. The United Nations Interregional Crime and Justice Research Institute is establishing the 'Artificial Intelligence for Safer Children' initiative, which is meant to serve as a global hub to leverage artificial intelligence to combat child sexual abuse material.[45]

Transparency in capacity building between states is key to ensuring that human rights are respected when transferring technologies and skills, especially in a field that is already clouded in so much secrecy. An international instrument could provide a stronger platform to connect these ad hoc projects and create better transparency, with the UN's involvement possibly being able to mitigate some risk in technology transfer and capacity building if accountability measures are built into the treaty. Connecting reporting to that already done by bodies such as the United Nations High Commissioner for Refugees would create stronger synergies across the UN pillars.

Despite the considerable focus on training programmes, some states are expected to press for assistance that goes beyond training, seeking funding and avenues for improving technological capacity. In fact, in May 2021, during the meetings of the ad hoc committee set up to elaborate the international convention on cybercrime, Russia noted that the goal of the convention is to 'bridge the technological gap between developed and developing countries'.[46] Although technology transfer will likely not be part of a legally binding instrument, technical capacity will be a key bargaining chip. In the Third Committee debate on crime and ICT in October 2021, the EU stated that the instrument should be 'restricted to criminal justice elements', whereas Singapore, speaking on behalf of the Association of Southeast Asian Nations (ASEAN), detailed how ASEAN strengthens cybersecurity in the region through its capacity building programme.[47] Access to capacity building and technical assistance may in fact be a priority for a number of governments, and may increase their willingness to negotiate in other areas to achieve firm commitments of support.

These foundational issues set the stage for the upcoming negotiations and link directly to some of the already evident problems. The next section outlines the lead-up to the current process, the historical background of the geopolitical tensions and how they present in this context, and what it means for the future negotiations.

Although technology transfer will likely not be part of a legally binding instrument, technical capacity will be a key bargaining chip.

© Yuichiro Chino\Moment RF
via Getty Images

THE PROCESS

Getting to where we are today

The process of reaching international agreement on how to define cybercrime and dealing with it effectively has evolved over the course of three decades. The following timelines present three broad periods and key events in each, describing how we got to where we are today.

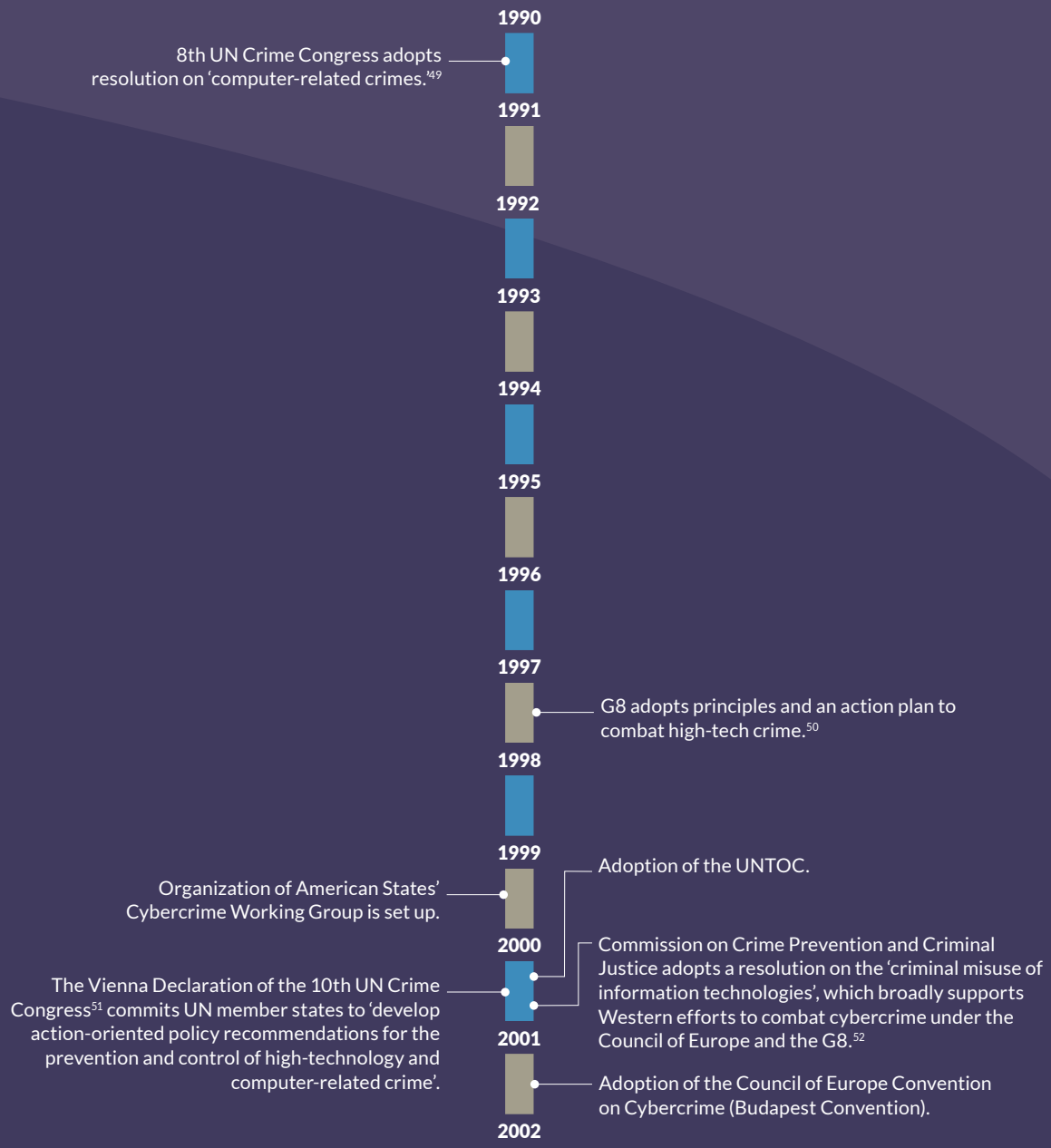
Emerging awareness shows the lead-up to establishing the UNTOC and the Budapest Convention between 1990 and 2001.

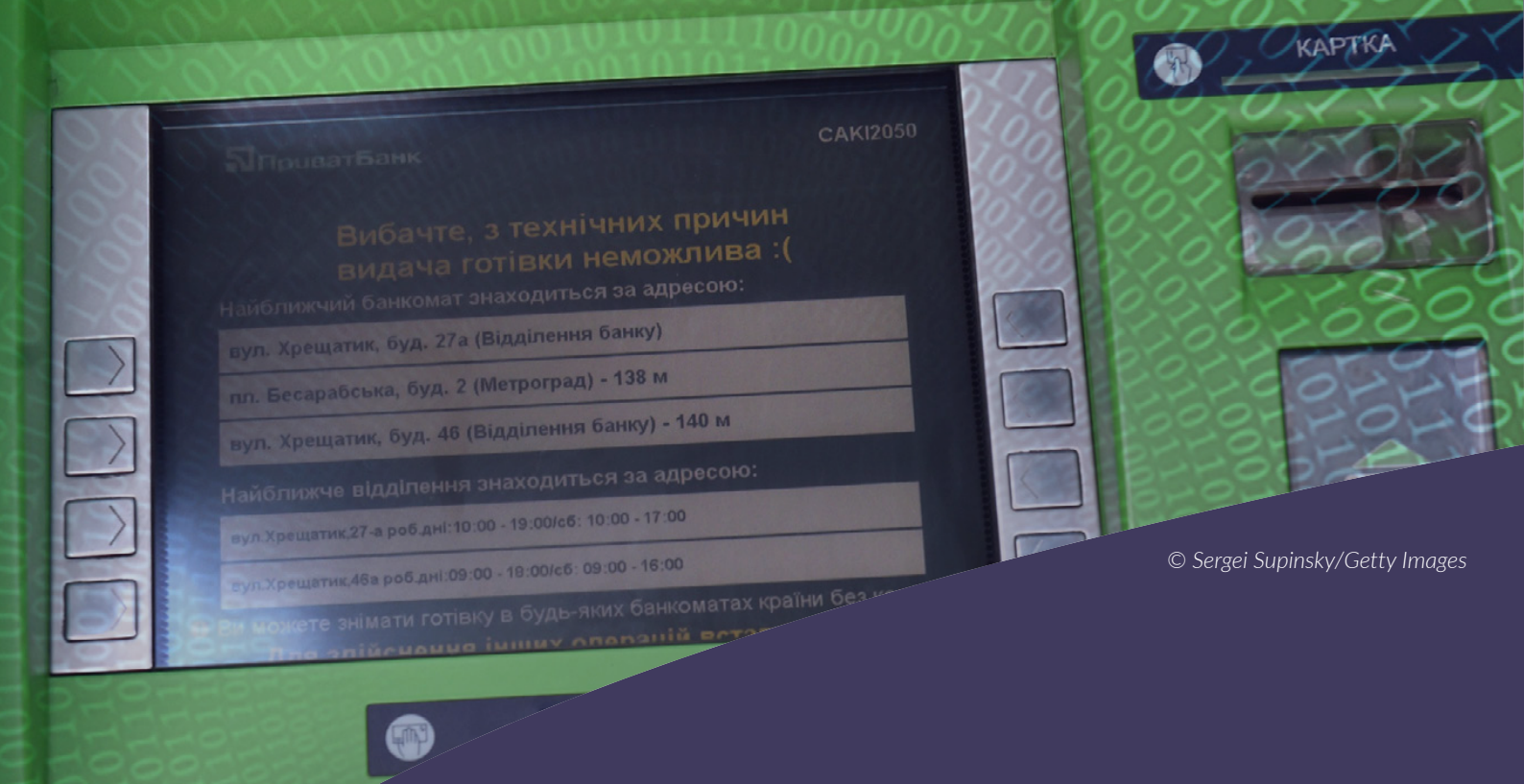
Multilateral inertia illustrates a period between 2001 and 2010 during which countries tried to make sense of instruments and adapted them to their specific contexts.

Polarized approaches outlines the divergence that has developed since 2010, with some countries advocating for a new convention while others lobby for retaining the existing instruments.

EMERGING AWARENESS: TOWARDS UNTOC AND BUDAPEST (1990–2001)

During the 1990s, as the process towards outlining a UN Convention against Transnational Organized Crime was being advanced,[48] the UN recognized the need to counter computer-related crimes in a resolution as early as the 8th Crime Congress in Havana in 1990. By 2000, initiatives driven mainly by Western countries and the G8 (which then included Russia) culminated in the Budapest Convention being adopted in 2001. To date, this convention has been adopted by 66 countries, but never by Russia, despite their being a member of the Council of Europe.

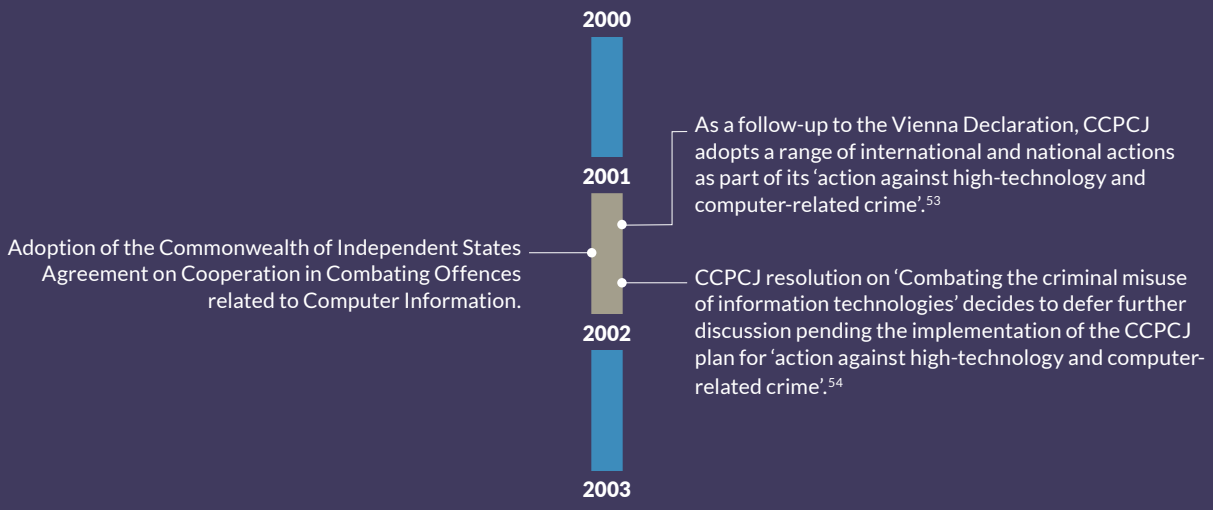




© *Sergei Supinsky/Getty Images*

MULTILATERAL INERTIA: ADAPTATION TO NEW INSTRUMENTS (2001–2010)

After the 10th UN Crime Congress in Vienna and the adoption of the Budapest Convention, it became clear that there was no consensus on what more to do at the multilateral level beyond signing and implementing the new Convention. The Commission on Crime Prevention and Criminal Justice (CCPCJ) did not adopt any specific resolutions on cybercrime between 2001 and 2010, a key decade in the growth of cybercrime and cyber-related crime. This period also coincided with the gradual decline of multilateralism, which continued in the decade after 2010.



POLARIZED APPROACHES (2010–NOW)

Between 2010 and 2019, the debate on dealing with cybercrime became increasingly polarized. Two distinct groups emerged: those seeking a new UN convention and those in favour of sticking with existing instruments while focusing on capacity building and improved technical assistance. This has been a clear dividing line since the inception of the EGM in 2011, which has yet to find consensus on this key issue.

2010

Russia submits a convention text to the 12th UN Crime Congress, but owing to lack of consensus it is not adopted. Instead, the 'Salvador Declaration' recommends setting up an intergovernmental expert group (EGM) on cybercrime under the CCPCJ,[55] with a mandate to consider potential new instruments against cybercrime.

CCPCJ decides to follow the Congress recommendation and convenes the EGM in a resolution subsequently adopted by the UN Economic and Social Council and the UN General Assembly.

2011

Adoption of Draft East African Community Framework for Cyberlaws.

Adoption of the Arab Convention on Combating Information Technology Offences.

First meeting of the EGM to conduct a comprehensive study of the problem of cybercrime.

2012

CCPCJ resolution on cybercrime welcomes the work of the expert group and encourages capacity building and technical assistance measures.

Adoption of the Economic Community of West African States directive on fighting cybercrime.

Second meeting of the EGM.

2013

CCPCJ resolution on cybercrime continues the EGM process, with a view to disseminate the findings and outcomes of the two meetings to date and for the 'draft cybercrime study' to be circulated in six official UN languages.

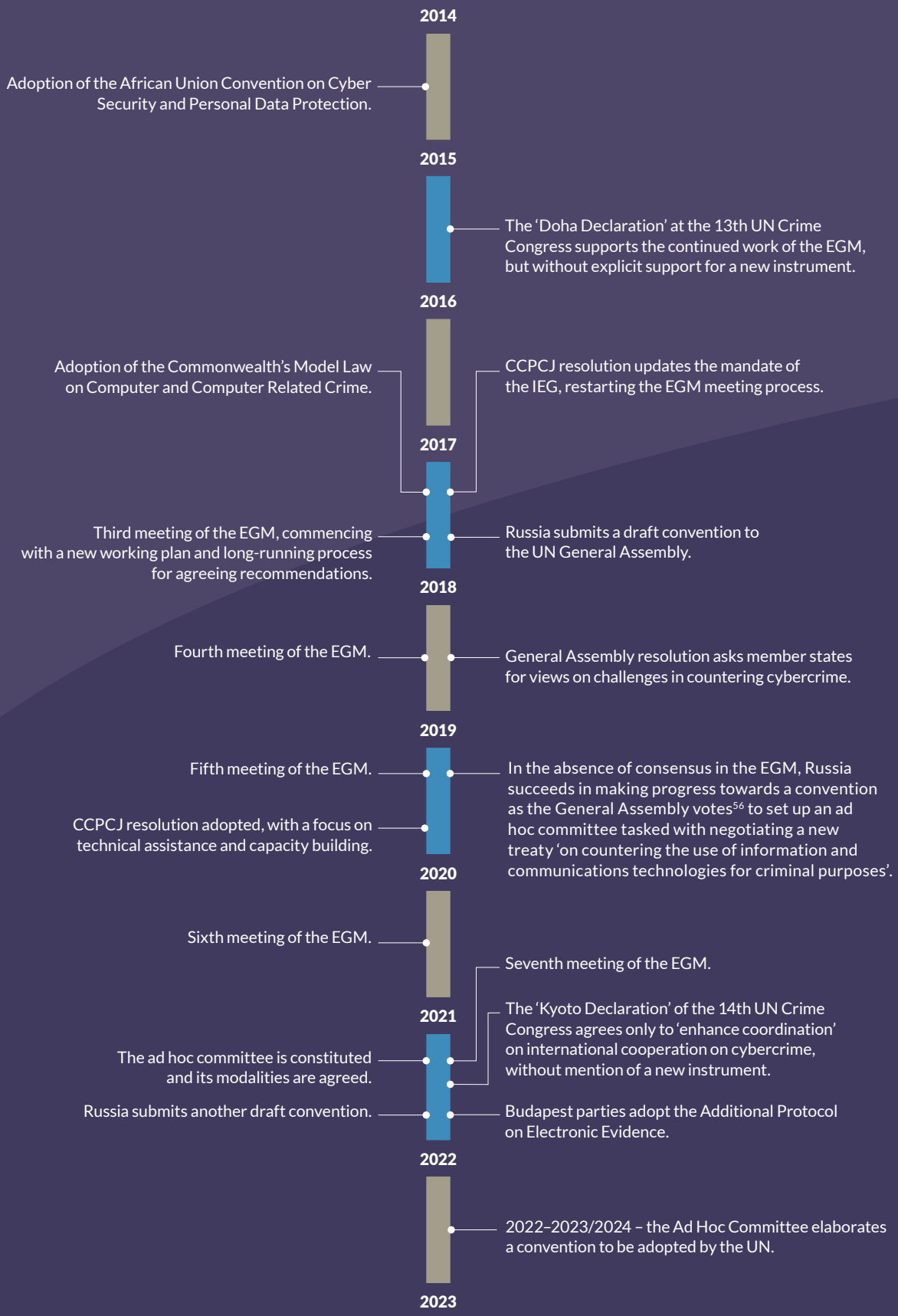
Additional CCPCJ resolution on cybercrime, which focuses on capacity building and technical assistance.

The draft UNODC cybercrime study recommends a new convention based on inputs from the EGM meetings. This is rejected by Western countries and the EGM process stalls.

Adoption of the Southern African Development Community model laws on cybersecurity, cybercrime, data protection and electronic transactions.

2014

© Robyn Beck/AFP via Getty Images


2014
Adoption of the African Union Convention on Cyber Security and Personal Data Protection.
2015
The 'Doha Declaration' at the 13th UN Crime Congress supports the continued work of the EGM, but without explicit support for a new instrument.
2016
Adoption of the Commonwealth's Model Law on Computer and Computer Related Crime.
CCPCJ resolution updates the mandate of the IEG, restarting the EGM meeting process.
2017
Third meeting of the EGM, commencing with a new working plan and long-running process for agreeing recommendations.
Russia submits a draft convention to the UN General Assembly.
2018
Fourth meeting of the EGM.
General Assembly resolution asks member states for views on challenges in countering cybercrime.
2019
Fifth meeting of the EGM.
CCPCJ resolution adopted, with a focus on technical assistance and capacity building.
In the absence of consensus in the EGM, Russia succeeds in making progress towards a convention as the General Assembly votes[56] to set up an ad hoc committee tasked with negotiating a new treaty 'on countering the use of information and communications technologies for criminal purposes'.
2020
Sixth meeting of the EGM.
Seventh meeting of the EGM.
2021
The ad hoc committee is constituted and its modalities are agreed.
Russia submits another draft convention.
The 'Kyoto Declaration' of the 14th UN Crime Congress agrees only to 'enhance coordination' on international cooperation on cybercrime, without mention of a new instrument.
Budapest parties adopt the Additional Protocol on Electronic Evidence.
2022
2022–2023/2024 – the Ad Hoc Committee elaborates a convention to be adopted by the UN.
2023

The current process

Understanding recent events

Russia has attempted to advance a cybercrime treaty within the UN system from as early as the 12th UN Crime Congress in Brazil in 2010, following the period of inertia on this issue since the Budapest Convention. Although this was not successful, it did lead to the creation of the open-ended intergovernmental EGM on cybercrime and put into practice under the CCPCJ.

The EGM process did manage to produce the 2013 UNODC draft study on cybercrime.

However, the divide remained. Russia and its pro-convention allies pushed for agreement on a convention through the EGM, while the West and other pro-Budapest countries continued to be opposed, resulting in an impasse. However, the EGM process did manage to produce the 2013 UNODC draft study on cybercrime,[57] which proposed a new convention, based on some of the outcomes of the first two EGM meetings. But the issue of a new convention was so totemic that it temporarily derailed the entire work programme of the EGM: even the vague suggestion for a new instrument in the (quite long and detailed) report was too much for the pro-Budapest camp, and subsequently the EGM did not meet again until 2017. This group of countries used every procedural means available to avoid the EGM meeting again to advance further discussion around a new convention – and they were successful for several years. When the EGM work eventually did restart, the study was never officially adopted or approved by the member states. In addition, the EGM's revised working plan was intentionally (from the viewpoint of Western countries) very long (until 2021), with conclusions and recommendations not to be agreed until the end of the process.

Unsurprisingly, the patience of those in favour of a new convention was wearing thin. Despite a preference for making progress through the consensus decision-making forums in Vienna, they turned to the General Assembly as the preferred decision-making authority. In 2017, Russia again submitted a draft cybercrime convention to the secretary-general. They did not submit it formally to the General Assembly, but rather advanced an official process in 2018, during which the secretary-general collected states' views on the challenges of countering the use of ICT for criminal purposes.[58]

In 2019, Russia again raised the idea of drafting a treaty in the Third Committee. When it was clear it was opposed by EU member states, the US, Canada and others, Russia took the resolution to a vote at the General Assembly, where it was approved – albeit with minority approval: 79 votes in favour of the proposal against 60 opposition votes and 33 abstentions.

Both camps mobilized a massive lobbying campaign targeting 'middle-ground' countries, and although Russia could be pleased with the victory as a vindication of their belief that most of the non-West was behind them, the pro-Budapest camp could also be pleased that the win looked far from overwhelming. This continuing polarization and lack of clear majority would go on to damage Russia's vision for a negotiation process later on.

From 2021 onwards: Where is the process headed?

Although the process to debate and develop a legal instrument on cybercrime technically begins only in 2022, meetings during 2021 have already exposed the tensions that will shape the negotiations.

UN General Assembly Resolution 74/247, which was adopted in December 2019, allowed for an open-ended ad hoc intergovernmental committee to be set up to advance the issue of a new universal instrument for dealing with cybercrime.[59] The next steps of the process, including agreeing on the membership – and chairmanship – was delayed because of the COVID-19 pandemic. Russia unsuccessfully attempted to have the initial meetings on schedule in early 2021 and in person – Russia's strong preference at the UN even when, during the height of the pandemic, in-person UN meetings were not taking place.

The process eventually restarted in May 2021, and the long-held tensions among groups of member states were clear. But some interesting nuances in traditional coalitions were beginning to emerge. It was clear that Russia, as the initiator of the process, felt it could dictate the terms of the process to the other member states. It had, after all, succeeded in holding the procedural meeting in New York, where decision by vote is commonplace.

The meetings proved highly contentious, not only among those who voted for Resolution 74/247 originally but also among states who wanted greater representation, a decision-making process that was more inclusive, and more transparent engagement modalities that included civil society.

The May meeting was convened for states to set out procedural rules – so-called modalities – for the treaty negotiation process. Although this sounds like a basic task, procedure at the UN is never simply about procedure. Instead, undercurrents are gauged to determine the locus of control of a process, e.g. who chairs the committee (and who their allies are), how decisions are made, where debates will take place. Ultimately, it comes down to which parts of the UN membership contribute most consistently, and who is able to participate from outside the UN. Procedural rules can allow for greater participation and transparency – or cut off access to a process before it even begins.

Organizational meeting of the ad hoc committee (10–12 May 2021): A false start

The organizational meeting was meant to conclude with an agreed set of modalities and a full slate of regionally diverse 'officers' to guide the work of the committee. The meeting succeeded in appointing officers; in fact, the members of the ad hoc committee were appointed immediately and assumed their roles.[60] The bargaining among country blocs for these roles had largely taken place ahead of the meeting, so there was little surprise. But pro-Budapest countries had held out some hope that their nominee for the chairmanship (El Salvador's Permanent Representative in Vienna) would take the role over the successful nominee favoured by Russia and its allies (Algerian Permanent Representative in Vienna – Faouzia Mebarki).

The remainder of the officers are mainly either Vienna-based ambassadors or diplomats (Egypt, Poland, Indonesia, Portugal, Australia and Nicaragua) or country-based senior officials (Nigeria, China, Japan, Estonia, Russia, Dominican Republic, US), with only one diplomat based in New York (Suriname) among the officers. The secretariat of the ad hoc committee is the Vienna-based UNODC, working through the Organized Crime and Illicit Trafficking branch of the Division for Treaty Affairs.

Despite the swift election of officers, the meeting was not able to conclude its more complicated decisions on how the negotiation process itself would run. In fact, the committee was presented with two competing resolutions setting out how the process to draft a cybercrime treaty should take place – one submitted by Russia and one by the US.

Throughout the meeting, states argued over two central, interlinked issues and which are both rooted in the ability to influence the content of a future convention: the location for the upcoming process (New York or Vienna) and how decisions would be made (by vote or consensus). Russia favoured a process based in New York under General Assembly rules, by which decisions can be taken by majority vote (50 + 1) rather than consensus – thereby avoiding the 'Vienna spirit' of consensus-based decision-making. Western and Latin American states, many of whom voted against the resolution that set up the process back in 2019, heavily supported a consensus-based process running out of Vienna, where previous cybercrime debates have been held through the CCPCJ, the parent body of the EGM. Although China, a key country in cyber issues, remained largely silent in the debate, it provided quiet support to the Russian position.[61]

Arguments around accessibility make location an important factor. All states are present in New York, whereas far fewer are represented in Vienna. For this reason, the Caribbean Community (CARICOM) countries, for example, wanted meetings held in New York. Over the course of the meeting, it was clear that many New York-based missions felt excluded, including when the US and Russia worked behind closed doors to try to reconcile their two competing resolutions.

A third issue, raised largely by the UK and Switzerland, was access for civil society, an increasingly divisive issue at the UN in general, and a longstanding point of debate on crime issues in Vienna. The UK and Switzerland did not feel that the tabled proposals were inclusive enough for civil society, and fought for stronger language to include them.

On the last day, and with roughly an hour left for the meeting, a compromise text was submitted by Russia and the US. As the chair began the review process, it became clear that the compromise[62] was skewed heavily in Russia's favour: Russia agreed to hold meetings in Vienna (against their preference of New York), but only if under General Assembly rules, including the 50 + 1 vote. In that last hour, a number of countries who were uncomfortable with the General Assembly voting rules requested a compromise of a two-thirds voting structure being instituted.

There was a clear division between states who had been part of earlier negotiations and those who had not, and the committee chair was not able to find consensus before time ran out. The meeting ended abruptly, with the microphones cut off and uncertainty around what was next.

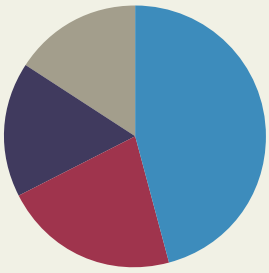
Amendments at the General Assembly help advance the process: The vote on 26 May

While it appeared that states would finalize the text during ongoing informal meetings, Russia submitted, on 24 May, the existing compromise resolution to the General Assembly for a vote on 26 May. This set the stage for a second acrimonious meeting amid growing reservations by many states that any future treaty would be built upon a divisive voting process and exclusionary modalities (for both civil society and member states not represented in Vienna), resulting in a treaty not widely adopted.

The resolution on cybercrime is adopted at the UN General Assembly, New York, 26 May 2021. *© UN Photo/Eskinder Debebe*

MEMBER STATES VOTE ON CYBERCRIME RESOLUTION AMENDMENTS

Vote on L90
(Civil society – Brazil)



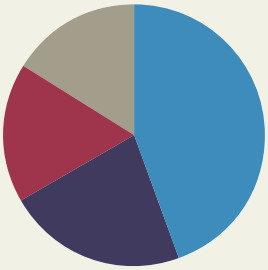
In favour: 88

Against: 42

Abstained: 32

None: 29

Vote on L92
(Civil society – UK)



In favour: 86

Against: 33

Abstained: 43

None: 31

In favour of both L90 and L92

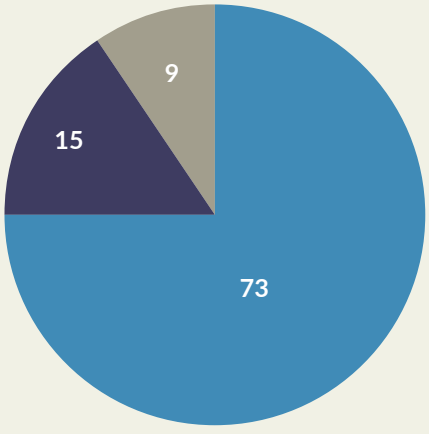
Albania*
Andorra*
Argentina*
Australia*
Austria*
Barbados
Belgium*
Brazil
Bulgaria*
Canada*
Chile*
Colombia*
Costa Rica*
Croatia*
Cyprus*
Czech Republic*
Denmark*
Dominican Republic*
Ecuador
El Salvador
Estonia*
Fiji
Finland*
France*
Georgia*
Germany*
Greece*
Guatemala
Haiti
Honduras
Hungary*
Iceland*
Ireland*
Israel*
Italy*
Japan*
Kiribati
Latvia
Liechtenstein*
Lithuania*
Luxembourg*
Malta*
Mexico
Micronesia
Monaco*
Montenegro*
Netherlands*
New Zealand
Nigeria
North Macedonia*
Norway*
Panama*
Papua New Guinea
Paraguay*
Peru*
Poland*
Portugal*
Rep of Moldova*
Romania*
Samoa
San Marino*
Sierra Leone
Slovakia*
Slovenia*
South Korea
Spain*
Sweden*
Switzerland*
Tunisia
Tuvalu
Ukraine*
United Kingdom*
United States*

In favour of L90 only

Antigua and Barbuda L92
Bosnia and Herzegovina L92
Côte d'Ivoire L92
Dominica L92
Guyana L92
Iraq L92
Madagascar L92
Malaysia L92
Morocco
Nauru
Palau
Philippines* L92
Trinidad and Tobago L92
Turkey* L92
Uruguay L92

In favour of L92 only

Armenia* L90
Botswana L90
India L90
Jordan L90
Lebanon L90
Maldives L90
Qatar L90
Saint Kitts and Nevis
Uganda



* denotes membership or signatory of Budapest Convention

L90 abstained on L90
L92 abstained on L92
L90 against L90
L92 against L92

With the amendments incorporated, the Russian resolution was adopted without a vote, showing a general acceptance to move forward.

After the vote was tabled, efforts led by Brazil, the CARICOM countries and the UK resulted in three amendments being submitted to advance the approval of the resolution, bringing fairly significant changes to the proposed resolution:

- Brazil suggested a two-thirds voting structure, rather than the simple majority favoured by Russia.[63]
- Haiti (on behalf of CARICOM) requested meetings to be split 50/50 between Vienna and New York.[64]
- The UK recommended that any objection to external participants must be agreed by the ad hoc committee (i.e. decreasing single member states' ability to exclude members of civil society).[65]

Despite the ensuing debate, the three amendments were approved by voting (for those lodged by Brazil and the UK) and by consensus (for the amendment lodged by Haiti). With the amendments incorporated, the Russian resolution was adopted without a vote, showing a general acceptance to move forward. The results showed some predictable alignment. For example:

- Brazil's amendment was largely carried by Latin American, North American, European and Pacific Island member states, as well as Japan.
- The UK amendment was approved largely because of support by the same group, with more abstentions.
- A clear group emerged that voted in line with Russia against both the UK and Brazil amendments. Although this group was geographically spread out, they were largely strategically aligned, including China, Cuba, Egypt, Ethiopia, Pakistan, Nicaragua, Venezuela and Zimbabwe.

These meetings exposed new faultlines in the pro-treaty faction, with Brazil (previously in lockstep with Russia on the need for a new convention) leading the charge for a more inclusive and consensus-based process. The UK's leadership on civil society inclusivity has also shown the strong feeling on this issue, which suggests that Russia's desire to push for a closed-door process is a minority-backed endeavour and that they cannot count on their previous allies to support them on all issues (notably countries such as Brazil, India and South Africa). This fracturing of support for the Russian position means that the process has become more open and inclusive than what Russia and its closest allies would prefer.

This resolution determined that the first official meeting of the ad hoc committee will take place in January 2022. However, several organizational issues still have to be finalized at the meeting itself, which will take place from 17 to 28 January in New York (for example, which NGOs will be accepted as observers and how COVID-19 will impact in-person participation), alongside the general lack of substantive agreement on what the scope of the convention should be. Member states had until 29 October 2021 to submit proposals and ideas to the chair, yet Russia has already submitted a draft convention for consideration, months ahead of even the first meeting.

© E+/Getty Images

CONCLUSION

Taken together, the arguments and process so far have revealed significant political, ideological and substantive obstacles to the creation of a new treaty on cybercrime. The geopolitics does not lend itself to building trust in these times of declining multilateralism, with the cybersphere as a key battleground. The lack of transparency that surrounds current responses to high-level cybercrime attacks begs the question of whether states want a convention that draws their actions into the light.

Nonetheless, the range of cybercrime threats to states and citizens justifies the existence of the process. As it develops, along with escalations in significant cyber attacks and online crime, the general public's awareness of this process will increase. Such increased awareness will bring an expectation that the process will enhance global and national capacities to prevent and counter cybercrime. There will also be suspicion from citizens and advocacy organizations that any new instrument could be used to counter human rights, freedom of expression and internet freedoms. Some in the private sector may welcome elements that make it easier to prevent and control illegal online activity (without putting companies or their directors in the firing line of the law), but they will also be wary of anything that restricts their freedoms and ability to profit from ICT. Civil society will want to know how, in practice, this treaty will safeguard their communities against online criminal activity and how companies and governments will be held accountable for its implementation and follow-up.

Given the bipolar nature of the cybercrime discussions up to this point, it will be interesting to see what leaders emerge from outside the Russia–Budapest axis. At present, Russia has submitted a draft convention and the Budapest Convention will be held as the standard by the Western Europe and Others Group (WEOG) countries and potentially also some other member states.

Given these two poles, we outline four possible scenarios for the outcome of the negotiations:

1. **CONTROL: A new convention in line with the Russian draft.** Over the years, Russia's drafts have moved closer to the language and doctrine of the Budapest Convention. But some key red flags remain, which WEOG states will not accept. It is possible – but unlikely – that a convention that favours a highly restrictive view on digital sovereignty, data ownership and human rights will be adopted by vote and not finalized through consensus (although a two-thirds majority vote is required throughout the process). Although it would not be adopted by many countries in the West (and therefore exclude large parts of the tech industry), it would come with a UN badge and therefore a degree of credibility. It would increase Russia's, and possibly China's, role in capacity building among signatories, but not do much to facilitate international cooperation beyond countries already cooperating with each other. Adopting a Russian-driven convention would likely be a step backwards for human rights and freedom of expression online, and a challenge for international companies operating in the countries that adopt it.
2. **CONTROL/ALT: A compromise convention.** The two-thirds voting structure lends itself to this conclusion, with the resulting convention including substantial compromises on terminology and leaving political issues such as human rights and sovereignty open to interpretation. It would be flexible in how provisions can be adopted domestically. This would likely achieve widespread adoption, following in the footsteps of UNTOC, which is almost universally adopted, flexible and apolitical (but without the tools to monitor whether it is implemented effectively). This could provide guidance for criminalization and agreements on principles such as jurisdiction, and create new guidance for international cooperation. It would also advance technical capacity programmes. A review mechanism could increase overall transparency in cybercrime cooperation and create spaces to share innovative approaches and lessons with governments, stakeholders, the private sector and civil society. Like UNTOC, it will face challenges in monitoring implementation, and thereby understanding its impact.
3. **ALT: The alter ego of the Budapest Convention.** A treaty in the Budapest mould and adopted by vote would subvert Russia's intentions and boost the profile and acceptance of the framework and values of the Council of Europe convention, giving that framework a UN badge. Again it would not do much to increase international cooperation across geographies and would not be adopted by some major powers, although it would enhance cooperation between the West and new signatories (and boost the UN's cybercrime capacity-building programme in the process). This would have human rights standards most acceptable to advocacy groups and be acceptable to the private sector, who are already working with the provisions of Budapest.
4. **DELETE: No result.** It is possible that the negotiations are so acrimonious that no result is achieved. This would be a failure, primarily for the Russian government, who have pushed this agenda for so long and have maintained their political priority for it while other allies have waxed and waned. This would also represent a failure for multilateralism, but would not significantly change the current order of the day on cybercrime cooperation, which is regionally fragmented, ad hoc at times and, in some cases, operates in secret.

NOTES

1 See The Global illicit economy: Trajectories of organized crime, GI-TOC, March 2021, https://globalinitiative.net/wp-content/uploads/2021/03/The-Global-Illicit-Economy-GITOC-Low.pdf.

2 Summer Walker, Cyber insecurities? A guide to the UN cybercrime debate, GI-TOC, 2019, https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf.

3 This follows a trend in international cooperation on transnational organized crime more broadly as outlined in a recent study published by the GI-TOC: Yvon Dandurand and Jessica Jahn, The future of international cooperation against Transnational Organized Crime, GI-TOC, 2021, https://globalinitiative.net/analysis/international-cooperation-organized-crime/.

4 The Budapest Convention is a binding instrument addressing cross-border cybercrime cooperation and encouraging harmonization of laws. Drawn up by the Council of Europe and adopted by its Committee of Ministers at the end of 2001, it is the current standard for international efforts to deal with cybercrime.

5 Summer Walker, Cyber insecurities? A guide to the UN cybercrime debate, GI-TOC, 2019, pp 6–7, https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf.

6 Ibid., p 3.

7 Bobby Allyn, Senators demand TikTok reveal how it plans to collect voice and face data, NPR, 18 August 2021, https://www.npr.org/2021/08/18/1028633650/senators-demand-tiktok-reveal-how-it-plans-to-collect-voice-and-face-data.

8 In November 2021, China's new national data privacy statute also took effect, largely modelled on the GDPR. The GDPR is an EU law on data protection and privacy and also addresses the transfer of personal data outside the EU and European Economic Area areas; see also https://gdpr.eu/; Scott Pink, What China's new data privacy law means for US tech firms, Tech Crunch, 9 September 2021, https://techcrunch.com/2021/09/09/what-chinas-new-data-privacy-law-means-for-us-tech-firms/.

9 Tambiama Madiega, Digital sovereignty for Europe, EPRS Ideas Paper, European Parliament, July 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

10 Tom Balmforth and Anton Zverev, Russia arrests top – UN logo executive in treason case, Reuters, 29 September 2021, https://www.reuters.com/technology/moscow-office-group-ib-cybersecurity-firm-searched-by-police-company-2021-09-29/.

11 Kane Wu and Julie Zhu, Billionaire Alibaba founder Jack Ma reappears in Hong Kong – sources, Reuters, 13 October 2021, https://www.reuters.com/world/china/billionaire-alibaba-founder-jack-ma-reappears-hong-kong-sources-2021-10-12/.

12 Jack Nicas, Raymond Zhong, Daisuke Wakabayashi, Censorship, surveillance and profits: A hard bargain for Apple in China, *The New York Times*, 17 June 2021, https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.

13 Salvador Rodriguez, TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance. CNBC, 25 June 2021, https://www.theverge.com/2020/10/15/21517403/tiktok-security-servers-separate-bytedance-china-trump-ban; Kim Lyons, TikTok chief security officer says its servers are already separate from ByteDance, The Verge, 15 October 2020, https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html.

14 Natasha Lomas, Apple and Google bow to pressure in Russia to remove Kremlin critic's tactical voting app, TechCrunch, 17 September 2021, https://techcrunch.com/2021/09/17/apple-and-google-bow-to-pressure-in-russia-to-remove-kremlin-critics-tactical-voting-app/.

15 Tate Ryan-Mosley, Why you should be more concerned about internet shutdowns, MIT Technology Review, 9 September 2021, https://www.technologyreview.com/2021/09/09/1035237/internet-shutdowns-censorship-exponential-jigsaw-google/; United Nations human Rights Council, Ending Internet shutdowns: a path forward, United Nations, 15 June 2021, https://undocs.org/A/HRC/47/24/Add.2.

16 AccessNow, #KeepItOn, https://www.accessnow.org/keepiton/.

17 Defined as 'a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit'. United Nations Office on Drugs and Crime, United Nations Convention against Transnational Organized Crime and the Protocols thereto, United Nations. New York, 2004, https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC/Convention/TOCebook-e.pdf.

18 United Nations Office on Drugs and Crime, United Nations Convention against Corruption, United Nations, New York, 2004, https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf.

19 Japan, Submissions from Member States related to the first session of the ad hoc committee, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/National_submission_JAPAN_AHC.pdf.
20 United Nations Economic and Social Council, Report on the meeting of the Expert Group to conduct a Comprehensive Study on Cybercrime, held in Vienna from 3 to 5 April 2018, United Nations, 2018, https://undocs.org/E/CN.15/2018/12.
21 Russia, Submissions from Member States related to the first session of the ad hoc committee, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.
22 African Union Convention on Cyber Security and Personal Data Protection, Doc. No. EX.CL/846(XXV), African Union, https://www.opennetafrica.org/?wpfb_dl=4.
23 League of Arab States General Secretariat, Arab Convention on Combating Information Technology Offences, League of Arab States, n.d., https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab/Convention/on/Combating/Information/Technology/Offences.pdf.
24 Summer Walker, Cyber insecurities? A guide to the UN cybercrime debate, GI-TOC, 2019, https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf.
25 Adrian Shahbaz and Allie Funk, The global drive to control Big Tech, Freedom House, Washington DC, https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.
26 Biden rows back on Facebook 'killing people' comment, BBC News, 20 July 2021, https://www.bbc.co.uk/news/technology-57901710.
27 Clean out online cesspit now, Keir Starmer tells Boris Johnson, BBC News, 20 October 2021, https://www.bbc.co.uk/news/uk-politics-58980384.
28 Council of Europe, Convention on Cybercrime, Budapest, 23.XI.2001, Title 3 – Content-related offences, Article 9 – Offences related to child pornography, https://rm.coe.int/1680081561.
29 Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28 January 2003, https://rm.coe.int/168008160f.
30 African Union, African Union Convention on Cyber Security and Personal Data Protection, 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.
31 League of Arab States General Secretariat, Arab Convention on Combating Information Technology Offences, League of Arab States, n.d., https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab/Convention/on/Combating/Information/Technology/Offences.pdf.
32 Shanghai Cooperation Organization, Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization.
33 Russia, United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Draft, Unofficial translation, 29 June 2021, Submissions from Member States related to the first session of the ad hoc committee https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.
34 Russia, Submissions from Member States related to the first session of the ad hoc committee, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.
35 Mexico, Elements of the Government of Mexico for the United Nations Ad Hoc Committee to elaborate a comprehensive international Convention on countering the use of information and communications technologies for criminal purposes, Submissions from Member States related to the first session of the ad hoc committee, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.
36 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, https://www.unodc.org/documents/Cybercrime/SG_report/V1908182_E.pdf.
37 For example, where the offence occurs in one country, a service provider is in another and the data is stored in a third country.
38 Michael Sheils McNamee, HSE cyber-attack: Irish health service still recovering months after hack, BBC, 5 September 2021, https://www.bbc.com/news/world-europe-58413448.
39 Joseph Menn, Kaseya ransomware attack sets off race to hack service providers – researchers, Reuters, 3 August 2021, https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/.
40 David Sanger and Nicole Perlroth, Biden warns Putin to act against ransomware groups, or U.S. will strike back, *The New York Times*, 9 July 2021, https://www.nytimes.com/2021/07/09/us/politics/biden-putin-ransomware-russia.html.
41 Ryan Browne, Hackers behind Colonial Pipeline attack reportedly received $90 million in bitcoin before shutting down, CNBC, 18 May 2021, https://www.cnbc.com/2021/05/18/colonial-pipeline-hackers-darkside-received-90-million-in-bitcoin.html.
42 Joseph Menn, Kaseya ransomware attack sets off race to hack service providers – researchers, Reuters, 3 August 2021, https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/.
43 Jamaica's comments on the scope, objectives and structure of an International Convention On Countering The Use Of Information And Communications Technologies For Criminal Purposes, submissions from Member States related to the first session of the ad hoc committee, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.

44 Training on investigation involves evidence techniques and how to combine traditional investigation methods with new technologies. Training on evaluation and analysis involves how to analyze the evidence that is presented, how to make sure the evidence has not been altered, and how to connect current laws with modern crimes. Also see: Organization of American States, Inter-American Portal on Cybercrime, http://www.oas.org/en/sla/dlc/cyber-en/programa-capacitacion.asp.

45 United Nations Interregional Crime and Justice Research Institute, AI for safer children, 8 March 2021, http://www.unicri.it/news/AI-Safer-Children-Online.

46 Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Organizational session of the Ad Hoc Committee, New York, 10-12 May 2021.

47 United Nations Third Committee, Interactive dialogues under the following items:108, 109 and 110: Crime; Information and Technologies; Drugs(virtual), 11 October 2021.

48 Ian Tennant, The promise of Palermo, GI-TOC, October 2020.

49 United Nations, Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August–7 September 1990, https://www.unodc.org/documents/congress//Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf.

50 G8 Communiqué, Meeting of Justice and Interior Ministers, December 9–10, 1997, https://www.justice.gov/sites/default/files/ag/legacy/2004/06/08/97Communique.pdf.

51 United Nations, Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century, 2000, https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/010_ACONF.187.4.Rev.3_Vienna_Declaration_on_Crime_and_Justice.pdf.

52 United Nations General Assembly, Resolution adopted by the General Assembly: Combating the criminal misuse of information technologies, United Nations, 22 January 2001, https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2000/General_Assembly-/A-RES-55-63.pdf.

53 United Nations General Assembly, Resolution adopted by the General Assembly: Combating the criminal misuse of information technologies, United Nations, 23 January 2002, https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2001/General_Assembly-/A-RES-56-121.pdf.

54 United Nations General Assembly, Resolution adopted by the General Assembly: Combating the criminal misuse of information technologies, United Nations, 23 January 2002, https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2001/General_Assembly-/A-RES-56-121.pdf.

55 United Nations, Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime prevention and criminal justice systems and their development in a changing world, 2010, https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf.

56 United Nations, General Assembly Resolution A/RES/74/247, Countering the use of information and communications technologies for criminal purpose, https://digitallibrary.un.org/record/3841023?ln=en.

57 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime: Draft – February 2013, United Nations, Vienna, 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

58 UN Doc. A/RES/73/187, 17 December 2018.

59 United Nations General Assembly, Resolution adopted by the General Assembly on 27 December 2019: Countering the use of information and communications technologies for criminal purposes, United Nations, 20 January 2020, https://undocs.org/A/Res/74/247.

60 Ad hoc committee established by General Assembly resolution 74/247, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

61 Summer Walker, Contested domain: UN cybercrime resolution stumbles out of the gate, GI-TOC, 2 June 2021, https://globalinitiative.net/analysis/un-cybercrime-resolution/.

62 Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Draft resolution countering the use of information and communications technologies for criminal purposes, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Draft_proposal_12_May_2021.pdf.

63 Brazil: amendment to revised draft resolution A/75/L.87/Rev.1, Countering the use of information and communications technologies for criminal purposes, UN Doc. A/75/L.90 25 May 2021, https://www.undocs.org/en/A/75/L.90; see also Summer Walker, Contested domain: UN cybercrime resolution stumbles out of the gate, GI-TOC, 2 June 2021, https://globalinitiative.net/analysis/un-cybercrime-resolution/.

64 Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname and Trinidad and Tobago: amendment to revised draft resolution A/75/L.87/Rev.1, Countering the use of information and communications technologies for criminal purposes, UN Doc. A/75/L.91, 25 May 2021, https://www.undocs.org/en/A/75/L.91; see also Summer Walker, Contested domain: UN cybercrime resolution stumbles out of the gate, GI-TOC, 2 June 2021, https://globalinitiative.net/analysis/un-cybercrime-resolution/.

65 United Kingdom of Great Britain and Northern Ireland: amendment to revised draft resolution A/75/L.87/Rev.1, Countering the use of information and communications technologies for criminal purposes, UN Doc. A/75/L.92, 25 May 2021, https://undocs.org/A/75/L.92; see also Summer Walker, Contested domain: UN cybercrime resolution stumbles out of the gate, GI-TOC, 2 June 2021, https://globalinitiative.net/analysis/un-cybercrime-resolution/.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with 500 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net