From Budapest to Hanoi: Comparing the Council of Europe and United Nations Cybercrime Conventions

Kenneth Propp and DeBrae Kennedy-Mayo

Introduction

On Christmas Eve 2024, the United Nations General Assembly (UNGA) adopted[1] the Convention Against Cybercrime (UN Convention), elaborately subtitled "Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes"[2]. Later this year, Viet Nam will host a signing ceremony in Hanoi, at which many UN members are expected to sign the UN Convention.[3] It will enter into force once forty UN members have completed their domestic ratification procedures[4], which likely will take several years.

The UN Convention has been dogged by controversy from its beginning. Many Western countries, including the United States and Europe, initially opposed the very idea of a universal cybercrime treaty. Instead, they encouraged countries to accede to the 2001 Council of Europe (COE) Cybercrime Convention and its protocols. Their efforts have yielded considerable success: today the COE Cybercrime Convention[5] (popularly known as the Budapest Convention after the city that hosted its signing conference) boasts 78 parties, with more than 10 of these countries joining the Budapest Convention during the time that the UN Convention was being negotiated.[6]

But even widespread adherence to the Budapest Convention will never yield universal coverage. Major countries including China, India, and Russia have not joined it, nor are likely to. The Budapest Convention originally was negotiated by the COE membership along with a handful of

[1] UN General Assembly Adopts Landmark Convention on Cybercrime, United Nations Office on Drugs and Crime (December 24, 2024), https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html.

[2] United Nations Convention Against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (December 24, 2024) [hereinafter UN Convention], https://www.unodc.org/unodc/en/cybercrime/convention/home.html.

[3] Gia Nghi, "Hanoi to Host UN Cybercrime Convention Signing in 2025," The Saigon Times (December 25, 2024), https://english.thesaigontimes.vn/hanoi-to-host-un-cybercrime-convention-signing-in-2025/.

[4] UN Convention, Article 65, https://www.unodc.org/unodc/en/cybercrime/convention/home.html.

[5] Council of Europe Convention on Cybercrime, European Treaty Service No. 185 (November 23, 2001) [hereinafter Budapest Convention], https://rm.coe.int/1680081561.

[6] During this time, the countries that acceded to the Budapest Convention included Brazil and Nigeria. As of this writing, additional countries are in the process of accession or are considering signing the Budapest Convention. "Rwanda becomes the 78th Party to the Convention on Cybercrime and accedes to the First Protocol – Cybercrime," T-CY News, Council of Europe Cybercrime (January 10, 2025), https://www.coe.int/en/web/cybercrime/-/rwanda-becomes-the-78th-party-to-the-convention-on-cybercrime-and-accedes-to-the-first-protocol; *see* Charter of Signatures and Ratifications of Treaty, Treaty Office, Council of Europe, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

non-COE countries invited to these negotiations,[7] leading some countries in the Global South to regard it as "in name and spirit a European convention" and to "dismiss [it] as non-inclusive and non-representative."[8] Some ex-colonies viewed it as insufficiently sensitive to state sovereignty.[9]

In addition to encouraging a wide range of countries to join the Budapest Convention, Western countries pursued the parallel strategy of resisting the notion of a universal convention. Russia sensed an opening. In 2017, Russian diplomatic representatives sent a letter to the UN membership containing a draft UN convention on cybercrime, putting Western countries on the back foot.[10] Two years later, Russia and a number of other authoritarian states put before the General Assembly a resolution calling for negotiation of a UN convention on cybercrime; the United States and Europe opposed it. The contentious resolution was adopted by a close 79-60 vote.[11]

Negotiations on the UN Convention began in 2022, conducted by an Ad Hoc Committee of UN members, and supported by the secretariat of the UN Office of Drugs and Crime (UNODC). Russia and like-minded countries proposed as chair of the negotiations Algerian Ambassador Faouzia Boumaiza-Mebarki. The United States and Europe opposed her selection – but again were defeated. (In the event, Ambassador Mebarki proved a fair-minded chair of the negotiations.) Talks stretched over three years.

UNODC had also been the host for the negotiations two decades ago that resulted in the 2000 UN Convention Against Transnational Organized Crime (UNTOC) and the 2003 Convention Against Corruption (UNCAC). Both instruments are today widely regarded as successes. The UNTOC Convention has 192 parties,[12] and the Corruption Convention has 191.[13] UNTOC and UNCAC were negotiated during the late 1990's in a greatly different geopolitical environment. Russia, then led by Boris Yeltsin, and China were broadly supportive of both initiatives. The UNTOC and UNCAC negotiations proved largely harmonious, and the UN membership approved both by consensus.

---

[7] The United States, Canada, Japan, and South Africa took part in the negotiations of the Budapest Convention. Joining the Convention on Cybercrime: Benefits, Budapest Convention on Cybercrime, Council of Europe (April 19, 2023), https://rm.coe.int/cyber-buda-benefits-19april2023-en/1680aafa3d. South Africa later decided against ratifying the Budapest Convention, raising concerns related to sovereignty. Mailyn Fidler "South Africa Introduces Revised Cybercrime Legislation, Acknowledging Criticism," Council of Foreign Relations (March 7, 2017), https://www.cfr.org/blog/south-africa-introduces-revised-cybercrime-legislation-acknowledging-criticism.

[8] Gatra Priyandita & Bart Hogeveen, "The UN Cybercrime Convention: A Victory for State Sovereignty," The Strategist, Australian Strategic Policy Institute (August 16, 2024), https://www.aspistrategist.org.au/the-un-cybercrime-convention-a-victory-for-state-sovereignty/.

[9] *Id*.

[10] Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, United Nations Digital Library (October 11, 2017), https://digitallibrary.un.org/record/1327693?ln=en&v=pdf.

[11] Countering the Use of Information and Communications Technologies for Criminal Purposes, Resolution adopted by the General Assembly on December 27, 2019, A/RES/74/247, United Nations (January 20, 2020, n1944028.pdf.

[12] Signatories to the United Nations Convention Against Transnational Crime and its Protocols, United Nations, https://www.unodc.org/unodc/en/treaties/CTOC/signatures.html.

[13] Signature and Ratification Status, United Nations Convention Against Corruption, https://www.unodc.org/corruption/en/uncac/ratification-status.html.

The UN Convention negotiations were a different story. Putin's Russia was at war with Ukraine, and consequently at odds with many members of the United Nations. Russia's positions enlisted sympathy from a sizeable number of authoritarian states, including Belarus, China, Cuba, Iran, North Korea, and Venezuela. Over eight lengthy and contentious rounds, negotiators clashed over fundamental visions of the UN Convention.

Key issues including what types of criminality the UN Convention would address were settled only during the very last session in August 2024. In a dramatic development, Iran, supported by Russia, insisted on seven rounds of voting in an effort to defeat a series of human rights safeguards sought by Western countries. It was the first time ever in a UN crime convention negotiation that voting had been needed. Each vote only mustered twenty or so countries against the safeguards, however.[14] The UN Convention then moved to the UNGA, which ultimately approved it by consensus.

The UN Convention continued to attract strong criticism from civil society groups and major technology companies even after UNGA passage. A series of press articles have appeared bearing provocative titles such as "The UN finally advances a convention on cybercrime…and no one is happy about it,"[15] and "UN Cybercrime Treaty: Why is the Tech Industry up in arms?"[16].

One helpful way to analyze the UN Convention, and to understand why it has generated such controversy, is to examine its provisions in light of those of the Budapest Convention.[17] This article pursues such a comparative approach. It identifies commonalities and differences between the two multilateral cybercrime instruments to determine how far the UN Convention departs from its predecessor and to aid an assessment of how it might affect the work of cybercrime investigators and prosecutors. This article also explores selected major criticisms that have been made of the UN Convention, focusing mainly on those from representatives of civil society and technology companies.

---

[14] Gatra Priyandita & Bart Hogeveen, "The UN Cybercrime Convention: A Victory for State Sovereignty," The Strategist, Australian Strategic Policy Institute (August 16, 2024), https://www.aspistrategist.org.au/the-un-cybercrime-convention-a-victory-for-state-sovereignty/.

[15] Lisandra Novo, "The UN finally Advances a Convention on Cybercrime . . . and No One is Happy About It," Atlantic Council (August 14, 2024), https://www.atlanticcouncil.org/blogs/new-atlanticist/the-un-finally-adopts-a-convention-on-cybercrime-and-no-one-is-happy/.

[16] Kristian McCann, "UN Cybercrime Treaty: Why Is the Tech Industry up in Arms?" Cyber Magazine (November 18, 2024), https://cybermagazine.com/articles/un-cybercrime-treaty-why-is-the-tech-industry-up-in-arms.

[17] The Second Additional Protocol to the Budapest Convention addresses concerns related to the globalization of criminal evidence as well as to data protection, particularly after the enactment of the EU's General Data Protection Regulation (GDPR) and the implementation of similar laws in countries around the world. Second Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224), Convention on Cybercrime, Council of Europe, https://www.coe.int/en/web/cybercrime/second-additional-protocol; *see* Jennifer Daskal & DeBrae Kennedy-Mayo, "Budapest Convention: What Is It and How Is It Being Updated?" Cross-Border Data Forum (July 2, 2020), https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/; Jennifer Daskal, Peter Swire, & Théodore Christakis, "The Globalization of Criminal Evidence," IAPP (October 16, 2018), https://iapp.org/news/a/the-globalization-of-criminal-evidence/.

It is important as a preliminary matter to understand which countries are eligible to join the UN Convention as compared to those eligible for the Budapest Convention. The 193 countries that are members of the UN are eligible to accede to the UN Convention, which means that countries with all types of governments – both democracies and non-democracies – are welcome.[18]

Conversely, the Budapest Convention has a stringent process in place for determining those countries that can benefit from its provisions. Prior to a country which is not part of the COE [19] (or was not part of the original negotiations of the Budapest Convention) being formally invited to accede to the Budapest Convention, it must undergo an approval process, which includes an examination of the country's relevant substantive law and procedural law as well as adherence to the safeguards outlined in Article 15 of the Budapest Convention.[20] All parties to the Budapest Convention must unanimously consent to an application, and the COE's governing Committee of Ministers must approve by a two-thirds majority.[21] Assuming the new country makes it through this COE process, then its internal accession process may proceed.[22] This approach assures that

---

[18] UN Convention, https://www.unodc.org/unodc/en/cybercrime/convention/home.html. Non-member observer States the Holy See and the State of Palestine are also eligible to join the Convention, as are regional economic integration organizations such as the European Union.

[19] Notably, Ireland signed the Budapest Convention in 2002, but has yet to ratify the instrument. Chart of Signatures and Ratifications of Treaty 185, Convention of Cybercrime (ETS No. 185), Treaty Office, Council of Europe, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

[20] Article 15(1) states, "Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality." Budapest Convention, https://rm.coe.int/1680081561.

[21] The Budapest Convention opened for signature in 2001. "20 Years of Budapest Convention: An Important Milestone in the Flight Against Cybercrime," Delegation of the European Union to the Council of Europe, European Union (November 17, 2021), https://www.eeas.europa.eu/delegations/council-europe/20-years-budapest-convention-important-milestone-fight-against-cybercrime_en?s=51. The four non-COE countries invited to the original negotiations of the Budapest Convention – Canada, Japan, South Africa, and the United States – were able to forego this invitation process. The United States was the first non-COE member to ratify the treaty in 2007, followed by Japan in 2012, and Canada in 2015. Chart of Signatures and Ratifications of Treaty 185, Convention of Cybercrime (ETS No. 185), Treaty Office, Council of Europe, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. Although South Africa signed the treaty in 2001, the country did not subsequently ratify the Budapest Convention. Mailyn Fidler "South Africa Introduces Revised Cybercrime Legislation, Acknowledging Criticism," Council of Foreign Relations (March 7, 2017), https://www.cfr.org/blog/south-africa-introduces-revised-cybercrime-legislation-acknowledging-criticism.

[22] Countries wishing to be part of the Budapest Convention are required to undergo a review of the country's legal system which typically includes an examination of relevant substantive law, procedural law, and the safeguards described in Article 15 of the Budapest Convention. *See* Convention on Cybercrime (ETS No. 185): Request by Mozambique to be Invited to Accede (January 15, 2025), Rapporteur Group, Appendix 2, Section 3.2 Safeguards, Package presented GR-J at January 31, 2025 meeting, https://search.coe.int/cm?i=0900001680ae2c8d. This country-specific review is conducted by the COE Committee on Ministers' Rapporteur Group on Legal Co-operation (GR-J) and then the COE Committee of

countries that join the Budapest Convention meet threshold requirements in their domestic legal framework and in international human rights treaties to which they are party, such as the International Covenant for Civil and Political Rights.[23]

This paper now turns to a detailed examination of the UN Convention's provisions, combined with analysis of similarities and differences with the Budapest Convention, and discussion of criticisms that have been published about the UN Convention. An appendix contains a side-by-side chart of the texts of the two Conventions, enabling readers to discern precisely what each provides.

UN Convention Chapter I – General Provisions

Chapter I contains definitions, scope provisions, and a provision on respect for human rights, among other subjects.

Article 2 (use of terms) defines key terms, including "information and communications technology system" (Article 2(a)). "Serious crime" (Article 2(h)) constitutes an offense punishable by four years or more of imprisonment, in line with the definition set out in the UNTOC Convention.

The Convention applies to the prevention of criminalized offenses as well as to their investigation and prosecution (Article 3(a)).

Article 4 (offences established in accordance with other United Nations conventions and protocols) stipulates that offenses criminalized under other UN conventions, such as UNTOC and UNCAC, shall also be considered criminal "when committed through the use of information and communications technology systems (ICTS)" (Article 4(1)).

Article 5 (protection of sovereignty) recognizes the principle of judicial sovereignty, stating that the UN Convention does not entitle one State Party "to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law" (Article 5(2)). This provision is commonly found in UN criminal law conventions; it carries important symbolic weight for many countries.

Article 6 (respect for human rights) ensures that States Parties carry out their obligations under the UN Convention in a manner consistent with their obligations under international human rights law. (Article 6(1)). It also includes an admonishment that the UN Convention shall not be interpreted as permitting suppression of rights related to free expression and other fundamental freedoms. (Article 6(2)). These two measures are not found in prior UN criminal law conventions. Many governments consider the latter provision as a significant innovation to prevent use of the UN Convention for purposes of suppressing dissent.

Ministers. Accession by States Which Are Not Member States of the Council of Europe and Which Have Not Participated in the Elaboration of the Convention, Convention on Cybercrime, Directorate of Legal Advice and Public International Law Treaty Office, Council of Europe (May 2022), https://rm.coe.int/16808ff396.

[23] United Nations International Covenant on Civil and Political Rights (December 16, 1966), https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights. Notably, China is not a party to the International Covenant on Civil and Political Rights. Status for International Covenant on Civil and Political Rights, United Nations Treaty Collection, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en.

Relevant Budapest Convention Provision

An analysis by the Council of Europe Cybercrime Division states that the definitional provisions of the Budapest Convention (Article 1) are "identical with or similar to" those of Article 2 of the UN Convention.[24] There are certain terminological differences. For example, the term "computer system" is used to describe the subject-matter of the Budapest Convention, whereas the UN Convention uses "information and communication technology system" instead.

Although the Budapest Convention does not have a separate express human rights provision, the preamble recognizes "the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties...."[25]

Critics' Concerns

The term "cybercrime", used in the title to the UN Convention, is undefined, which some critics regard as potentially overbroad and vague.[26] (The Budapest Convention also fails to define this term.) Other critics see the subtitle of the UN Convention as further muddling the concept of cybercrime.[27]

Some critics disagreed with the decision to include within the scope of the UN Convention offenses criminalized under other UN conventions, pointing instead approvingly to the narrower scope of the Budapest Convention.[28]

Businesses raised concerns that the requirement in Article 6 for states to implement their obligations under the UN Convention "consistent with their obligations under international human rights law" could be "unevenly implemented across jurisdictions".[29] The Office of the UN High

---

[24] Conventions on Cybercrime: The Budapest Convention and the Draft UN Treaty, Briefing Note, Council of Europe (August 27, 2024), https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a.

[25] Preamble, Budapest Convention, https://rm.coe.int/1680081561.

[26] Letter from Software & Information Industry Association (SIIA) and Computer & Communications Industry Association (CCIA) (November 1, 2024), https://www.siia.net/wp-content/uploads/2024/11/Industry-Letter-UN-Convention-Against-Cybercrime.pdf.

[27] Cybersecurity Tech Accord Submission to the Resumed Concluding Session of the Ad Hoc Committee to Elaborate a UN Convention on Countering Cybercrime (July 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Cybersecurity_Tech_Accord_-_7th_AHC_resumed_session_submission_E.pdf.

[28] "GNI calls on Member States not to support the UN Cybercrime Convention," Global Network Initiative (October 7, 2024), https://globalnetworkinitiative.org/gni-statement-on-uncc/.

[29] Industry Perspectives Ahead of the Reconvened Concluding Session of the UN Ad Hoc Committee on Cybercrime, International Chamber of Commerce (June 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/ICC_industry_perspectives_AHC_reconvened_concluding_session.pdf; *see* Andrew Adams & Daniel Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention," *Lawfare* (December 9, 2024), https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention.

Commissioner for Human Rights advocated for explicitly referencing specific human rights instruments, such as the International Covenant for Civil and Political Rights, in Article 6.[30]

UN Convention Chapter II – Criminalization

The UN Convention elaborates eleven criminalization obligations (Articles 7-17). Each State Party must adopt legislation establishing these offenses in its domestic law.

Criminalization obligations are a well-known feature of multilateral crime conventions, such as UNTOC and UNCAC, and the Budapest Convention. These provisions establish agreed common elements of newer types of crimes with international impact, ensuring that governments have conceptually unified bases for addressing them, and helping provide dual criminality to enable recognition by one country that another country's laws prohibit the same conduct.[31]

Articles 7-17 (criminalization) of the UN Convention contain two types of obligations. One type, cyber-dependent offenses, such as illegal access (Article 7), can only be committed through use of an information and communications technology system. The other offenses addressed in this chapter, such as solicitation for purposes of committing a sexual offense against a child (Article 15) or money laundering (Article 17) are not necessarily cyber-dependent, but they can be committed through use of an ICTS. The Convention obliges criminalization of such conduct to the extent that an ICTS is utilized.

The offenses to be criminalized are: illegal access to an ICTS (Article 7); illegal interception (Article 8); interference with electronic data (Article 9); interference with an ICTS (Article 10); misuse of devices (Article 11); ICTS-related forgery (Article 12); ICTS-related theft or fraud (Article 13); offenses related to online child sexual abuse (Article 14); solicitation or grooming for purposes of committing a sexual offense against a child (Article 15); non-consensual dissemination of intimate images (Article 16); and laundering of proceeds of crime (Article 17).

Chapter II also establishes the liability of legal persons (Article 18) for participation in the offenses criminalized. In addition, participation in and attempt to commit (Article 19) these offenses is also criminalized. These two articles were adapted from counterparts in UNTOC and UNCAC.

---

[30] Submission of the Office of the United Nations High Commissioner for Human Rights, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (July 22, 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/OHRC_AHC_Cybercrime_-_reconvened_concluding_session.pdf; *see* United Nations International Covenant on Civil and Political Rights (December 16, 1966), https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

[31] *See* Jonathan Clough, "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization," Monash University Law Review (2014), https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf; *see also* Ophelie Brunelle-Queraishi, "Assessing the Relevancy and Efficacy of the United Nations Convention Against Corruption: A Comparative Analysis" 2 Notre Dame J. Int'l & Comp. L. 101 (2011). Brunelle-Queraishi discusses the usefulness of requiring criminalization to ensure international cooperation and dual-criminality, a requirement for extradition.

Due process protections in criminal prosecutions are addressed by providing that a State Party must ensure that an accused person receives "all rights and guarantees in conformity with domestic law and consistent with the applicable international obligations of the State Party" (Article 21(4)). This provision makes specific mention of the right to a fair trial and the rights of a defendant (Article 21(4)).

Relevant Budapest Convention Provisions

Articles 7-14 of the UN Convention are "more or less identical with" those of Articles 2-9 of the Budapest Convention, according to the COE analysis.[32] Articles 15 and 16 of the UN Convention on child sexual offenses, however, have no counterpart in the Budapest Convention. The COE analysis considers that "these articles add value to the UN treaty". Money laundering also is not dealt with in the Budapest Convention. On the other hand, the Budapest Convention does contain an article related to copyright infringement (Article 10), which is not addressed in the UN Convention.

Article 11 of the Budapest Convention (attempt or aiding and abetting) corresponds to Article 19 of the UN Convention. Article 12 of the Budapest Convention (corporate liability) corresponds to Article 18 of the UN Convention.

The Budapest Convention omits any specific language referring to due process protections such as the right to a fair trial or the rights of a defendant in a criminal proceeding, but it does reference the International Covenant for Civil and Political Rights[33] which protects these due process rights (Article 15).

Critics' Concerns

A chorus of companies argued that the scope of the UN Convention should be limited to cyber-dependent crimes, since a variety of cyber-enabled crimes, such as money laundering, are already addressed in other international criminal law instruments.[34]

Two U.S. criminal defense lawyers further assert that the articles on illegal access, illegal interception, and interference with electronic data (Articles 7-10) "do not contain any meaningful intent requirement".[35] Article 7, for example, "subtly but importantly diverges from the Budapest Convention" in such a way that could potentially permit a party to circumvent generally accepted criminal intent requirements.[36] The UN Convention tracks analogous language in the Budapest

---

[32] Conventions on Cybercrime: The Budapest Convention and the Draft UN Treaty, Briefing Note, Council of Europe (August 27, 2024), https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a.

[33] United Nations International Covenant on Civil and Political Rights, Article 9 (December 16, 1966), https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

[34] Industry Perspectives Ahead of the Reconvened Concluding Session of the UN Ad Hoc Committee on Cybercrime, International Chamber of Commerce (June 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/ICC_industry_perspectives_AHC_reconvened_concluding_session.pdf.

[35] Andrew Adams & Daniel Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention," *Lawfare* (December 9, 2024), https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention.

[36] *Id*.

Convention by including "the intent of obtaining electronic evidence" and "other dishonest… intent" but the UN Convention then adds "or criminal intent."[37] In the view of these critics, this broad reference to intent in relation to illegal access could open the door to targeting of journalists or dissidents.[38]

Other critics worry that the UN Convention articles on illegal access and interception are broad enough to cover legitimate activity by cybersecurity researchers and ethical hackers.[39] They believe that the UN Convention should have provided specific protection for these activities. Advocates for these actors did succeed in having inserted in Article 53 (preventive measures) an approving reference to the "legitimate activities of security researchers", but that provision, while helpful, is far from the criminalization exemption they sought.

The UN Convention's provision on ICTS-related theft or fraud (Article 13) has drawn criticism because it criminalizes factual deception "that causes a person to do or omit to do anything which that person would not otherwise do or omit to do." This broad element conceivably could reach the activities of cybersecurity researchers and ethical hackers, it is alleged.[40] The counterpart Budapest Convention provision on computer-related fraud (Article 8) more narrowly requires that the fraud cause a loss of property.

Corporate representatives also argued that the innovative provision on online child sexual abuse and sexual exploitation material (Article 14) is so broadly worded that it could criminalize children taking and transmitting sexually suggestive photos ('sexting').[41] They felt that countries should be

---

[37] UN Convention, Article 7, https://www.unodc.org/unodc/en/cybercrime/convention/home.html; *see* Budapest Convention, Article 2, https://rm.coe.int/1680081561.

[38] Andrew Adams & Daniel Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention," *Lawfare* (December 9, 2024), https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention (*citing* Anna Brakha, "How Russia Silences Critical Coverage of its War in Ukraine," Committee to Protect Journalists (August 7, 2024), https://cpj.org/2024/08/how-russia-silences-critical-coverage-of-its-war-in-ukraine/).

[39] Katitza Rodriguez, "If Not Amended, States Must Reject the Flawed Draft UN Cybercrime Convention Criminalizing Security Research and Certain Journalism Activities," Electronic Frontier Foundation (June 14, 2024), https://www.eff.org/deeplinks/2024/06/if-not-amended-states-must-reject-flawed-draft-un-cybercrime-convention. With regard to this concern, the Explanatory Notes for the UN Convention acknowledge "the work of ethical hackers and security researchers who provide authorized penetration testing and vulnerability testing," including the inclusion of the term "without right" in Articles 6 to 10. Explanatory Notes on the Revised Draft Text of the Convention, Articles 6 to 10: Offenses Against the Confidentiality, Integrity, and Availability of Data Systems (January 24, 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Documents/Ad_Hoc_Committee_-_Explanatory_notes_RDTC.pdf. Additionally, Article 11 (criminalizing misuse of devices) clarifies that it should not be interpreted to impose criminal liability where the activity is not for the purpose of committing an offense. UN Convention, Article 11(2), https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdf.

[40] "GNI calls on Member States not to support the UN Cybercrime Convention," Global Network Initiative (October 7, 2024), https://globalnetworkinitiative.org/gni-statement-on-uncc/.

[41] Cybersecurity Tech Accord Submission to the Resumed Concluding Session of the Ad Hoc Committee to Elaborate a UN Convention on Countering Cybercrime (July 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Cybersecurity_Tech_Accord_-_7th_AHC_resumed_session_submission_E.pdf.

required – rather than simply permitted by Article 14(4) – to except material maintained exclusively for the private and consensual use of the persons involved.

The article establishing corporate liability for participation in a criminalized offense (Article 18), modeled on UNTOC and UNCAC, does not contain an express intent requirement, leading to the charge that it potentially could be wielded against companies engaged in content moderation.[42] Article 19 (participation and attempt) drew a similar complaint for conceivably expanding criminal liability to third-party platforms. "The thresholds and intent standards of these provisions [of the UN Convention] are lower than those of corresponding articles of the Budapest Convention," according to the COE.[43]

Similar to their questions about the sufficiency of Article 6 (respect for human rights), critics also raised concerns that the due process protections (Article 21) are restricted to those found in each State Party's domestic law and its international commitments.[44]

UN Convention Chapter IV – Procedural Measures and Law Enforcement

This Chapter prescribes a range of powers and procedures that States Parties must have in place for purposes of investigating and prosecuting cybercrime. Article 23 requires that these tools be available not only for the offenses criminalized under Chapter II, but also for other criminal offenses committed by means of an ICTS and for the collection of electronic evidence of any criminal offense.

These powers and procedures are to be exercised subject to safeguards provided for "pursuant to the domestic law of each State Party" and in accordance with each State Party's "obligations under international human rights law" (Article 24). The article identifies the following safeguards: judicial or other independent review, the right to an effective remedy, and the principle of proportionality (Article 24). These safeguards apply both in domestic proceedings and in international cooperation (Article 24(4)). However, whereas other articles in this chapter require that "each State Party shall adopt such legislation and other measures as may be necessary to" enact the particular requirements[45], Article 24 does not. During the final round of negotiations, many Western governments which participated in the UN cybercrime negotiations intervened to cite these Article

---

[42] "Civil Society Sends Joint Letter Urging EU and Member States to Withdraw Support From Rights-harming UN Cybercrime Convention," CyberPeace Institute (October 22, 2024), https://cyberpeaceinstitute.org/news/civil-society-joint-letter-un-cybercrime-convention/#:~:text=We%2C%20the%20undersigned%20organisations%20and%20individual%20experts%2C%20urge,comes%20to%20a%20vote%20at%20the%20General%20Assembly.

[43] Conventions on Cybercrime: The Budapest Convention and the Draft UN Treaty, Briefing Note, Council of Europe (August 27, 2024), https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a.

[44] *See* Andrew Adams & Daniel Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention," *Lawfare* (December 9, 2024), https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention; "GNI calls on Member States not to support the UN Cybercrime Convention," Global Network Initiative (October 7, 2024), https://globalnetworkinitiative.org/gni-statement-on-uncc/.

[45] *See* UN Convention, Article 23, 25-31, https://www.unodc.org/unodc/en/cybercrime/convention/home.html.

24 safeguards as a crucial protection against abuse of the Convention, as observed by one of the authors of this article.

The principal powers and procedures are: expedited preservation of stored electronic data (Article 25); expedited preservation and partial disclosure of traffic data (Article 26); orders requiring the production of stored electronic data (Article 27); powers to search and seize stored electronic data (Article 28); real-time collection of traffic data (Article 29); interception of content data (Article 30); and asset freezing, seizure and confiscation (Article 31).

Relevant Budapest Convention Provisions

With regard to safeguards (Article 15), the Budapest Convention requires that each Party ensure that its domestic law provide for "adequate protection of human rights and liberties."[46] As with the preamble to the Budapest Convention, this article specifically mentions the 1950 COE Convention on Human Rights and the 1966 UN International Covenant on Civil and Political Rights when referencing applicable human rights instruments. The discussion of safeguards also includes the principle of proportionality, judicial supervision, and rights of third parties.

With regard to procedural powers, the COE analysis describes the UN and Budapest Conventions as "more or less identical".[47] For example, both make these powers available not only for offenses criminalized but also for other crimes committed by means of an ICTS. The procedural powers common to both are: expedited preservation of stored data (including traffic data), production orders, search and seizure, real-time collection of traffic data, and interception of content data.

On the other hand, the Second Additional Protocol to the Budapest Convention[48] goes beyond the UN Convention by providing certain innovative tools for cross-border cooperation, specifically for the disclosure and expedited production of subscriber information (Articles 7-8) and for expedited disclosure of stored computer data in an emergency (Article 9).

The Budapest Convention lacks a provision on asset confiscation, which the drafters of the UN Convention instead modeled on UNTOC and UNCAC.

Like the UN Convention, the Budapest Convention allows parties to impose confidentiality requirements on persons who carry out orders, such as those for expedited preservation of stored data, including traffic data (Article 16(3)).

Critics' Concerns

Critics deemed the availability of the UN Convention's procedural powers for any crime committed by means of an ICTS (Article 23) to be too broad, urging that they be limited to the offenses

[46] Budapest Convention, Article 15(1), https://rm.coe.int/1680081561.
[47] Conventions on Cybercrime: The Budapest Convention and the Draft UN Treaty, Briefing Note, Council of Europe (August 27, 2024), https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a.
[48] Second Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224), Convention on Cybercrime, Council of Europe, https://www.coe.int/en/web/cybercrime/second-additional-protocol.

specifically criminalized by the UN Convention[49] – notwithstanding the similar scope of the Budapest Convention. They fear that the lack of definition regarding such other offenses could enable use of the UN Convention's procedural measures for human rights abuse, such as online censorship or preventive content take-downs.

The Article 24 safeguards also were viewed as inadequate by numerous entities. The Office of the UN High Commissioner for Human Rights opined that "article 24 fails to establish a robust binding regime of human rights-based guardrails by merely listing a range of possible conditions and safeguards but leaving it to the discretion of the State Parties when and how to apply these."[50] Other critics similarly assert that implementation of the Article 24 safeguards are left open to a State Party's interpretation, likely resulting in little to no practical effect in certain countries.[51] Commentators from business pointed out that that the human rights safeguards, while drawn from the Budapest Convention, have been "significantly weakened" with the UN Convention's inclusion of the phrase "under its domestic law" and with the general reference to "obligations under international human rights law" [52] while failing to refer to specific international instruments or to include language requiring that each party's domestic law ensures "adequate protection of human rights and liberties,"[53] both of which the Budapest Convention does.

---

[49] Microsoft Submission to the Seventh Reconvened Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (August 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Microsoft_-_Reconvened_Substantive_Session.pdf.

[50] Submission of the Office of the United Nations High Commissioner for Human Rights, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (July 22, 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/OHRC_AHC_Cybercrime_-_reconvened_concluding_session.pdf.

[51] Andrew Adams & Daniel Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention," *Lawfare* (December 9, 2024), https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention; Industry Perspectives Ahead of the Reconvened Concluding Session of the UN Ad Hoc Committee on Cybercrime, International Chamber of Commerce (June 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/ICC_industry_perspectives_AHC_reconvened_concluding_session.pdf; *see* Arun Sukumar & Arindrajit Basu, "Back to the Territorial State: China and Russia's Use of UN Cybercrime Negotiations to Challenge the Liberal Cyber Order," *Journal of Cyber Policy,* Volume 9, Issue 2 (December 13, 2024), https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2436591?src=recsys#abstract.

[52] Microsoft Submission to the Seventh Reconvened Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (August 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Microsoft_-_Reconvened_Substantive_Session.pdf; *see* International Chamber of Commerce Industry Perspective Ahead of the Reconvened Concluding Session of the UN Ad Hoc Committee on Cybercrime (June 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/ICC_industry_perspectives_AHC_reconvened_concluding_session.pdf.

[53] Budapest Convention, Article 15, https://rm.coe.int/1680081561.

Numerous civil society organizations asserted that the UN Convention should have included a mandatory requirement to notify an individual affected by use of the procedural powers (Article 24).[54]

Similarly, critics objected to the requirement that service providers receiving a request for expedited preservation of stored electronic data (Article 25) keep the matter confidential pursuant to domestic law, viewing it as mandating indefinite secret cooperation between private sector entities and states.[55] Confidentiality of evidence is a routine element of investigative proceedings that have yet to proceed to trial, however.

The power to conduct searches and seizures of "any person who has knowledge" about the functioning of an ICTS system (Article 28(4)) also drew fire. One company complained that this provision could compel its ICT professionals travelling abroad to hand over proprietary information exposing critical infrastructure to cyberattack.[56]

A coalition of technology companies similarly explained how an unsuspecting third country could receive a request related to an invented criminal defense as a pretext for demanding access to a travelling security contractor's official laptop under Article 28(4). The coalition also sketched out how a travelling government official unsuspectingly could be subjected to real-time collection of traffic or content data (Articles 29-30) on the basis of an invented and malicious request for assistance.[57]

UN Convention Chapter V – International Cooperation

The UN Convention establishes a broad scope for international cooperation. It extends not only to the investigation and prosecution of criminalized offenses, but also to collecting, preserving and

---

[54] "Civil Society Sends Joint Letter Urging EU and Member States to Withdraw Support From Rights-harming UN Cybercrime Convention," CyberPeace Institute (October 22, 2024), https://cyberpeaceinstitute.org/news/civil-society-joint-letter-un-cybercrime-convention/#:~:text=We%2C%20the%20undersigned%20organisations%20and%20individual%20experts%2C%20urge,comes%20to%20a%20vote%20at%20the%20General%20Assembly.

[55] "GNI calls on Member States not to support the UN Cybercrime Convention," Global Network Initiative (October 7, 2024), https://globalnetworkinitiative.org/gni-statement-on-uncc/.

[56] Microsoft Submission to the Seventh Reconvened Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (August 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Microsoft_-_Reconvened_Substantive_Session.pdf; *see also* Industry Perspectives Ahead of the Reconvened Concluding Session of the UN Ad Hoc Committee on Cybercrime, International Chamber of Commerce (June 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/ICC_industry_perspectives_AHC_reconvened_concluding_session.pdf.

[57] Cybersecurity Tech Accord Submission to the Resumed Concluding Session of the Ad Hoc Committee to Elaborate a UN Convention on Countering Cybercrime (July 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Cybersecurity_Tech_Accord_-_7th_AHC_ https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdfresumed_session_submission_E.pdf.

sharing of electronic evidence of any serious crime, as well as to ancillary proceedings for asset freezing and confiscation (Article 35).

A relatively summary article of the UN Convention (Article 36) governs transferred personal data. Transfers are subject to the transferring State Party's domestic data protection laws or to specific conditions; requested transfers that do not comply with domestic data protection laws may be refused (Article 36(1a)). Onward transfers to a third country are equally protected (Article 36(3)). The European Union and the United States collaborated to arrive at the text of this article, a welcome contrast to their bilateral struggles in recent years over data protection for transferred personal data.

Lengthy provisions of the UN Convention govern extradition (Article 37) and mutual legal assistance (Article 40). A person may be extradited for cybercrime offenses criminalized by the instrument (Article 37(1)). The UN Convention thus operates to supplement the offenses defined in a separate extradition treaty between States Parties. In the absence of a bilateral treaty, the UN Convention may serve as a free-standing basis under international law for extradition for such offenses. Article 37 therefore replicates the many safeguards found in bilateral extradition treaties, such as the right to refuse an extradition request if there are substantial grounds for believing that it has been made for purposes of prosecuting or punishing a person on account of sex, race, religion, or political opinions (Article 37(15)).

A wider scope of cooperation is envisaged for the collection of evidence at the request of a foreign state than it is for extradition, which – because it relates to transfer of persons -- historically has been considered more sensitive from a state sovereignty perspective. Mutual legal assistance (Article 40(1)) is available for electronic evidence of serious crimes generally as well as for electronic evidence of criminalized offenses. A State Party also may transmit information to another State Party spontaneously if it could assist in another state's criminal proceedings (Article 40(4)).

As with extradition, the mutual legal assistance provisions of the UN Convention supplement those of bilateral mutual legal assistance treaties (MLATs) or, in the absence of a bilateral MLAT, afford a separate international legal basis (Article 40(7)). Article 40 includes not only the grounds for refusal found in most bilateral MLATs, such as violation of *ordre public* or other essential interests (Article 40(21)), but also the same non-discrimination protection (Article 40(22)) as is prescribed for extradition. The UN Convention is the first treaty governing mutual legal assistance to provide non-discrimination protection; many Western participants stated during the negotiations that they consider this safeguard to be an important innovation, as observed by an author of this article.

In addition to prescribing traditional forms of mutual legal assistance, this chapter also elaborates newer methods tailored to the fast-moving internet environment. These include: establishment of a point of contact in each State Party available on a twenty-four hour basis seven days a week (Article 41): provisions enabling international cooperation specifically for the purpose of expedited preservation of stored electronic data (Article 42); expedited disclosure of preserved traffic data (Article 43); access to stored electronic data (Article 44); real-time collection of traffic data (Article 45); and interception of content data (Article 46). Other articles allow joint investigative teams (Article 47), a relatively recent technique, and cooperation in relation to confiscation (Articles 50-52).

Relevant Budapest Convention Provisions

The COE analysis describes the scope of international cooperation under the UN Convention as "both broader and narrower" than that of the Budapest Convention. The UN Convention is narrower in that it limits cooperation to serious crimes, whereas the Budapest Convention permits it for any criminal offense (Article 23). On the other hand, the UN Convention is broader because of its reach to cooperation in asset freezing and confiscation, a topic on which the Budapest Convention is silent.

The Budapest Convention lacks a counterpart to Article 36 of the UN Convention on data protection, although it does contain an article permitting use limitations in certain circumstances (Article 28). Data protection law in Europe was much less robust at the time the Budapest Convention was negotiated; the EU did not adopt the General Data Protection Regulation, for example, until 2016. A provision in the Second Additional Protocol (Article 14) to the Budapest Convention addressing data protection measures in detail will largely fill this gap.[58] The EU and the United States negotiated Article 14 of the Second Additional Protocol at great length, an experience that eased their subsequent collaboration on the much briefer counterpart in the UN Convention.

The Budapest Convention's general provisions on extradition and mutual legal assistance (Articles 24-25) are broadly similar to those in the UN Convention, though less precise; the latter's greater detail was largely derived from UNTOC and UNCAC. This is due to the fact that many countries in

[58] It is important to point out that, although Article 14 of the Second Additional Protocol to the Budapest Convention is welcomed by many, the provision also has numerous detractors who do not believe sufficient protections are in place for the personal data at issue. Article 14 permits several approaches for protecting the personal data that is being transferred. One of these approaches requires the country receiving the data to provide the types of protections common in comprehensive data protection laws, including use limitations, safeguards for sensitive data, and restrictions on automated decisions. Budapest Convention, Second Additional Protocol, Article 14, Section 1.a, https://rm.coe.int/1680a49dab; *see* Article 14, Sections 2-15. Article 14 also recognizes a second approach to data protection that is found in a framework put in place by an agreement to which both the requesting country and the receiving country are bound – such as Convention 108+, the EU-U.S. Umbrella Agreement, and likely Executive Agreements under the U.S. Cloud Act. Budapest Convention, Second Additional Protocol, Article 14, Section 1.b; *see* DeBrae Kennedy-Mayo & Peter Swire, "Update to Budapest Convention Expected to be Finalized This November," Cross-Border Data Forum (October 11, 2021), https://www.crossborderdataforum.org/update-to-budapest-convention-expected-to-be-finalized-this-november/#_ednref41. According to Article 14, transfers of personal data under either of these two approaches are deemed to meet each Party's requirements for international transfer and "no further authorization for transfer shall be required under that legal framework." Budapest Convention, Second Additional Protocol, Article 14, Section 1.d, https://rm.coe.int/1680a49dab. When transfers occur in accordance with protections commonly found in comprehensive data protection laws, few question that the transfers would be deemed to meet each Party's requirements for international transfer. The more controversial instance is where these transfers are deemed compliant is when they occur with respect to the second approach. *See* Katitza Rodriquez, "EFF to Council of Europe: Cross Border Surveillance Treaty Must Have Ironclad Safeguards to Protect Individual Rights and Users' Data," EFF (September 8, 2021), https://www.eff.org/deeplinks/2021/09/eff-council-europe-cross-border-police-surveillance-treaty-must-have-ironclad; Privacy & Human Rights in Cross-Border Law Enforcement, Joint Civil Society Comment to the Parliamentary Assembly of the Council of Europe (PACE) on the Second Additional Protocol to the Cybercrime Convention (CETS 185), Version 2 (August 9, 2021), https://www.eff.org/files/2021/08/17/20210816-2ndaddprotocol-pace-ver2-final.pdf.

the Global South lack the extensive networks of bilateral extradition and mutual legal assistance treaties found in more developed countries.

The articles of the UN Convention on methods of mutual assistance specific to computer systems and data (Articles 41-46) "reproduce" corresponding articles of the Budapest Convention, according to the COE analysis.[59]

Critics' Concerns

Some critics take aim at the availability of mutual legal assistance under the UN Convention for serious crime generally as well as criminalized offenses (Article 40), believing that only the latter should be within scope.[60] One civil society organization described the international cooperation provisions as a "blank check for surveillance abuses", fearing that authoritarian states could use them to harass and pursue prosecution of dissidents residing abroad, particularly in smaller, weaker or less sophisticated states.[61]

Others expressed dissatisfaction with the relative brevity of the data protection provision (Article 36), preferring the greater precision of the GDPR.[62]

Grounds for refusing mutual assistance (Article 40) encountered concentrated attack from U.S. critics. They noted that some U.S. MLATs with authoritarian states, e.g. China, contain greater latitude for rejecting requests than the UN Convention does, for example by inserting a dual criminality requirement and a political offense exception. They predict that the UN Convention "will undoubtedly complicate the Justice Department's ability to push back on bad-faith requests under existing MLATs."[63]

The provision for spontaneous transmission of information (Article 40(4)) also elicited unease as a potential avenue for states to conspire in suppressing human rights.[64]

---

[59] Conventions on Cybercrime: The Budapest Convention and the Draft UN Treaty, Briefing Note, Council of Europe (August 27, 2024), https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a.

[60] Microsoft Submission to the Seventh Reconvened Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (August 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Microsoft_-_Reconvened_Substantive_Session.pdf.

[61] Kate Graham-Shaw, "New UN Cybercrime Treaty Could Threaten Human Rights," *Scientific American* (August 9, 2024), https://www.scientificamerican.com/article/0724--un-cybercrime/.

[62] "Civil Society Sends Joint Letter Urging EU and Member States to Withdraw Support From Rights-harming UN Cybercrime Convention," CyberPeace Institute (October 22, 2024), https://cyberpeaceinstitute.org/news/civil-society-joint-letter-un-cybercrime-convention/#:~:text=We%2C%20the%20undersigned%20organisations%20and%20individual%20experts%2C%20urge,comes%20to%20a%20vote%20at%20the%20General%20Assembly.

[63] Andrew Adams & Daniel Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention," *Lawfare* (December 9, 2024), https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention.

[64] "Civil Society Sends Joint Letter Urging EU and Member States to Withdraw Support From Rights-harming UN Cybercrime Convention," CyberPeace Institute (October 22, 2024),

UN Convention Chapter IX --Final Provisions

The UN Convention may be supplemented in the future by one or more protocols (Article 61). States that are party to the UN Convention may choose whether or not to join a protocol. Allowing for optional protocols to take account of future developments is a common feature of multilateral crime conventions, including the Budapest Convention.

However, the negotiators of the UN Convention took an unusual further step: they struck a compromise under which the UN Convention itself would enter into force, but further negotiation on a protocol is expressly envisaged. The UNGA resolution adopting the UN Convention calls for negotiators to hold two sessions of talks on a protocol before the end of 2027.[65] The Conference of the States Parties to the UN Convention would consider the results, with a two-thirds majority of States Parties required for adoption of the protocol if consensus on it cannot be reached.

The decision to link advancement of the Convention to subsequent protocol negotiations had its seeds in Russia's role as its initial advocate. When Russia first put forward a draft text for the Convention, it called for criminalizing a wide-ranging set of conduct including "incitement to subversive activity," and "terrorism" and "extremism" facilitated by means of ICTS.[66] Many countries found these proposals vague and ominous, and suspected an agenda to control information. Russia and a number of other authoritarian states stuck to them, nonetheless, through much of the negotiation. The Chair eventually decided to exclude these Russian proposals from the text, but in return negotiators agreed to revert to them later.

Critics' Concerns

Many critics objected to the deal envisaging future consideration of additional criminalization measures, on grounds that it has the potential to further broaden the already wide scope of the UN Convention in uncertain ways, and potentially to threaten online freedoms.[67]

Conclusions

The UN Convention has the potential to significantly aid countries – particularly in the Global South – in combatting crimes committed through use of ICTS. All states joining the UN Convention must

---

https://cyberpeaceinstitute.org/news/civil-society-joint-letter-un-cybercrime-convention/#:~:text=We%2C%20the%20undersigned%20organisations%20and%20individual%20experts%2C%20urge,comes%20to%20a%20vote%20at%20the%20General%20Assembly.

[65] UN General Assembly Resolution 79/43, paragraph 5 (December 24, 2024), https://digitallibrary.un.org/record/4071955?v=pdf.

[66] Letter of the Russian Federation to the United Nations Secretary-General (July 30, 2021), https://digitallibrary.un.org/record/3942230?ln=en&v=pdf.

[67] *See, e.g.,* Microsoft Submission to the Seventh Reconvened Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (August 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Microsoft_-_Reconvened_Substantive_Session.pdf*; see also* Cybersecurity Tech Accord Submission to the Resumed Concluding Session of the Ad Hoc Committee to Elaborate a UN Convention on Countering Cybercrime (July 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Cybersecurity_Tech_Accord_-_7th_AHC_resumed_session_submission_E.pdf.

incorporate the agreed array of cyber offenses into their criminal codes. In addition, they must equip their criminal investigators and prosecutors with a common arsenal of procedural powers. They also must stand ready to assist other parties' cybercrime investigations that have a transnational element, through extradition, mutual legal assistance, and asset freezing and confiscation. Numerous countries in the Global South currently lack these measures in their domestic laws, so the UN Convention would serve to stimulate the necessary legislation.

A series of safeguards cabin these powerful new tools. The principal ones are found in Article 6 (respect for human rights), Article 21(4) (due process guarantees), Article 24(4) (procedural powers safeguards), Article 36 (personal data protection), and Article 40(22) (non-discrimination in mutual legal assistance.) These protections as a whole go beyond earlier UN crime conventions such as UNTOC and UNCAC.[68] Many governments view these protections as comparable to – if not exceeding – those in the Budapest Convention.[69]

The COE's analysis commends the UN Convention as a "major *political* achievement given the current international context" (emphasis added).[70] The COE observes that the "core concepts and measures" of the UN Convention are drawn from the Budapest Convention, as well as from UNTOC and UNCAC.[71] In sum, the COE concludes, the "UN treaty represents a narrow criminal justice treaty that is largely consistent with the Budapest Convention and that contains minimum safeguards necessary for international cooperation."[72]

Why then has the UN Convention excited such impassioned opposition? Many observers have distrusted the global initiative from the very beginning, due to Russia's role as protagonist and its persistent efforts to criminalize vague conduct relating to extremism and terrorism. Many critics are not persuaded by the battery of safeguards that negotiators managed to incorporate into the instrument. One U.S. critique dismissed their value as "difficult to reconcile with the intent of the Draft Convention's staunchest proponents or with the domestic and transnational repression practiced by those states."[73]

A second reason for persisting unease is the prospect of a protocol negotiation at which Russia is very likely to re-introduce its problematic criminalization proposals. The COE delicately observes that this occasion "provides some States with a further opportunity to promote information

---

[68] Conventions on Cybercrime: The Budapest Convention and the Draft UN Treaty, Briefing Note, Council of Europe (August 27, 2024), https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a.

[69] *See* "UN Approves its First Treaty Targeting Cybercrime," The Strait Times (August 9, 2024), https://www.straitstimes.com/world/un-approves-its-first-treaty-targeting-cybercrime; Anja Jakobi & Lena Herbst, "Between a Rock and a Hard Place: The UN Cybercrime Convention," PRIF Blog (December 9, 2024), https://blog.prif.org/2024/12/09/between-a-rock-and-a-hard-place-the-un-cybercrime-convention/.

[70] Conventions on Cybercrime: The Budapest Convention and the Draft UN Treaty, Briefing Note, Council of Europe (August 27, 2024), https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a.

[71] *Id*.

[72] *Id*.

[73] Andrew Adams & Daniel Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention," *Lawfare* (December 9, 2024), https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention.

control."[74] Although Russia and its allies are unlikely to muster sufficient global support for these proposals in a protocol negotiation, Western powers including the United States and Europe must engage forcefully to ensure that the Convention is not supplemented in ways that could damage free expression.

Beyond Russia-related concerns lies a structural reason for the level of public controversy that the UN Convention negotiations have caused. Historically, national law enforcement authorities, bolstered by their diplomatic representatives, have dominated UN crime convention negotiations, which took place largely out of the public eye; UNTOC and UNCAC exemplified this approach. There were only limited UN institutional arrangements in place at the time for the human rights community and companies to inject their concerns directly into negotiations.

The Ad Hoc Committee responsible for negotiating the UN Convention, by contrast, allowed accredited outside observers an unprecedented degree of transparency into the negotiation. For example, observers' position papers were circulated through the UN document system, their representatives roamed the halls buttonholing national delegations, and they were given discrete opportunities to formally address negotiating sessions as well.

In addition, during the two decades since the earlier UN crime conventions were negotiated, human rights organizations have grown in strength, and some now maintain a permanent presence in Vienna, home of UNODC. Moreover, companies that transfer data across borders, such as cloud service providers, have expanded the reach of their international public policy operations to track multilateral crime negotiations.

The maturing of human rights and corporate advocacy left its mark on the UN Convention negotiating process, as negotiators from national law enforcement agencies were continually confronted with civil society and corporate concerns. Indeed, the arguments by these two sets of stakeholders dovetailed to a remarkable extent, as their representatives periodically reminded governments.[75] Governments responded, to an extent, by expanding safeguards provisions and acknowledging the legitimate role of cybersecurity researchers, for example.

Critics, however, remain largely unmoved by the result. Many continue to regard the UN Convention as a dangerous expansion from the Budapest Convention, despite their substantial degree of parallelism. Commentators suggest that the provisions concerning human rights protections are unlikely to significantly increase protections against the practices of non-democratic countries such as China and Russia.[76] Various commenters consider that the Budapest Convention can be

---

[74] Conventions on Cybercrime: The Budapest Convention and the Draft UN Treaty, Briefing Note, Council of Europe (August 27, 2024), https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a.

[75] Statement by Cybersecurity Tech Accord Statement to Reconvened Concluding Session of the Ad Hoc Committee (July 30, 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Cybersecurity_Tech_Accord_Statement_07.30_AHC7.13.pdf.

[76] Andrew Adams & Daniel Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention," *Lawfare* (December 9, 2024), https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention; "GNI calls on Member States not to support the UN Cybercrime Convention," Global Network

more demanding when it comes to adherence to human rights standards.[77] Moreover, the Budapest Convention is trusted because it is a known commodity, with a body of interpretation that has developed over twenty years, and dedicated oversight through the COE secretariat and the committee representing parties. The fact that many, though not all, parties to the Budapest Convention are democratic governments also contributes significantly to that Convention's credibility among civil society and companies -- something that a universal convention at the UN level will never achieve.

Civil society and tech company advocates now are urging governments not to sign the UN Convention.[78] The Biden Administration issued a temporizing statement before joining consensus final passage at UNGA[79]. The Trump Administration – distrustful of multilateralism and attuned to tech industry concerns and to risks to free expression – may well be skeptical. The European Data Protection Board has expressed caution, though European governments appear to be more favorable.[80] The European Parliament's Civil Liberties Committee (LIBE) has held meetings at which doubts have been expressed whether the EU and its member states should sign.[81]

A decision by the United States or leading European countries not to sign the UN Convention would substantially weaken the instrument's effectiveness, since most repositories of data sought by foreign governments are currently stored in their territories. "Without US participation and access to its vast pool of data, the treaty's operational value will be close to zero," concludes one

---

Initiative (October 7, 2024), https://globalnetworkinitiative.org/gni-statement-on-uncc/; *see* Tatiana Tropina, "'This is Not a Human Rights Convention!': The Perils of Overlooking Human Rights in the UN Cybercrime Convention," *Journal of Cyber Policy,* Volume 9, Issue 2 (October 29, 2024), https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2419517#abstract.

[77] Microsoft Submission to the Seventh Reconvened Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (August 2024), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Microsoft_-_Reconvened_Substantive_Session.pdf; "GNI calls on Member States not to support the UN Cybercrime Convention," Global Network Initiative (October 7, 2024), https://globalnetworkinitiative.org/gni-statement-on-uncc/; Kate Graham-Shaw, "New U.N. Cybercrime Treaty Could Threaten Human Rights," *Scientific American* (August 9, 2024), https://www.scientificamerican.com/article/0724--un-cybercrime/.

[78] *See, e.g.* Katitza Rodriquez, "Still Flawed and Lacking Safeguards, UN Cybercrime Treaty Goes Before the UN General Assembly, then States for Adoption," Electronic Frontier Foundation (December 16, 2024), https://www.eff.org/deeplinks/2024/12/still-flawed-and-lacking-safeguards-un-cybercrime-treaty-goes-un-general-assembly; "GNI calls on Member States not to support the UN Cybercrime Convention," Global Network Initiative (October 7, 2024), https://globalnetworkinitiative.org/gni-statement-on-uncc/

[79] Explanation of Position of the United States on the Adoption of the Resolution on the UN Convention Against Cybercrime in UNGA's Third Committee, United States Mission to the United Nations (November 11, 2024), https://usun.usmission.gov/explanation-of-position-of-the-united-states-on-the-adoption-of-the-resolution-on-the-un-convention-against-cybercrime-in-ungas-third-committee/.

[80] EDPB Reply to the open letter to the EDPB on the United Nations Convention against Cybercrime | European Data Protection Board, EDPB (December 17, 2024), https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-reply-open-letter-edpb-united-nations-convention-against_en.

[81] As reported by *Politico* in the CyberInsights newsletter, February 11, 2025.

organization focused on combatting transnational crime.[82] Such an outcome unquestionably would be a bitter defeat for law enforcement's efforts to combat the latest forms of criminality. As Viet Nam prepares its grand signing conference, the eventual practical value of the UN Convention remains in doubt.

[82] "UN cybercrime Treaty Faces Uncertain Future Under Trump", Global Initiative against Transnational Organized Crime (November 27, 2024), https://www.scoop.it/topic/fatf/p/4162595905/2024/11/27/un-cybercrime-treaty-faces-uncertain-future-under-trump.