

Internationale Cyberdiplomatie unter Druck: Gemeinsam handlungsfähig bleiben

Die internationale Cyberdiplomatie steht vor einer doppelten Herausforderung: Wachsende Bedrohungen aus dem Cyberraum erfordern mehr globale Zusammenarbeit, während geopolitische Spannungen diese zunehmend erschweren. Die Cyberdiplomatie der *Vereinten Nationen* (VN) gerät dadurch unter Druck. Um ihre Handlungsfähigkeit zu stärken, sollte sich Deutschland im VN-System dafür einsetzen:

- Gesprächs- und Verhandlungsformate zu verstetigen, um den Dialog auch bei anhaltenden politischen Gegensätzen aufrechtzuerhalten,
- technische Expertise stärker einzubinden, um Verhandlungen sachlich zu fundieren und politische Machtkämpfe abzufedern, und
- bestehende und neue Verhandlungs- und Austauschformate besser aufeinander abzustimmen, um Überschneidungen zu reduzieren und einer weiteren Fragmentierung entgegenzuwirken.

Trotz wachsender Bedrohungen aus dem Cyberraum wird die globale Zusammenarbeit in der Cyberdiplomatie schwieriger. Angesichts wachsender geopolitischer Spannungen setzen Staaten zunehmend auf unilaterale Abschreckung und offensive Fähigkeiten und stellen zugleich den Nutzen internationaler Verhandlungen infrage. Innerhalb der Vereinten Nationen (VN), wo solche Verhandlungen maßgeblich stattfinden, nehmen Polarisierung, Politisierung und Fragmentierung zu. Dies erschwert gemeinsame Entscheidungen und globale Regelfindung. Deutschland sollte sich dafür einsetzen, die VN-Cyberdiplomatie institutionell zu stärken und so ihre Handlungsfähigkeit zu sichern.

VN-CYBERDIPLOMATIE ZWISCHEN KONSENSFINDUNG UND KRÄFTEMESSEN

Die Vereinten Nationen (VN) sind das zentrale multilaterale Forum für internationale Cyberdiplomatie. Seit über 20 Jahren werden hier wesentliche Fragen der Cybersicherheit verhandelt – vom staatlichen Verhalten im Cyberraum über die Anwendung des Völkerrechts bis hin zur Bekämpfung von Cyberkriminalität. Neue Technologien wie künstliche Intelligenz (KI) oder Quantencomputing schaffen zusätzliche Herausforderungen für die Cybersicherheit und internationale Regulierung. Einen Meilenstein markiert die 2024 verabschiedete internationale Cyberkriminalitätskonvention als erstes und bislang einziges völkerrechtlich verbindliches VN-Abkommen in diesem Bereich.

Zugleich gerät die VN-Cyberdiplomatie immer stärker unter Druck: Verschärfte politische Rivalitäten und ökonomische Herausforderungen verstärken die Fliehkräfte im System. Angesichts wachsender Cyberbedrohungen setzen manche Staaten ver-

stärkt auf digitale Resilienz, Abschreckung und offensive Fähigkeiten und stellen den Nutzen von internationalen Verhandlungen zunehmend in Frage. Konfliktlinien verhärten sich, technische Fragen werden von machtpoliti-

schen Interessen überlagert und Verhandlungen verlagern sich immer häufiger in informelle oder regionale Foren. Zentrale globale Verhandlungen – etwa über staatliches Verhalten und staatliche Sorgfaltspflichten im Cyberraum sowie die Anwendung des Völkerrechts auf Cyberoperationen – kommen dadurch nur sehr langsam voran.

Gefragt sind daher Maßnahmen, die der Polarisierung, Politisierung und Fragmentierung entgegenwirken und die die VN-Cyberdiplomatie strukturell stärken. Deutschland sollte entsprechende Bemühungen aktiv unterstützen.

POLARISIERUNG: DIALOG- UND AUSTAUSCH- FORMATE DAUERHAFT ETABLIEREN

Polarisierungen in internationalen Verhandlungen über Cybersicherheit sind nicht neu. Anhaltende Gegensätze bestehen insbesondere zwischen westlichen Staaten, allen voran den USA und der EU, auf der einen sowie Russland und China auf der anderen Seite. Während Erstere für eine eher offene und menschenrechtsorientierte Regulierung des Cyberraums eintreten, vertreten Letztere ein staatszentriertes Verständnis von Informationssicherheit. Sie setzen auf nationale Kontrolle des Cyberraums und verbindliche internationale Regeln.

Besonders deutlich treten diese Gegensätze in zeitlich begrenzten Verhandlungsformaten zutage. Die Cyberkriminalitätskonvention von 2024 ist zwar ein

**„DIE VN SIND DAS
ZENTRALE MULTI-
LATERALE FORUM
FÜR INTERNATIONALE
CYBERDIPLOMATIE.“**

verbindliches Abkommen und das Ergebnis internationaler Diplomatie, beruht jedoch auf Kompromissen, die wichtige Fragen offenlassen. So ist umstritten, wie weit staatliche Befugnisse reichen und wie Menschenrechtsstandards gewährleistet werden. Dass einige Staaten mit der Unterzeichnung oder Ratifizierung zögern und bei der Vorbereitung der Vertragsstaatenkonferenz neue Konflikte auftreten, zeigt: Mit der Verabschiedung der Konvention sind die grundlegenden Gegensätze nicht überwunden.

Die VN-Cyberdiplomatie sollte daher mehr dauerhafte Dialog-, Austausch- und Überprüfungsformate etablieren. Da sich die Positionen der Staaten zur Cybersicherheit in absehbarer Zeit kaum grundlegend verändern dürften, ist kontinuierlicher Austausch umso wichtiger. Er hält Gesprächskanäle offen und kann insbesondere bei der Umsetzung bereits vereinbarter Regeln helfen, trotz politischer Gegensätze zu einer gemeinsamen Auslegung zu gelangen.

POLITISIERUNG: TECHNISCHE EXPERTISE EINBINDEN

Cybersicherheit ist längst nicht mehr nur eine technische Frage. Sie berührt wirtschaftliche Interessen, nationale Sicherheit und geopolitischen Einfluss. Damit werden auch fachliche Fragen zusehends von politischen Konflikten überlagert. Dies zeigt sich etwa im kürzlich ins Leben gerufenen *Global Mechanism on Developments in the Field of Information and Communication Technologies* (ICTs). Das Gremium führt die Arbeit der bisherigen *Open-Ended Working Group on ICTs* (OEWG) fort und erarbeitet Regeln für die verantwortungsvolle Nutzung von Informations- und Kommunikationstechnologien. Inhaltliche Fortschritte werden dort weiterhin durch grundsätzliche politische Differenzen erschwert. So ist umstritten, ob man überhaupt neue Cybernormen entwickeln soll und wie das Völkerrecht hier zur Anwendung kommt. Hinzu kommt, dass Russland, China und ihnen nahe-

stehende Staaten es ablehnen, ziviles gesellschaftliche und private Akteure im Verhandlungsprozess zu beteiligen.

Technische Expertise kann diese Konflikte nicht auflösen, aber dazu beitragen, Verhandlungen stärker auf konkrete Sachfragen auszurichten und so arbeitsfähig zu halten. Nichtstaatliche Akteure verfolgen zwar ebenfalls eigene Interessen, verfügen jedoch häufig über Fachwissen, das staatliche Delegationen nicht in gleichem Umfang haben. Stakeholder-Konsultationen, wie sie bei den Verhandlungen zur Cyberkriminalitätskonvention bereits praktiziert wurden, oder wissenschaftliche Beratergremien nach dem Vorbild der internationalen Umweltpolitik können hier als Modelle dienen. Daher sollte technische Expertise stärker und dauerhaft in der VN-Cyberdiplomatie verankert werden.

FRAGMENTIERUNG: VERHANDLUNGSPROZESSE BESSER KOORDINIEREN

Neben Polarisierung und Politisierung stellt die zunehmende Fragmentierung der internationalen Cyberdiplomatie eine weitere Herausforderung für das VN-System dar. Zahlreiche neue Verhandlungsforen, Mandate und Institutionen befassen sich mit einzelnen, oft jedoch eng miteinander verknüpften Aspekten der Cybersicherheit. Sie schaffen zusätzliche Möglichkeiten für den diplomatischen Austausch, vereinzeln aber Debatten und können zugleich Überschneidungen und konkurrierende Zuständigkeiten begünstigen. Für Staaten und andere beteiligte Akteure wird es dadurch schwieriger, den Überblick zu behalten: Wo werden relevante Fragen verhandelt? Wo können sie sich einbringen? Wie werden die Ergebnisse zusammengeführt?

„GEOPOLITISCHE
RIVALITÄTEN
VERSCHÄRFEN
DIE FLIEHKRÄFTE
IM VN-SYSTEM.“

Besonders deutlich wird dies bei den Querschnittsthemen neue Technologien und künstliche Intelligenz (KI): Ein zentrales Verhandlungsforum gibt es nicht. Stattdessen sind innerhalb kurzer Zeit mehrere parallele Strukturen im VN-System entstanden. Diese befassen sich mit ähnlichen Fragen, unterscheiden sich jedoch in ihrer Zusammensetzung und Funktion – von wissenschaftlicher Beratung und politischem Austausch bis hin zur Regelsetzung. Zugleich verlagern sich Debatten zusehends in regionale Organisationen. So gewinnt etwa die *Europäische Union* (EU) im Bereich der KI-Regulierung an Bedeutung. Gerade bei solchen Querschnittsthemen sollten die verschiedenen Formate und Organisationen jedoch enger zusammenarbeiten und Informationen regelmäßig austauschen. Hierfür gilt es, Schnittstellen zu stärken, zentrale Anlaufstellen zu schaffen und wirksame Koordinierungsinstrumente zu etablieren.

DEUTSCHLANDS AUFTRAG: CYBERDIPLOMATIE STÄRKEN UND WEITERENTWICKELN

Nirgendwo sonst wird so umfassend über globale Cybersicherheit verhandelt wie in den VN. Neue Institutionen und Austauschformate unterstreichen ihre zentrale Rolle. Zugleich erschweren politische Rivalitäten und institutionelle Fragmentierung die internationale Zusammenarbeit. Deutschland sollte sich daher aktiv dafür einsetzen, die Cyberdiplomatie innerhalb der VN weiterzuentwickeln, damit sie auch unter schwierigen geopolitischen Bedingungen handlungsfähig bleibt.

ÜBER DEN AUTOR

Lena Herbst ist Wissenschaftliche Mitarbeiterin am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH).

ÜBER DAS PROJEKT

Dieser Policy Brief entstand im Rahmen des Forschungs- und Transferprojekts „Internationale Cybersicherheit“, das vom Auswärtigen Amt gefördert wird.

ÜBER DAS INSTITUT

Das Institut für Friedensforschung und Sicherheitspolitik (IFSH) erforscht die Bedingungen von Frieden und Sicherheit in Deutschland, Europa und darüber hinaus. Das IFSH forscht eigenständig und unabhängig. Es wird von der Freien und Hansestadt Hamburg finanziert.

Gefördert von:



Auswärtiges Amt



Gefördert von:

Behörde für Wissenschaft,
Forschung, Gleichstellung
und Bezirke

DOI: <https://doi.org/10.25592/ifsh-policy-brief-0126>

Copyright Cover Photo: dpa Picture Alliance / Xinhua News Agency | Xie E Text License: Creative Commons CC-BY-ND (Attribution/NoDerivatives/4.0 International).



IFSH – Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Beim Schlump 83 20144 Hamburg Germany Phone +49 40 866077-0 ifsh@ifsh.de www.ifsh.de