PERSPECTIVE

Multilateralismus auf dem Prüfstand

Umsetzung der UN-Konvention gegen Cyberkriminalität nach Hanoi

Pavlina Pavlova, Christina Rupp, Sven Herpig

December 18, 2025

Table of Contents

Veröffentlicht von Pavlina Pavlova, Christina Rupp, und Sven Herpig in der Zeitschrift für die Vereinten Nationen und ihre Sonderorganisationen unter dem Titel "Die Bekämpfung von Cyberkriminalität".

Das Übereinkommen der Vereinten Nationen gegen Cyberkriminalität gilt als politischer Meilenstein. Es soll globale Ansätze zur Bekämpfung von Cyberkriminalität harmonisieren, birgt jedoch Risiken für Menschenrechte und Cybersicherheitsforschung.

English Abstract: In October 2025, the United Nations Convention against Cybercrime opened for signature following its 2024 adoption by the UN General Assembly. The treaty represents a major political milestone, yet exposes deep geopolitical divides between advocates of state-centered and multistakeholder governance. While it could harmonize global efforts to combat cybercrime, critics warn that its broad procedural powers and weak human rights safeguards may enable abuse. Its implementation now depends on signatories ensuring effective, rights-respecting implementation.

Im Dezember 2024 verabschiedete die UN-Generalversammlung das Übereinkommen der Vereinten Nationen gegen Cyberkriminalität. Vorausgegangen waren weniger als drei Jahre intensiver Verhandlungen des Ad-hoc-Ausschusses, der mit der Ausarbeitung des Vertrags beauftragt war.[1] Die Einigung über das Übereinkommen war ein großer politischer Erfolg und wurde als Zeichen dafür gewertet, dass Multilateralismus trotz aller Skepsis erfolgreich sein kann. Die unterschiedlichen Standpunkte während der Verhandlungen haben jedoch gezeigt, dass es tiefergehende geopolitische Differenzen zwischen den Mitgliedstaaten gibt, die einen staatszentrierten Multilateralismus befürworten, und denen, die eine Multi-Akteurs-Governance unterstützen. Diese Dichotomie kann sich nachteilig auf die Zielsetzung, die künftige Effizienz und die internationalen Bemühungen zur Bekämpfung der Cyberkriminalität im Rahmen des ersten rechtlich bindenden globalen Vertrags zu diesem Thema auswirken.

Was ist Cyberkriminalität?

Cyberkriminelle Aktivitäten stellen weltweit eine der größten Bedrohungen für Wirtschaft und Gesellschaft dar, insbesondere in Ländern, die stark von internetbasierten Infrastrukturen abhängig sind. Es gibt keine international einheitliche Definition für Cyberkriminalität. Daher handelt es sich um einen inhärent politischen Begriff, der je nachdem, welche Handlungen mit welcher

1 UN-Dok. A/RES/79/243 v. 24.12.2024.

Absicht und in welchem Kontext unter Strafe gestellt werden, unterschiedlich verwendet wird. Der Tatbestand solcher Straftaten wird durch die Rechtsvorschriften definiert, in denen sie kodifiziert sind.

Konzeptionell ist es sinnvoll, zwischen zwei Kategorien von Cyberkriminalität zu unterscheiden: Cyberkriminalität im engeren Sinne (CCieS) und Cyberkriminalität im weiteren Sinne (CCiwS). CCieS sind cyberabhängige Delikte, die sich auf »Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen« beziehen, während CCiwS cybergestützte Straftaten sind, die zusätzlich »computer- und inhaltsbezogene Straftaten sowie Straftaten im Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte« umfassen.[2]

In der Praxis bedeutet dies, dass CCieS sich auf Aktivitäten bezieht, die direkt auf IT-Systeme und -Infrastrukturen abzielen – wie beispielsweise die Verbreitung von Erpressungssoftware (Ransomware) in Unternehmensnetzwerken. CCiwS dagegen beinhaltet alle Straftaten, bei denen IT-Systeme und -Infrastrukturen genutzt werden, wie beispielsweise bei der Verbreitung von Inhalten über den sexuellen Missbrauch von Kindern oder der Veröffentlichung von Hassreden in sozialen Medien.

Cyberkriminalität als nationales Sicherheitsproblem

Cyberkriminelle Aktivitäten können erhebliche finanzielle Schäden verursachen – Schätzungen zufolge werden sich diese im Jahr 2025 weltweit auf fast neun Billionen Euro belaufen.[3] Darüber hinaus kann Cyberkriminalität auch emotionale Schäden, Selbstverletzungen und andere Formen psychischer Belastungen zur Folge haben. In Fällen wie koordinierten Hassreden oder gezielten Angriffen mit Erpressungssoftware kann Cyberkriminalität auch zu einer weitreichenden Destabilisierung der Gesellschaft führen. Damit stellen solche illegalen Aktivitäten eine komplexe und schwer quantifizierbare Bedrohung für die nationale Sicherheit dar.[4]

Die Akteure hinter der Cyberkriminalität spielen eine ganz unterschiedliche Rolle: Die an CCieS beteiligten Bedrohungsakteure sind sowohl Einzelpersonen[5] als auch

2 Diese Unterscheidung beruht auf dem Budapester Übereinkommen, Europarat, Übereinkommen über Computerkriminalität, 23.11.2001, rm.coe.int/168008157a.
3 Ani Petrosyan, Cybercrime Worldwide – Statistics & Facts, Statista, 30.5.2025, www.statista.com/topics/13546/cybercrime-worldwide/.
4 Max Smeets, Ransom War. How Cyber Crime Became a Threat to National Security, London 2025.

informelle Gruppen,[6] organisierte kriminelle Netzwerke[7] und sogar staatlich gesteuerte Gruppierungen.[8] Regierungen können diese Aktivitäten nicht nur durch offizielle Maßnahmen fördern, sondern auch durch die Bereitstellung sicherer Zufluchtsorte für illegale Aktivitäten[9] oder indem sie ihren Bediensteten erlauben, ihr Wissen und ihre Arbeitsmittel für kriminelle Aktivitäten außerhalb ihres Regierungsjobs einzusetzen.[10] Die Akteure im Bereich CCiwS sind vielfältiger und reichen von übergriffigen Ehepartnern[11] über extremistische Gruppierungen[12] und Drogenkartelle[13] bis hin zu staatlich unterstützten Bedrohungsakteuren.

Zu den wichtigsten Bedenken der Mitgliedstaaten der Europäischen Union (EU) zählen die erheblichen Auswirkungen der Cyberkriminalität auf kritische Infrastrukturen wie Krankenhäuser, Kraftwerke oder Flughäfen sowie auf den öffentlichen Sektor.

Die Bekämpfung von CCieS erfordert sowohl einen internationalen als auch einen nationalen Ansatz. Bei letzterem liegt der Schwerpunkt auf verbesserten Basis-Schutzmaßnahmen, wie Schwachstellen-Management und zuverlässlige Backup-Prozesse. Diese Cybersicherheitsmaßnahmen können die Resilienz nationaler IT-Systeme und kritischer Infrastrukturen verbessern und so die Auswirkungen von Cyberkriminalität erheblich reduzieren. Darüber hinaus ist die Zerschlagung krimineller Infrastrukturen[14] und die strafrechtliche Verfolgung von Straftätern[15] äußerst wichtig und erfordert vor allem internationale Zusammenarbeit. Bei der Bekämpfung von Cyberkriminalität ist die multilaterale Koordination von entscheidender Bedeutung.

Die Zusammenarbeit mit globalen Social-Media-Unternehmen, der

5 Esteban Borges, Cybercriminals: Tactics, Impacts, and Defense Strategies, Recorded Future, 5.2.2024, www.recordedfuture.com/threat-intelligence-101/threat-actors/cybercriminals.

6 Sam Sabin, How Scattered Spider Hackers are Wreaking Havoc on Corporate America, Axios, 8.7.2025, www.axios.com/2025/07/08/scattered-spider-cybercrime-hackers.

7 United Nations Office on Drugs and Crime (UNODC), Criminal Groups Engaging in Cyber Organized Crime, sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html.

8 Federal Bureau of Investigation (FBI), North Korea Responsible for $1.5 Billion Bybit Hack, 26.2.2025, www.ic3.gov/psa/2025/psa250226.

9 Max Zuber, Explaining Organizational Instability in Russian Ransomware Gangs, The Henry M. Jackson School of International Studies, 16.10.2023, jsis.washington.edu/news/explaining-organizational-instability-in-russian-ransomware-gangs/.

10 Joseph Menn/Jack Stubbs/Christopher Bing, Chinese Government Hackers Suspected of Moonlighting for Profit, Reuters, 7.8.2019, www.reuters.com/article/business/chinese-government-hackers-suspected-of-moonlighting-for-profit-idUSKCN1UX1JN/.

11 Coalition Against Stalkerware, stopstalkerware.org.

12 International Centre for Counter-Terrorism (ICCT), Testimonies of Victims of Russian (Extremist) Doxing, 13.3.2025, icct.nl/publication/testimonies-victims-russian-extremist-doxing.

13 Raphael Satter, Sinaloa Cartel Used Phone Data and Surveillance Cameras to Find FBI Informants, DOJ Says, Reuters, 27.6.2025, www.reuters.com/world/americas/sinaloa-cartel-hacked-phones-surveillance-cameras-find-fbi-informants-doj-says-2025-06-27/.

14 Sven Herpig/Anushka Shah, Active Cyber Defense Operations: Case Studies Cheat Sheets, interface, 10.7.2024, www.interface-eu.org/publications/active-cyber-defense-operations-case-studies-cheat-sheets.

15 U.S. Attorney's Office, Central District of California, Russian National and Leader of Qakbot Malware Conspiracy Indicted in Long-Running Global Ransomware Scheme, 22.5.2025, www.justice.gov/usao-cdca/pr/russian-national-and-leader-qakbot-malware-conspiracy-indicted-long-running-global.

grenzüberschreitende Austausch von Telekommunikationsdaten oder anderen relevanten Daten sowie die Beachtung internationaler Rechtsvorschriften sind unerlässlich. Aufgrund des transnationalen Charakters der Cyberkriminalität gewinnen die Vereinten Nationen als Forum für die Bewältigung der aktuellen Herausforderungen zunehmend an Bedeutung.

Die Motivation der Staaten

Das UN-Übereinkommen wird andere multilaterale Instrumente ergänzen, insbesondere das Übereinkommen des Europarats über Cyberkriminalität – das sogenannte Budapester Übereinkommen –, das im Jahr 2004 in Kraft getreten ist, sowie andere Instrumente, die Straftaten ahnden, die unter Verwendung von Informations- und Kommunikationstechnologiesystemen (IKT-Systemen) begangen wurden.[16] Bis heute ist das Budapester Übereinkommen mit 81 Vertragsstaaten, von denen die meisten während der UN-Verhandlungen über Cyberkriminalität beigetreten sind,[17] das am weitesten verbreitete und am häufigsten ratifizierte Übereinkommen. Dieses Rahmenabkommen des Europarats wurde inzwischen weltweit ratifiziert, insbesondere Russland und China sprachen sich jedoch gegen das Dokument aus. Kritiker behaupteten, die Bestimmungen des Budapester Übereinkommens würden die staatliche Souveränität verletzen und enthielten Vorgaben, die eine universelle Gültigkeit verhindern würden. Außerdem könne ein globales Übereinkommen nur unter UN-Schirmherrschaft ausgearbeitet werden.[18]

Im Jahr 2019 brachte Russland in der Generalversammlung eine Resolution zur Einrichtung des Ad-hoc-Ausschusses ein, die mit 79 Ja-Stimmen, 60 Nein-Stimmen und 33 Enthaltungen angenommen wurde. Damit wurden die Vertragsverhandlungen eingeleitet, die zwischen Februar 2022 und August 2024 stattfanden.[19]

Widerspruch gegen ein neues Übereinkommen zur Bekämpfung der Cyberkriminalität auf UN-Ebene kam in erster Linie von EU-Mitgliedstaaten, den USA und gleichgesinnten Ländern, die bereits dem Übereinkommen des Europarats beigetreten waren und das Budapester Übereinkommen für angemessen und

16 Other regional instruments include the African Union Convention on Cybersecurity and Data Protection 2014 (Malabo Convention), the League of Arab States' 2010 Convention on Combating Information Technology Offences, the 2013 EU Directive on Attacks Against Information Systems, frameworks of the Commonwealth of Independent States and the Shanghai Cooperation Organization, as well as various model laws and non-binding instruments.

17 Council of Europe, Parties/Observers to the Budapest Convention and Observer Organizations to the T-CY, www.coe.int/en/web/cybercrime/parties-observers.

18 Tatiana Tropina, This is not a Human Rights Convention!: The Perils of Overlooking Human Rights in the UN Cybercrime Treaty, Journal of Cyber Policy, 9. Jg., 2/2024, S. 200–220.

19 Joyce Hakmeh, The UN Convention on Cybercrime: A Milestone in Cybercrime Cooperation?, Journal of Cyber Policy, 9. Jg., 2/2024, S. 125.130 und UN-Dok. A/RES/74/247 v. 27.12.2019.

effizient hielten. Da sie jedoch das Interesse der UN-Mitgliedstaaten an einem Übereinkommen erkannten, dass die Ansätze in den verschiedenen Regionen vereinheitlichen würde,[20] beteiligten sich die Delegationen in gutem Glauben an dem Prozess. Sie befürchteten nämlich, dass die Verhandlung eines potenziellen UN-Übereinkommens ohne ihre Beteiligung möglicherweise weiter gefasste Bestimmungen und schwächere Maßnahmen zum Schutz der Menschenrechte enthalten könnte, die später weltweit gelten könnten.

Was die Staaten aushandelten

Das UN-Übereinkommen orientiert sich inhaltlich am Budapester Übereinkommen und an anderen UN-Abkommen, dem Übereinkommen der Vereinten Nationen gegen die grenzüberschreitende Organisierte Kriminalität (United Nations Convention against Transnational Organized Crime – UNTOC) und dem Übereinkommen der Vereinten Nationen gegen Korruption (United Nations Convention against Corruption – UNCAC). Der Text folgt einer dreigliedrigen Struktur miteinander verknüpfter Bestimmungen: Erstens legt er eine Reihe bestimmter Straftatbestände fest. Zweitens definiert das Übereinkommen verfahrensrechtliche Rahmenbedingungen für die Untersuchung strafbarer Handlungen. Und drittens wird ein Instrumentarium für die internationale Zusammenarbeit bei strafrechtlichen Ermittlungen geschaffen, das die gegenseitige Rechtshilfe beim grenzüberschreitenden Austausch von Beweismitteln erleichtert.[21]

Straftatbestände

Das Übereinkommen stellt in erster Linie cyberabhängige Straftaten unter Strafe, wie beispielsweise rechtswidrigen Zugang, rechtswidriges Abfangen, Eingriff in elektronische Daten, Missbrauch von Vorrichtungen, IKT-bezogenen Betrug und Fälschung (Art. 7–13). Das Kapitel zur Kriminalisierung erstreckt sich darüber hinaus auf ausgewählte cybergestützte Cyberstraftaten, ohne diejenigen auszuschließen, die nicht ausdrücklich erwähnt sind, wie zum Beispiel Straftaten mit Bezug zu Online-Material mit sexuellem Missbrauch oder sexueller Ausbeutung von Kindern (Art. 14), Kontaktanbahnung oder Kontaktaufnahme zum Zweck der Begehung einer Sexualstraftat an einem Kind (Art. 15) und die ohne Zustimmung erfolgende Verbreitung von Intimbildern (Art. 16).

20 Tropina, This is not a Human Rights Convention!, a.a.O. (Anm. 18).
21 Ebd.

Rechtsrahmen für die Ermittlung bei kriminellem Verhalten

Die Bestimmungen über die Gerichtsbarkeit für Straftaten (Art. 22) gewähren Staaten die Befugnis, die Gerichtsbarkeit für außerhalb ihrer Grenzen begangene Straftaten geltend zu machen, wenn ihre Staatsangehörigen betroffen sind. Die folgenden verfahrensrechtlichen Maßnahmen und Rechtsdurchsetzungsvorschriften (Art. 23–25) gewähren staatlichen Stellen weitreichende Befugnisse, wie beispielsweise den Zugriff auf elektronische Daten von Personen, die sich in ihrem Land befinden, unabhängig davon, wo die Daten gespeichert sind (Art. 27), die Erhebung von Verkehrsdaten in Echtzeit (Art. 29) oder das Abfangen von Inhaltsdaten (Art. 30). In Anlehnung an das UNTOC und das UNCAC enthält das UN-Übereinkommen Bestimmungen über das Einfrieren, die Beschlagnahme und Einziehung der Erträge aus Straftaten, einschließlich virtueller Vermögenswerte (Art. 31). Der Zeugenschutz (Art. 33) und die Hilfe und der Schutz für Opfer (Art. 34) sind zwar für die Durchsetzung von Gerechtigkeit und Wiedergutmachung sowie für die Berücksichtigung der Bedürfnisse von Personen in prekären Situationen wichtig, unterliegen jedoch ausschließlich dem innerstaatlichen Recht.

Mechanismen für die internationale Zusammenarbeit bei strafrechtlichen Ermittlungen

Die internationale Zusammenarbeit (Art. 35–52) erstreckt sich auf die Erhebung, Erlangung, Sicherung und den Austausch von Beweismitteln in elektronischer Form für jede schwere Straftat. Diese Ausweitung auf jede schwere Straftat, die in Artikel 2 lit. h als ein Verhalten definiert ist, das eine strafbare Handlung darstellt, die mit einer Freiheitsstrafe von mindestens vier Jahren im Höchstmaß oder einer schwereren Strafe bedroht ist, erweitert den potenziellen Anwendungsbereich des Instruments beträchtlich. Die Bedingungen für die Rechtshilfe (Art. 40) sind weit gefasst, ermöglichen es den Staaten jedoch, die Rechtshilfe unter Berufung auf das Fehlen beiderseitiger Strafbarkeit zu verweigern. Das Übereinkommen enthält begrenzte Garantien für den Schutz der Grundfreiheiten und personenbezogener Daten. So können Staaten beispielsweise die Zusammenarbeit verweigern, wenn es wesentliche Gründe für die Annahme gibt, dass ein Ersuchen gestellt worden ist, um eine Person wegen ihres Geschlechts, ihrer Sprache, ihrer Religion, ihrer Staatsangehörigkeit, ihrer ethnischen Herkunft oder ihrer politischen Anschauungen zu verfolgen (Art. 40 (22)).

Zusätzliche Elemente und Umsetzung

Im Gegensatz zum Budapester Übereinkommen enthält das UN-Instrument detaillierte Bestimmungen zu vorbeugenden Maßnahmen (Art. 53), technischer Hilfe und Kapazitätsaufbau (Art. 54), einschließlich Ausbildung und anderer Formen der Hilfe, des Austauschs von sachdienlichen Erfahrungen und Fachwissen und der Weitergabe von Technologie zu einvernehmlich festgelegten Bedingungen. Das Dokument tritt 90 Tage nach Hinterlegung der Ratifikationsurkunde durch den 40. Staat in Kraft. Um die Anwendung des Vertrags zu fördern und zu überprüfen, wird eine Konferenz der Vertragsstaaten eingerichtet, um die Fähigkeit der Vertragsstaaten und die Zusammenarbeit zwischen ihnen zu verbessern (Art. 57).

Externe Kritik

Als strafrechtliches Instrument wird das Übereinkommen Auswirkungen auf die Menschenrechte haben. Diese Auswirkungen können positiv sein, wenn der Rechtsrahmen Opfer schützt und Rechenschaftspflicht gewährleistet, aber auch negativ, wenn er ein Verhalten unter Strafe stellt, das geschützt werden sollte, oder wenn er keine ausreichenden Garantien für Ermittlungen und Strafverfolgung vorsieht.[22] Daher gehören die Menschenrechtsgarantien des Übereinkommens (Art. 6) zu den grundlegendsten – und umstrittensten – Artikeln. Eine breite Koalition aus zivilgesellschaftlichen Organisationen und Einrichtungen des privaten Sektors beteiligte sich am Verhandlungsprozess, da sie den Schutz und die Garantien für unzureichend hielten, um potenzielle Menschenrechtsverletzungen zu verhindern. Sie waren auch der Ansicht, dass diese in scharfem Kontrast zu den weitreichenden Verfahrens- und Durchsetzungsbefugnissen standen. Sie appellierten anschließend an die Staaten, das Übereinkommen nicht zu ratifizieren.[23]

Drei wesentliche Problembereiche

Erstens: Das Übereinkommen überlässt den Schutz der Menschenrechte weitgehend den innerstaatlichen Rechtssystemen und enthält keine konkreten Verweise auf etablierte internationale Rechtsrahmen, die die Einhaltung der

22 Ian Andrew Barber/Sheetal Kumar, Learning From the Ground Up: Lessons From Civil Society Engagement in Addressing the Human Rights Implications of Cybercrime Legislation, Journal of Cyber Policy, 9. Jg., 2/2024, S. 131–148.

23 UNODC, Urgent Appeal to Address Critical Flaws in the Latest Draft of the UN Cybercrime Convention, www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP8/Civil_Society_Joint_Open_Letter.pdf und Human Rights Watch, EU: Member States Should Vote 'No' on UN Cybercrime Treaty, 21.10.2024, www.hrw.org/news/2024/10/21/eu-member-states-should-vote-no-un-cybercrime-treaty.

Menschenrechtsverpflichtungen gewährleisten. Dieses Defizit kann dazu führen, dass bei der Umsetzung von Schutzmaßnahmen unterschiedliche innerstaatliche Rechtsvorschriften zur Anwendung kommen. Die begrenzten Schutzmaßnahmen in Verbindung mit weitreichenden Verfahrens- und Strafverfolgungsbefugnissen können zu einer ausufernden Überwachung führen. Gleichzeitig verpflichten die Bestimmungen zur internationalen Zusammenarbeit die Staaten, sich gegenseitig bei der Aufklärung und Verfolgung von Cyberkriminalität zu unterstützen, indem sie elektronische Beweismittel für alle Straftaten, die nach innerstaatlichem Recht als schwerwiegend gelten, sammeln, sicherstellen und austauschen.[24] Insbesondere der Privatsektor hat davor gewarnt, dass das Übereinkommen aufgrund minimaler und optionaler Menschenrechtsschutzmaßnahmen den Austausch personenbezogener Daten durch Regierungen weltweit erleichtern könnte.[25] Die vielen in dem Dokument enthaltenen Optionen zur Geheimhaltung von Anfragen geben Anlass zu Bedenken hinsichtlich der möglichen Verwendung der angeforderten Daten zu Überwachungs-, Strafverfolgungs- oder politisch motivierten Zwecken.[26] Darüber hinaus kann eine Bestimmung, die den Staaten die Gerichtsbarkeit über Straftaten einräumt, die weltweit gegen ihre Staatsangehörigen begangen werden (passives Personalitätsprinzip), zu einer deutlichen Ausweitung der Gerichtsbarkeit nach internationalem und nationalem Recht führen und die Souveränität, ein ordnungsgemäßes Verfahren und die Menschenrechte gefährden.[27]

Zweitens: Der Vertrag birgt Risiken für die Cybersicherheitsforschung.[28] Seitens der Sicherheitsforschung wurden erhebliche Bedenken geäußert, dass der Vertragstext die Rechte und Aktivitäten von Cybersicherheitsforscherinnen und -forschern, die in gutem Glauben handeln, einschränken könnte, da er nicht zwischen rechtmäßigen Sicherheitsforschungsaktivitäten und der vorsätzlichen Ausnutzung von Sicherheitslücken unterscheidet. Die Cybersicherheitsforschung hat es sich zur Aufgabe gemacht, Schwachstellen in Netzwerken, Betriebssystemen, Geräten, Firmware und Software aufzudecken und zu melden. Mehrere Bestimmungen des Übereinkommens bergen die Gefahr, diese Arbeit zu behindern, indem sie einen Großteil dieser Aktivitäten als kriminell einstufen und keine wirksamen Schutzmaßnahmen für ethisch handelnde Cybersicherheitsforscher und

24 Katitza Rodriguez, EFF's Concerns About the UN Draft Cybercrime Convention, Electronic Frontier Foundation, 29.7.2024, www.eff.org/deeplinks/2024/07/effs-concerns-about-un-draft-cybercrime-convention.

25 Cybersecurity Tech Accord, Press Release: Cybersecurity Tech Accord Calls for Changes to New UN Treaty to Prevent Damage to Global Security Online, 29.7.2024, cybertechaccord.org/press-release-cybersecurity-tech-accord-calls-for-changes-to-new-un-treaty-to-prevent-damage-to-global-security-online/.

26 Anastasiya Kazakova, UN Cybercrime Convention: Will States Give in Disagreements for the Sake of a Global Common Threat?, Geneva Internet Platform Digital Watch Observatory, 12.7.2024, dig.watch/updates/un-cybercrime-convention-will-states-give-in-disagreements-for-the-sake-of-a-global-common-threat.

27 Eli Scher-Zagier, Jurisdictional Creep: The UN Cybercrime Convention and the Expansion of Passive Personality Jurisdiction, Yale Journal of Law & Technology, 27. Jg., 1/2025, S. 327–389.

28 Laura Bartoli, Cybersecurity and the Fight Against Cybercrime: Partners or Competitors?, European Journal of Risk Regulation, 16. Jg, 2/2025, S. 498–513.

Penetrationstester vorsehen.[29]

Drittens: Das Umsetzungskapitel des Übereinkommens enthält nur unzureichende Kontrollbestimmungen. Ein Überprüfungsmechanismus ist nicht verpflichtend, ebenso wenig wie Beiträge von nichtstaatlichen Akteuren, die während der Verhandlungen eine wichtige Rolle gespielt haben. Daher wird die Umsetzung und Überprüfung des Übereinkommens weitgehend von den Modalitäten für die Arbeit und Teilnahme an der Konferenz der Vertragsstaaten und einem eventuellen Überprüfungsmechanismus abhängen, der von den Staaten als Geschäftsordnung vereinbart werden muss. Diese im Übereinkommen verankerte fakultative Regelung ermöglicht es den Regierungen, die Beteiligung nichtstaatlicher Akteure zu erschweren und eine externe Überprüfung staatlicher Maßnahmen zu beschränken.[30]

Was folgt nach Hanoi?

Das UN-Übereinkommen wurde bei der Unterzeichnungszeremonie in Hanoi, Vietnam, am 25. und 26. Oktober 2025 zur Unterzeichnung geöffnet und bleibt bis zum 31. Dezember 2026 zur Unterzeichnung offen. Die Staaten können ihm auch danach noch beitreten. 72 Länder haben das Übereinkommen bereits bei der Zeremonie unterzeichnet, darunter 13 EU-Mitgliedstaaten und die EU selbst. Es wird erwartet, dass viele weitere Länder das Dokument zu gegebener Zeit unterzeichnen werden. Die Tatsache, dass 121 Staaten das Übereinkommen in Hanoi noch nicht unterzeichnet haben – und Staaten erst nach der Ratifizierung rechtlich an das Übereinkommen gebunden sind –, zeigt jedoch, dass es noch eine ganze Weile dauern wird, bis das Übereinkommen weltweit akzeptiert ist.

Deutschland hat das Übereinkommen bisher nicht unterzeichnet, die USA ebenfalls, obwohl beide Vertragsparteien des Budapester Übereinkommens sind. Sollten die USA[31] diesem globalen Rahmenabkommen nicht beitreten, würde dies die Wirksamkeit des Vertrags erheblich schwächen, da zahlreiche wichtige Technologieunternehmen, bei denen elektronische Beweismittel gespeichert werden, ihren Firmensitz in den USA haben.

---

29 Karen Gullo, Protect Good Faith Security Research Globally in Proposed UN Cybercrime Treaty, Electronic Frontier Foundation, 7.2.2024, www.eff.org/deeplinks/2024/02/protect-good-faith-security-research-globally-proposed-un-cybercrime-treaty und Cybersecurity Tech Accord, Press Release, a.a.O. (Anm. 25).

30 Summer Walker/Ana Paula Oliveira, The Final Call: UN Member States Adopt a New Cybercrime Treaty, Global Initiative Against Transnational Organized Crime, 12.9.2024, globalinitiative.net/wp-content/uploads/2024/09/Summer-Walker-Ana-Paula-Oliveira-The-final-call-UN-member-states-adopt-a-new-cybercrime-treaty-GI-TOC-September-2024.pdf.

31 Alexis Steffaro, The U.S. and UN Cybercrime Convention: Progress, Concerns, and Uncertain Commitments, Center for Cybersecurity Policy and Law, 22.11.2024, www.centerforcybersecuritypolicy.org/insights-and-research/the-u-s-and-un-cybercrime-convention-progress-concerns-and-uncertain-commitments und United States Mission to the United Nations (USUN), Explanation of Position of the United States on the Adoption of the Resolution on the UN Convention Against Cybercrime in the UN General Assembly's Third Committee, 11.11.2024, 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-co

Angesichts des umfassenden Geltungsbereichs des Vertrags und der weitreichenden Befugnisse, die den staatlichen Stellen übertragen werden, wird ein menschenrechtsbasierter und an den beteiligten Akteuren orientierter Ansatz zur Überwachung und Umsetzung des Vertrags von größter Bedeutung sein. Nur so lassen sich missbräuchliche Anwendungen vermeiden und die erwarteten Vorteile des Vertrags mit seinen Nachteilen vereinbaren.[32] Kritikerinnen und Kritiker argumentieren, dass die Unterzeichnung des Übereinkommens die Staaten zu Komplizen eines möglichen Missbrauchs des Vertrags machen würde, da dieser keine ausreichenden Menschenrechtsschutzbestimmungen enthalte. Befürworter halten dem entgegen, dass Staaten nur dann einen positiven Einfluss auf die Überprüfung und Umsetzung nehmen können, wenn sie Vertragspartei würden.[33] Nun liegt es an den Unterzeichnern, alles in ihrer Macht Stehende zu tun, um sicherzustellen, dass das Übereinkommen nicht gegen Staaten und deren Bürger missbraucht wird und dass ihre Umsetzung zur internationalen Zusammenarbeit bei der Bekämpfung der Cyberkriminalität beiträgt, ohne Grundfreiheiten zu gefährden.

Aus dem Englischen von Angela Großmann

32 Walker/Oliveira, The Final Call, a.a.O. (Anm. 30).

33 Steffaro, The U.S. and UN Cybercrime Convention, a.a.O. (Anm. 31).

Authors

Pavlina Pavlova

Christina Rupp
Lead Cybersecurity Policy and Resilience
crupp@interface-eu.org
+49308145037880

Sven Herpig
Lead Cybersecurity Policy and Resilience | Advisor to the Executive Director
sherpig@interface-eu.org
+49 (0)30 81 45 03 78 91

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org
T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
c/o Publix
Hermannstraße 90
D-12051 Berlin

Design by Make Studio
www.make.studio
Code by Convoy
www.convoyinteractive.com