IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Cyberkriminalität: Gemeinsam Gefahren für den Frieden eindämmen

Ab Januar 2022 beraten die Mitgliedstaaten der Vereinten Nationen (VN) über einen globalen Vertrag gegen Cyberkriminalität. Mehr internationale Zusammenarbeit in diesem Bereich ist dringend geboten. Denn kriminelle Cyberattacken, etwa gegen Krankenhäuser oder Stromnetze, können lebensbedrohlich sein und zu Panikreaktionen in der Bevölkerung führen. Da sich die Urheber*innen solcher Attacken in der Regel im Ausland befinden, reichen rein nationale Gegenmaßnahmen nicht aus. Ein neues globales Regelwerk sollte:

- bewährte Standards, wie insbesondere diejenigen der Budapest-Konvention des Europarats, bekräftigen,
- mit geeigneten Instrumenten auf Eskalationsrisiken und Schutzlücken reagieren, und
- Menschenrechtsverletzungen, die unter dem Vorwand der Kriminalitätsbekämpfung begangen werden, verhindern.

07|21

MISCHA HANSEL UND JANTJE SILOMON | 2021

Cyberkriminalität wird zu einer wachsenden Gefahr für den internationalen Frieden. Attacken gegen kritische Infrastrukturen wie Krankenhäuser oder die Energieversorgung gefährden grundlegende Elemente der Daseinsvorsorge. Nicht selten decken Staaten Cyberkriminelle und nutzen deren Aktivitäten für ihre politischen Zwecke. Deshalb birgt das Thema international erheblichen Zündstoff und zwischenstaatliche Eskalationen nach kriminellen Attacken sind eine reale Gefahr. Mit Blick auf die anstehenden VN-Verhandlungen über eine „Globale Konvention zur Bekämpfung des kriminellen Missbrauchs von Kommunikations- und Informationstechnik“[1] ist daher dreierlei vonnöten: Erstens sollten bestehende Best Practices der grenzüberschreitenden Kooperation gegen Cyberkriminalität gestärkt werden. Zweitens sind neue Instrumente nötig, die zur Eskalationskontrolle beitragen und Schutzlücken schließen können. Drittens gilt es zu vermeiden, dass repressive Regime unter dem Vorwand der Kriminalitätsbekämpfung Menschenrechtsverletzungen begehen.

EINE NEUE QUALITÄT KRIMINELLER CYBERATTACKEN

Im Frühjahr und Sommer 2021 kam es zu mehreren gravierenden Ransomware-Attacken (Ransom: engl. für „Erpressung“) auf Ziele in den Vereinigten Staaten. Dabei versuchten russischsprachige Cyberkriminelle durch die Verschlüsselung kritischer Daten Lösegelder zu erpressen. Besonders folgenreich war eine Attacke auf das Abrechnungssystem eines großen Pipelinebetreibers. In zahlreichen US-Bundesstaaten brach danach die Treibstoffversorgung nahezu zusammen. Als Reaktion deutete US-Präsident Biden an, Cyberattacken gegen russische kritische Infrastrukturen als Vergeltung durchzuführen, sollte es zu weiteren Angriffen kommen. Wenige Wochen später beschwor er zudem das Szenario eines „realen Kriegs“ infolge zukünftiger Eskalationen im Cyberraum.[2]

„DIE INTERNATIONALE KOOPERATION BEI DER STRAFVERFOLGUNG HINKT DEN ENTWICKLUNGEN HINTERHER.“

Hier zeigt sich, dass kriminelle Cyberoperationen nicht nur erheblichen gesellschaftlichen Schaden anrichten, sondern auch zu einer ernstzunehmenden Gefahr für den internationalen Frieden werden können. Dies gilt insbesondere für Angriffe auf digitale Systeme, die von nichtstaatlichen Akteuren in erpresserischer Absicht durchgeführt werden.

DIE GRENZEN ZWISCHEN POLITIK UND KRIMINALITÄT VERSCHWIMMEN

Mehrere Faktoren erhöhen die Gefahr einer Eskalation, die mit dieser Form von Cyberkriminalität einhergeht. Erstens ist Cyberkriminalität durch wachsende Arbeitsteilung und Konkurrenz gekennzeichnet. Es gibt Anbieter, die spezialisierte Server zur Verfügung stellen; andere handeln mit Sicherheitslücken oder vermieten einsatzfertige Schadprogramme. Die Konkurrenz um „Kunden“ erschwert zunehmend die Eskalationskontrolle. Denn Cyberkriminelle bedienen im Zweifel auch risikobereite Abnehmer, die größtmöglichen Schaden anrichten wollen oder zumindest in Kauf nehmen. Zweitens ist es nicht immer möglich,

zwischen kriminellen Ransomware-Attacken und politisch motivierten Sabotageakten zu unterscheiden. In beiden Fällen werden kritische Daten im Zielsystem verschlüsselt und so der Zugriff auf diese blockiert. Dazu trägt drittens auch bei, dass einige Staaten strategische Kooperationen mit kriminellen Gruppen betreiben, um politisch motivierte Cyberattacken zu verschleiern. So können zwischenstaatliche Ansätze der Regulierung unterlaufen und die Verantwortung für Angriffe glaubwürdiger abgestritten werden.

„EIN NEUES REGELWERK MUSS KOOPERATIONS-LÜCKEN SCHLIESSEN UND MISSBRAUCH VERHINDERN."

Die internationale Kooperation bei der Strafverfolgung von Cyberkriminalität hinkt diesen Entwicklungen weitgehend hinterher. Dies hat zur Folge, dass angegriffene Unternehmen ihre Verteidigung selbst in die Hand nehmen oder sogar private Sicherheitsfirmen damit beauftragen, gegen kriminelle Infrastrukturen vorzugehen. Allerdings ist die Gefahr groß, dass durch solche „Hack-Backs" wiederum unbeteiligte Dritte zu Schaden kommen.

AUF DEM WEG ZU EINEM NEUEN REGELWERK?

Wirksamere internationale Maßnahmen gegen Cyberkriminalität würden daher einen wichtigen Beitrag zum internationalen Frieden leisten. Zumal die im VN-Kontext vereinbarten Normen verantwortlichen Staatenverhaltens Cyberkriminalität bislang nur indirekt behandeln. Vor diesem Hintergrund ist es grundsätzlich zu begrüßen, dass das auf Initiative Russlands einberufene Ad-Hoc-Komitee der VN ab Januar 2022 über einen internationalen Vertrag berät, mit dem die Kooperation gegen Cyberkriminalität gestärkt werden soll.

Der bereits vorliegende russische Vertragsentwurf ist indes aus mehrfacher Hinsicht problematisch.[3] Erstens werden Straftatbestände im Cyberraum nur sehr vage umschrieben, sodass Kriminalitätsbekämpfung in diesem Bereich auch politisch missbraucht werden kann. Fehlende Verweise auf Menschenrechtsstandards legen nahe, dass es hier primär um die Legitimierung von Internetzensur und Überwachung geht. So wird die russische Initiative selbst zu einem Risiko für den (gesellschaftlichen) Frieden. Zweitens lässt der Entwurf keinen direkten grenzüberschreitenden Zugriff auf die Daten von Internetprovidern zu – anders etwa als die Budapest-Konvention des Europarats. Sie ist das erste völkerrechtlich bindende Abkommen im Bereich Cyberkriminalität, dem auch mehr als 20 nichteuropäische Staaten angehören. Demgegenüber wäre der russische Entwurf ein Rückschritt, denn im Zeitalter von Clouddiensten sind die Spuren von Cyberkriminalität so schnell verwischt, dass klassische Rechtshilfeersuchen oft kaum mehr Aussicht auf Erfolg haben.

Allerdings gibt es ohne Zweifel Defizite und Schutzlücken, die dringend behoben werden müssen. Das betrifft zum Beispiel den globalen Handel mit Überwachungs- und Hacking-Tools. Dieser wird von vielen Staaten bislang kaum unterbunden, obwohl mit entsprechenden Tools im Ausland Straftaten begangen werden. Zudem leidet die internationale Strafverfolgung darunter, dass insbesondere Länder im Globalen Süden zu wenig technische und finanzielle Kapazitäten und Expertise besitzen, um grenzüberschreitend kooperieren und Zugriff auf ermittlungsrelevante Daten erhalten zu können. Doch gerade

das sollte im Interesse aller Staaten sein, damit nicht immer neue „sichere Häfen“ für Cyberkriminelle entstehen.

EIN BALANCEAKT IST NÖTIG

Die Ausgangslage für Verhandlungen ist kompliziert: Ein neues Regelwerk muss Kooperationslücken schließen, ohne dabei missbräuchlicher Anwendung Tür und Tor zu öffnen. Hierfür sollten zivilgesellschaftliche Akteur*innen aktiv an den Verhandlungen beteiligt werden und die Umsetzung der Vereinbarungen überwachen. Neben einem klaren Bekenntnis zu den Menschenrechten sollte ein neues Abkommen mit bestehenden Kooperationsverpflichtungen kompatibel sein, um bisherige Fortschritte bei der Kriminalitätsbekämpfung nicht zu gefährden. Des Weiteren sollte ein Abkommen gegen Cyberkriminalität die VN-Normen verantwortlichen Staatenverhaltens ergänzen und unterstützen, jedoch keinesfalls schwächen. Beispielsweise indem private Hack-Backs von den Staaten strafrechtlich möglichst einheitlich definiert und sanktioniert werden, wodurch die in den VN-Normen abstrakt umrissenen staatlichen Sorgfaltspflichten konkretisiert würden. Zu guter Letzt müssen die Länder des Globalen Südens besser unterstützt werden, damit diese sich an transnationalen Ermittlungsinitiativen beteiligen können. Nur wenn Staaten aus allen Weltregionen Vorteile sehen, kann ein neues globales Abkommen entstehen, das einen wirksamen Beitrag zum Friedensschutz leistet.

ENDNOTEN

1 United Nations General Assembly 2021. Resolution 75/282 – Countering the Use of Information and Communications Technologies for Criminal Purposes, https://undocs.org/en/A/RES/75/282.

2 The White House 2021. Remarks by President Biden, 27.07.2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/27/remarks-by-president-biden-at-the-office-of-the-director-of-national-intelligence.

3 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.

ÜBER DIE AUTOR*INNEN

Dr. Mischa Hansel ist wissenschaftlicher Mitarbeiter und Leiter des Forschungsschwerpunkts „Internationale Cybersicherheit“ am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH).
Dr. Jantje Silomon ist wissenschaftliche Mitarbeiterin am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH).

ÜBER DAS PROJEKT

Dieser Policy Brief ist im Rahmen des Forschungsschwerpunkts „Internationale Cybersicherheit“ entstanden, der 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:
Hamburg | Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke

DOI: https://doi.org/10.25592/ifsh-policy-brief-0721

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