: Global Governance Spotlight

5 | 2021

sef:

# UN-Abkommen gegen Cyberkriminalität – Menschenrechte und Entwicklung ins Zentrum rücken

Mischa Hansel

**Im Januar 2022 werden die Mitgliedstaaten der Vereinten Nationen (UN) Verhandlungen über ein globales Abkommen zur Bekämpfung der Cyberkriminalität aufnehmen. Mehr internationale Zusammenarbeit in diesem Bereich ist dringend geboten. Denn kriminelle Angriffe auf IT-Systeme können lebensbedrohlich sein, wie erpresserische Cyberattacken auf Krankenhäuser in vielen Ländern zeigen. Zudem ist Cyberkriminalität längst ein globales Risiko. Gerade in Ländern des Globalen Südens halten IT-Sicherheitsmaßnahmen oft nicht mit der rasanten Digitalisierung Schritt. Darunter leiden besonders Zukunftsbranchen wie E-Commerce oder mobile Finanzdienstleistungen, die für die wirtschaftliche Entwicklung entscheidend sind. Hinzu kommt, dass viele Länder nur unzureichend in die internationale Zusammenarbeit der Strafverfolgungsbehörden eingebunden sind.**

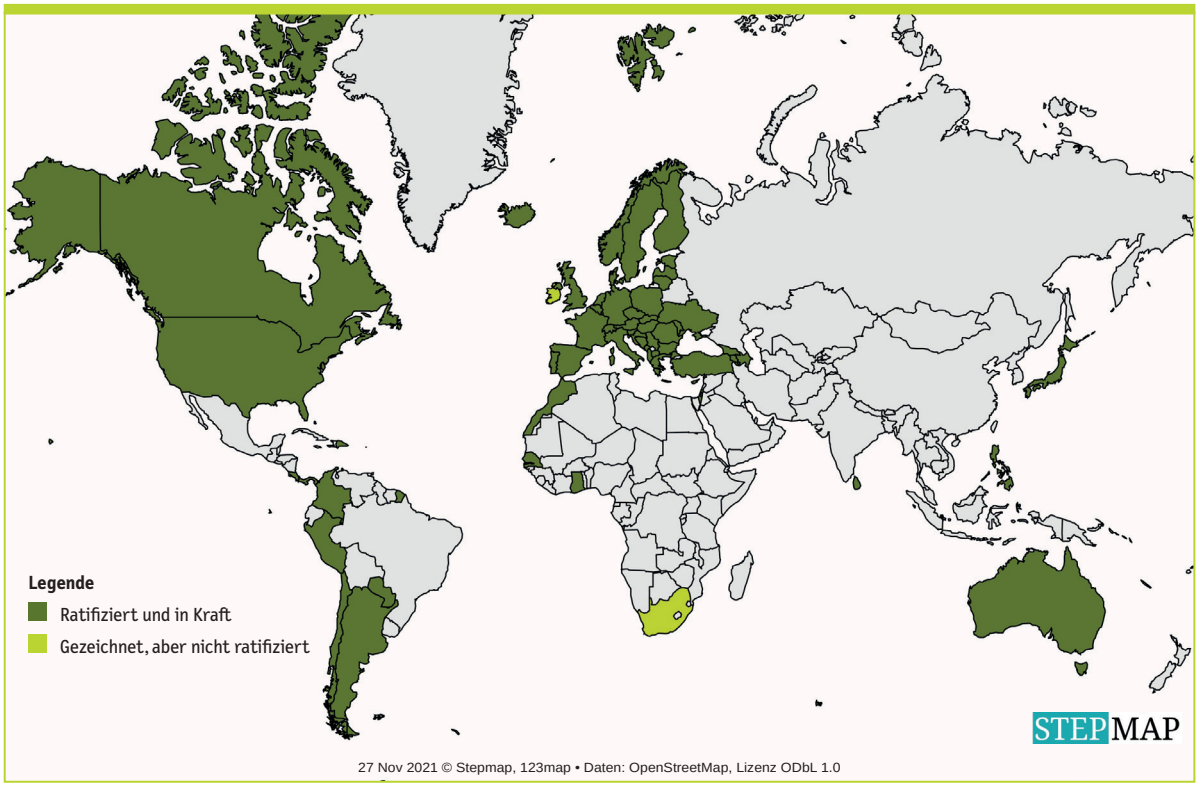
**Vor diesem Hintergrund wäre es in der Tat Zeit für ein umfassendes globales Abkommen gegen Cyberkriminalität. Doch es gibt auch Risiken. So könnten vage Verpflichtungen, etwa zur Überwachung des Internetverkehrs, von autoritären Regimen missbraucht werden, um unter dem Deckmantel der Kriminalitätsbekämpfung gegen Aktivisten und Oppositionelle vorzugehen. Um dies zu verhindern, müssen die Menschenrechte als Referenzrahmen gestärkt werden und zivilgesellschaftliche Akteure substanziell zu den Verhandlungen beitragen können. Zugleich sollte der Kapazitätsaufbau in Ländern des Globalen Südens ausgeweitet werden. Schließlich gilt es, bestehende Schutzlücken zu schließen und auch die sozialen Ursachen des Abdriftens in die Cyberkriminalität nicht zu ignorieren. So könnte eine globale Koalition für ein menschenrechtskonformes und entwicklungszentriertes Regime möglich werden.**

## Auf dem Weg zu einem globalen Abkommen?

Die dramatische Zunahme sogenannter Ransomware-Attacken auf Krankenhäuser, die Energieversorgung oder öffentliche Verwaltungen zeigt das ganze Zerstörungspotenzial krimineller Cyberoperationen deutlich. Durch diese Attacken werden kritische Daten verschlüsselt; erst nach Zahlung eines Lösegeldes wird eine Entschlüsselungs-Software bereitgestellt. Da die Täter in der Regel grenzüberschreitend operieren, müssen Polizei und Strafverfolgungsbehörden international kooperieren, um kriminelle Infrastrukturen auszuschalten oder die Täter überführen zu können. Das scheitert jedoch oft an uneinheitlichen rechtlichen Bestimmungen, fehlendem politischen Willen und ineffektiven Verfahren.

Hier könnten die Vereinten Nationen ansetzen und einen universell verbindlichen Rahmen für die Kooperation gegen Cyberkriminalität schaffen. Bislang wurde Cyberkriminalität als Unterthema im Rahmen der UN-Konvention gegen transnationale organisierte Kriminalität behandelt. Zudem hat die dem UN-Wirtschafts- und Sozialrat zugehörige Kommission für Kriminalprävention und Strafjustiz seit 2011 mehrfach Expertengruppen einberufen, um über die Verbesserung technischer Hilfen zu beraten und den

Austausch über gesetzliche Maßnahmen und Best Practices voranzutreiben. Die von Russland initiierte und am 27. Dezember 2019 von der UN-Generalversammlung mehrheitlich angenommene Resolution 74/274 sieht nun die Bildung eines Ausschusses (Ad Hoc Komitee) vor, der innerhalb von fünf Jahren einen Vertragsentwurf für ein spezifisches Abkommen gegen den kriminellen Missbrauch von Informations- und Kommunikationstechnik (IKT) ausarbeiten soll. Über den Umfang und die Form einer zukünftigen




Ratifzierungsstand des Übereinkommens über Computerkriminalität des Europarats (30.11.2021)

stärkeren Zusammenarbeit gibt es jedoch erhebliche Differenzen. Zudem ist das Verhältnis zu bestehenden Regimen ungeklärt. Das betrifft insbesondere das Übereinkommen über Computerkriminalität des Europarates (Budapest Konvention) von 2001, dem auch zahlreiche Nichtmitglieder weltweit angehören und das 2021 durch ein Zusatzprotokoll grundlegende modernisiert wurde.

## Geopolitische Konflikte

Bereits jetzt ist absehbar, dass geopolitische Konflikte und Interessengegensätze die Arbeit des Ad Hoc Komitees erschweren werden. So hat Russland einen Vertragsentwurf vorgelegt, der zwar eine große Bandbreite von Straftaten umfasst, jedoch ganz unter dem Leitstern nationaler Souveränität steht und grenzüberschreitende Kooperationen nur als klassische Rechtshilfeersuchen zulässt. Im Gegensatz dazu haben Strafverfolgungsbehörden im Rahmen der Budapest Konvention die Möglichkeit, auch direkt Datenabfragen an kommerzielle Internetdienstanbieter im Ausland zu stellen, ohne zuvor die Erlaubnis der dortigen Behörden einzuholen. Diese Möglichkeiten werden durch das zweite Zusatzprotokoll noch erweitert. Denn im Zeitalter von Cloud-Diensten können die Ermittlungsbehörden kaum mehr Schritt halten mit dem Tempo, in dem Kriminelle ihre Spuren verschleiern.

Weitere Gegensätze beziehen sich auf Datenschutzaspekte und den Schutz vor staatlicher Willkür. So fordert der russische Entwurf die nahezu lückenlose Speicherung von Verkehrsdaten durch Behörden oder Provider im Zuge der Verbrechensprävention. Straftaten wie „politischer Extremismus“ oder „Terrorismus“ sind zudem ausgesprochen vage definiert. Dies lässt sich geradezu als Einladung verstehen, diese Bestimmungen gegen jedwede politische Opposition einzusetzen. Die Mitgliedstaaten der Europäischen Union hingegen vertreten die Position, dass ein zukünftiger Vertrag nur wenige und sehr präzise umrissene Straftaten umfassen sollte. Tendenzen einer Lagerbildung zeigen sich auch im Rahmen der praktischen Zusammenarbeit, etwa gegen Ransomware. So wurden China und Russland, denen eine stillschweigende Zusammenarbeit mit cyberkriminellen Gruppierungen vorgeworfen wird, erst gar nicht eingeladen, an der US-geführten „International Counter-Ransomware Initiative“ teilzunehmen.

Der Blick allein auf die „Cybergroßmächte“ USA, China und Russland reicht jedoch nicht aus. Gerade aus europäischer Perspektive muss zu denken geben, dass die russischen Resolutionen zum Thema erheblichen Zuspruch auch von demokratischen Ländern

wie Nigeria, Indien oder Brasilien gefunden haben und dass das Übereinkommen des Europarates über Cyberkriminalität gerade auf dem afrikanischen Kontinent bislang nur von sehr wenigen Staaten ratifiziert wurde. Deshalb ist es unerlässlich, Cyberkriminalität wirklich als globales Problem wahrzunehmen, das nicht nur entwickelte Industriestaaten betrifft.

## Cyberkriminalität im globalen Süden

Die pandemiebedingte Wirtschaftskrise in Ländern des Globalen Südens hat dazu beigetragen, dass gut ausgebildete Arbeitskräfte vermehrt durch kriminelle Kartelle rekrutiert werden konnten. Ihre Ziele suchen sich diese Kartelle sowohl innerhalb als auch außerhalb ihrer Region. Einen globalen „Robin-Hood-Effekt“ gibt es nicht. Denn die Opfer von Cyberkriminalität kommen weltweit aus allen sozialen Schichten. Und gerade im Globalen Süden gefährden Cyberkriminelle Schlüsselbereiche der gesellschaftlichen Entwicklung wie digitale Finanzdienstleistungen oder den E-Commerce-Sektor. Leichtes Spiel haben Cyberkriminelle unter anderem aufgrund der weiten Verbreitung illegaler und schlecht gesicherter Software sowie der mangelnden technischen, personellen und finanziellen Ausstattung vieler lokaler Strafverfolgungsbehörden.

Zugleich sind nicht alle Defizite der Bekämpfung von Cyberkriminalität etwa auf dem afrikanischen Kontinent hausgemacht. Vielmehr erschweren mangelnde Zugriffsmöglichkeiten auf Daten global tätiger Internetkonzerne erfolgreiche Ermittlungsaktivitäten. Hinzu kommt die mangelnde Einbindung in operative Netzwerke der grenzüberschreitenden Kooperation von Strafverfolgungsbehörden. Schließlich gibt es Delikte, die über ein enges Verständnis von Cyberkriminalität hinausgehen, aber in besonderem Maße Gefahren für Frieden und Entwicklung auf dem afrikanischen Kontinent darstellen.

Dazu gehören der rasant wachsende Handel mit Konfliktgütern (Tropenholz, Mineralien, Waffen, Drogen) im sogenannten Dark Web und der internetgestützte Menschenhandel. Zudem sind afrikanische Länder in Zeiten gesellschaftlicher Instabilitäten besonders durch Gewaltaufrufe oder Desinformation in sozialen Medien betroffen, die oftmals von Dienstleistern außerhalb des afrikanischen Kontinents betrieben werden. Diese Interessenlagen und Prioritäten spiegeln sich nicht zuletzt in der Malabo-Konvention wider, einem regionalen Abkommen zur Förderung der Cybersicherheit und des Datenschutzes, das unter Cyberkriminalität auch inhaltsbezogene Delikte einschließt. Dieses breite Verständnis von Cyberkriminalität kollidiert wiederum mit der aktuellen Verhandlungsposition der EU-Mitgliedstaaten, die im UN-Rahmen ein schlankes Abkommen, bezogen auf wenige cyberabhängige Delikte, anstreben, sowohl um Dopplungen mit anderen Instrumenten zu vermeiden als auch um Missbrauchsrisiken durch autoritäre Regime zu begrenzen.

In dem Übereinkommen über Computerkriminalität des Europarates, das von vielen europäischen Staaten sowie den USA als Modell betrachtet wird, ist die Kriminalisierung von rassistischen oder gewaltverherrlichenden Inhalten nur optional durch ein Zusatzprotokoll geregelt, jedoch nicht zwingend für alle Vertragsstaaten. Angesichts sehr unterschiedlicher Verständnisse bezüglich der Grenzen der Meinungsfreiheit, etwa zwischen den USA sowie einigen EU-Staaten, wäre alles andere auch nicht durchsetzbar.

## Menschenrechte schützen und Entwicklung ermöglichen

Um trotz dieser unterschiedlichen Perspektiven und Interessenlagen eine möglichst breite Koalition für eine intensivierte globale Zusammenarbeit gegen Cyberkriminalität zu schmieden, sollten die besonderen Bedürfnisse der Länder im Globalen Süden entweder innerhalb eines zukünftigen Vertragswerkes oder außerhalb, durch flankierende politische Maßnahmen, berücksichtigt werden.

Ein zentraler Baustein sollte ein generelles Bekenntnis zum Ausbau des internationalen Capacity-Buildings sein, möglichst auch unterlegt mit der Einrichtung eines multilateralen Fonds. Angesichts extrem angespannter Haushalte in vielen Ländern des Globalen Südens ist nicht zu erwarten, dass sich die Ausstattung der Ermittlungsbehörden dort nachhaltig verbessern wird. Zugleich könnte ein Abkommen auch Leitlinien für die Priorisierung von Rechtshilfe-Ersuchen sowie grenzüberschreitender multilateraler Ermittlungen enthalten. Im Sinne internationaler Solidarität sollte dabei nicht primär die lokale Betroffenheit, sondern der bereits eingetroffene oder zu erwartende gesellschaftliche Schaden, gleich wo er entsteht, ausschlaggebend sein.

Im Rahmen des Kapazitätsaufbaus sowie der konkreten Kooperation muss es zugleich darum gehen, den Missbrauch von Gesetzen gegen Cyberkriminalität, der in vielen Ländern tägliche Praxis ist, einzudämmen. Ein globales Abkommen sollte sich an hohen rechtsstaatlichen Standards, wie beispielsweise denjenigen der Datenschutzkonvention des Europarates, orientieren. Es sollte Straftatbestände präzise definieren und darf fundamentale Menschenrechte, wie das Recht auf Privatsphäre, nicht relativieren. Vielmehr muss die Geltung der Menschenrechte für alle nationalen und grenzüberschreitenden Ermittlungs- und Strafverfolgungsmaßnahmen bekräftigt werden. Um staatlichem Missbrauch vorzubeugen, sollten zivilgesellschaftliche Akteure nicht nur im Verhandlungsprozess mitwirken können, sondern auch eine wichtige Rolle in der Phase der Implementierung und des Monitorings übernehmen. Dabei ist

selbstverständlich darauf zu achten, dass zivilgesellschaftliche Akteure aus dem Globalen Süden nicht durch finanzielle und logistische Hürden ausgeschlossen sind, etwa durch die Einrichtung regionaler Verbindungsbüros.

Flankierend zur Aushandlung eines völkerrechtlich bindenden Abkommens wäre es auf operativer Ebene zu begrüßen, wenn Länder des Globalen Südens stärker in den institutionalisierten Austausch von Strafverfolgungsbehörden eingebunden wären. Das kann auf regionaler Ebene geschehen, wie etwa durch das von INTERPOL initiierte „African Joint Operation against Cybercrime (AFJOC)"-Projekt. Über die regionale Kooperation hinaus braucht es aber auch Foren für die Zusammenarbeit etwa mit europäischen Partnerbehörden. Ein Beispiel ist die von EUROPOL eingerichtete „Joint Cybercrime Action Taskforce" (J-CAT), in der u.a. Kolumbien bereits als institutionalisierter Partner mitwirkt. Innerhalb solcher Netzwerke könnte insbesondere die Bekämpfung des internetgestützten Handels mit Konfliktgütern zu einem Schwerpunkt gemacht werden.

Ein weiterer Punkt betrifft die Regulierung von Internet-Plattformen und Software-Anbietern. Die jüngsten Handelsbeschränkungen gegenüber israelischen Überwachungsdienstleistern durch die US-Regierung sind hier nur ein Anfang, um die Unterstützung von Unterdrückung und Folter auch durch westliche IT-Konzerne einzudämmen. Über Maßnahmen gegen Einzelfirmen hinaus braucht es stärkere Exportkontrollen und eine verbindliche Regulierung digitaler Lieferketten. Dann können die Verantwortlichen mitunter auch strafrechtlich verfolgt werden, wie unlängst in Frankreich geschehen, wo Mitglieder der Geschäftsführung von Amesys, einer französischen Überwachungsfirma, angeklagt wurden. Auch reichen Regularien für den Umgang mit Desinformation und Hassrede nicht aus, wenn Plattformbetreiber und Dienstleister diese nur auf dem heimischen Markt einhalten müssen. Vielmehr müssen auch die auswärtigen Geschäftstätigkeiten von Social-Media-Diensten und digitalen Plattformen im Sinne unternehmerischer *due diligence* reglementiert werden.

Schließlich sollten nicht allein die Symptome des Phänomens Cyberkriminalität adressiert werden, sondern es müssen im Sinne der nachhaltigen UN-Entwicklungsziele und eines integrierten Ansatzes auch die sozialen Ursachen in den Blick genommen werden. Ohne die Schaffung einer ökonomischen Perspektive für Millionen gut ausgebildeter junger Menschen beispielsweise auf dem afrikanischen Kontinent wird es nicht gelingen, die Rekrutierungspraxis cyberkrimineller Kartelle zu durchkreuzen. Ein solcher präventiver Gedanke ist nicht ohne Vorbild. In den frühen 1990er Jahren etwa diente die amerikanisch-russische Zusammenarbeit bzgl. der internationalen Raumstation auch dazu, russischen Ingenieuren Beschäftigungsmöglichkeiten im zivilen Bereich zu sichern und sie so davon abzuhalten, an der lukrativen illegalen Proliferation von Raketentechnik nach Iran oder Nordkorea mitzuwirken. Dieselbe Weitsicht – in zugegebenermaßen viel größerem Maßstab – wäre heute nötig, um den Pull-Faktoren der Cyberkriminalität in vielen Ländern des Globalen Südens entgegenzuwirken. Das kann nicht allein im UN Ad Hoc Komitee geschehen. Gleichwohl bietet gerade die Verankerung in den UN die Chance, die Prävention und Bekämpfung von Cyberkriminalität in einem größeren Zusammenhang, der menschenrechtliche Sorgfaltspflichten und Entwicklungsperspektiven miteinschließt, anzugehen.

**Autor**

Dr. Mischa Hansel | Leiter des Forschungsschwerpunkts „Internationale Cybersicherheit" (ICS) am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH). @MischaHansel

**Literatur**

Europarat 2001: Übereinkommen über Computerkriminalität, https://rm.coe.int/1680081561.

Kommersant 2021: Draft United Nations Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, Unofficial Translation, https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf.

United Nations General Assembly 2020: Resolution 74/247: Countering the Use of Information and Communications Technologies for Criminal Purposes, https://undocs.org/A/Res/74/247.

**Impressum**

Die Stiftung Entwicklung und Frieden (sef:) wurde 1986 auf Initiative von Willy Brandt gegründet. Als überparteiliche und gemeinnützige Stiftung bietet sie ein hochrangiges internationales Forum für das gemeinsame Nachdenken über drängende Fragen von Frieden und Entwicklung.

Global Governance Spotlight ist ihre kompakte politikorientierte Publikationsreihe zur kritischen Begleitung internationaler Verhandlungsprozesse aus der Global-Governance-Perspektive.

**Herausgeberin**
Stiftung Entwicklung und Frieden (sef:)
Dechenstr. 2 : D-53115 Bonn
Tel. 0228 959 25-0 : Fax 0228 959 25-99
sef@sef-bonn.org : @sefbonn
www.sef-bonn.org

**Redaktion**
Dr. Michèle Roth

**Design Basiskonzept**
Pitch Black Graphic Design
Berlin/Rotterdam

**Gestaltung**
Gerhard Süß-Jung

**Papier**
Umweltzeichen Blauer Engel

Die Inhalte geben nicht unbedingt die Meinung der Herausgeberin wieder.

ISSN 2195-0873 (print)
ISSN 2566-6258 (online)