MUN-SH

MUN-SH 2025
Sicherheitsrat

Cyberkriminalität und internationale Sicherheit

Zusammenfassung

Cyberkriminalität ist eine wachsende Bedrohung für Einzelpersonen und die globale Sicherheit. Durch Hacking, Datendiebstahl und Angriffe auf kritische Infrastruktur können Cyberkriminelle ganze Volkswirtschaften destabilisieren. Die internationale Gemeinschaft steht vor der Herausforderung, den Cyberspace zu regulieren und Menschenrechte zu schützen. Die Vereinten Nationen haben bereits Maßnahmen ergriffen, um internationale Zusammenarbeit zu fördern und Regeln für staatliches Verhalten im digitalen Raum zu entwickeln.

Die von der UN-Generalversammlung beauftragte Gruppe der Regierungs Expert*innen (GGE) zur Förderung des verantwortungsvollen staatlichen Handelns im Cyberspace im Kontext der internationalen Sicherheit hat in ihrem Bericht 2021 bestätigt, dass das Völkerrecht auch im Cyberspace gilt und betont die staatliche Verantwortung zur Verhinderung schädlicher Cyber-Aktivitäten. Gleichzeitig wurde die Bedeutung von vertrauensbildenden Maßnahmen und der Unterstützung von Entwicklungsländern hervorgehoben. Die Offene Arbeitsgruppe (OEWG) für Cyberkriminalität bietet eine Plattform, auf der insbesondere Entwicklungsländer an der Festlegung internationaler Normen für den Cyberspace beteiligt sind. Auch Organisationen wie die Internationale Fernmeldeunion (ITU) und das Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC) tragen dazu bei, Länder bei der Sicherung ihrer digitalen Infrastruktur zu unterstützen.

Das Budapester Übereinkommen ist der umfassendste internationale Vertrag zur Bekämpfung von Cyberkriminalität. Es gibt also bereits große Bemühungen, den Cyberspace international zu regulieren. Doch einige Länder verfolgen eigene Prioritäten und betonen die staatliche Souveränität im Cyberspace. Beobachter*innen sagen, dass ein globaler Rechtsrahmen zur Bekämpfung von Cyberkriminalität notwendig ist. Dabei steht vor allem die technologische Unterstützung und internationale Kooperation im Mittelpunkt, um Staaten weltweit zu stärken und die wachsenden Bedrohungen im digitalen Raum effektiv zu bekämpfen.

Punkte zur Diskussion

— Wie kann ein globaler Rechtsrahmen zur Bekämpfung von Cyberkriminalität etabliert werden, insbesondere im Hinblick auf die Zusammenarbeit zwischen Ländern mit unterschiedlichen politischen Systemen?

— Wie können klare Mechanismen zur Zurechenbarkeit von Cyber-Angriffen entwickelt werden, um sicherzustellen, dass Staaten für ihre Handlungen im Cyberspace zur Rechenschaft gezogen werden?

— Welche Maßnahmen sind erforderlich, damit Entwicklungsländer in der Lage sind, sich gegen komplexe Cyber-Bedrohungen zu verteidigen?

— Wie kann die internationale Gemeinschaft effektiver gegen Cyberterrorismus und die Bedrohung durch nichtstaatliche Akteure im Cyberspace vorgehen?

— Wie können bestehende internationale Normen und Verträge aktualisiert oder erweitert werden, um neuen Formen von Cyberkriminalität und staatlich gesponserten Cyber-Angriffen gerecht zu werden?

Einleitung

In unserer zunehmend digitalen Welt ist die **Cyberkriminalität** zu einer erheblichen Bedrohung sowohl für den Einzelnen als auch für die globale Sicherheit geworden. Von Hacking und Datendiebstahl bis hin zu groß angelegten Angriffen auf kritische Infrastruktur – Cyberkriminelle haben die Möglichkeit, Volkswirtschaften, Regierungen und Gesellschaften zu destabilisieren. Angesichts dieser wachsenden Bedrohungen steht die internationale Gemeinschaft vor der Herausforderung, den Cyberspace zu regulieren, Sicherheit zu gewährleisten und gleichzeitig die Menschenrechte zu schützen. Organisationen wie die Vereinten Nationen haben Schritte unternommen, um dieses Problem anzugehen, aber der globale Charakter der Cyberkriminalität erfordert Zusammenarbeit und robuste Rahmenwerke, um Frieden und Sicherheit in einer vernetzten Welt zu erhalten.

Hintergrund und Grundsätzliches

Die Cyberkriminalität als globale Bedrohung hat parallel zur rasanten Entwicklung des Internets und der digitalen Technologien zugenommen. Im späten 20. Jahrhundert wurden Regierungen, Industrien und Institutionen stärker miteinander vernetzt, und diese digitale Expansion öffnete die Tür für neue Formen der Kriminalität und Kriegsführung. Frühe Cyber-Angriffe richteten sich in erster Linie gegen Einzelpersonen und kleine Netzwerke, aber in den 2000er Jahren entwickelte sich die Cyberkriminalität zu einem strategischen Instrument in internationalen Konflikten und zur Manipulation für politische Zwecke.

Cyberkriminalität umfasst kriminelle Handlungen, die durch oder gegen Computer und Netzwerke verübt werden. Dazu gehören Daten-Diebstahl, Hacking, Identitätsbetrug, sowie Verbreitung von Schadsoftware und Phishing.

Eines der frühesten Beispiele für die Beeinflussung geopolitischer Konflikte durch Cyberkriminalität war der Cyber-Angriff auf Estland im Jahr 2007, der sich gegen die Regierung, Banken und Medien des Landes richtete und die digitale Infrastruktur des Landes wochenlang lahm legte.

Kritische Infrastrukturen sind jene Einrichtungen, Systeme und Dienstleistungen, die für das Funktionieren einer Gesellschaft und Wirtschaft von zentraler Bedeutung sind. Dazu gehören Bereiche wie Energieversorgung, Wasser, Verkehr, Gesundheitswesen, Telekommunikation, Finanzwesen sowie staatliche Institutionen.

Staatliche Geheimdienste setzen heute fortschrittliche Cyber-Tools ein, um fremde Systeme zu infiltrieren, geheime Informationen zu stehlen und **kritische Infrastrukturen** zu stören. So gab es beispielsweise 2010 einen meist den USA und Israel zugeschriebenen Angriff auf iranische Nuklearanlagen, wodurch das iranische Atom-

programm erheblich beeinträchtigt wurde. Dies machte deutlich, dass Cyber-Angriffe in Konflikten eingesetzt werden können und sich auf die nationale Sicherheit und die internationalen Beziehungen auswirken.

Auf gesellschaftlicher Ebene ist die Cyberkriminalität zu einer großen Bedrohung für die globale Stabilität geworden. Regierungen und nichtstaatliche Akteure nutzen Cyber-Tools nicht nur zur Spionage, sondern auch zur Manipulation von Wahlen, zur Destabilisierung von Volkswirtschaften und zur Verbreitung von Desinformationen. Cyberoperationen können so politische Systeme schwächen und internationalen Unfrieden stiften, ohne dass traditionelle militärische Kräfte eingesetzt werden müssen. Diese Entwicklungen haben Cyberkriminalität zu einem zentralen Thema der internationalen Sicherheitspolitik gemacht.

Server | Quelle: CC, Mark Seery

Aktuelles

In den letzten Jahren haben die Vereinten Nationen die Bedrohung der globalen Sicherheit durch Cyberkriminalität erkannt und Maßnahmen ergriffen. Als treibende Kraft in der Förderung von internationaler Zusammenarbeit und Normen für staatliches Verhalten im digitalen Raum spielen sie eine zentrale Rolle.

Die **Gruppe der Regierungs Expert*innen (GGE)** zur Förderung des verantwortungsvollen staatlichen Handelns im Cyberspace im Kontext der internationalen Sicherheit, wurde 2018 durch Resolution 73/266 der Generalversammlung gegründet und hat 2021 einen Bericht ihrer Arbeit vorgelegt. Dieser Bericht bekräftigt, dass das Völkerrecht auch im **Cyberspace** gilt, und betont die Verantwortung der Staaten bei der Verhinderung bösartiger Aktivitäten. Er schlägt freiwillige Normen für verantwortungsvolles staatliches Verhalten, einschließlich des Schutzes kritischer Infrastrukturen und der Verbesserung der Transparenz vor. In dem Bericht werden vertrauensbildende Maßnahmen und der Aufbau von Kapazitäten zur Unterstützung von Entwicklungsländern angeregt. Er betonte auch die internationale Zusammenarbeit bei der Bekämpfung der Cyberkriminalität und die Verbesserung der Rahmenbedingungen für die Zuordnung von Cyber-Angriffen, um die Rechenschaftspflicht und die globale Cyber-Stabilität zu fördern.

Die **Gruppe der Regierungs Expert*innen (GGE)** zur Förderung des verantwortungsvollen staatlichen Handelns im Cyberspace im Kontext der internationalen Sicherheit ist ein von den Vereinten Nationen eingesetztes Gremium aus internationalen Expert*innen, das sich mit Fragen der Cybersicherheit und des verantwortungsvollen staatlichen Verhaltens im digitalen Raum beschäftigt.

Cyberspace bezeichnet den virtuellen Raum, der durch vernetzte Computersysteme, das Internet und digitale Kommunikationstechnologien entsteht.

Die **Offene Arbeitsgruppe (OEWG)** für Cyberkriminalität wurde von den Vereinten Nationen als integrative Plattform für alle Mitgliedsstaaten gegründet, um internationale Diskussionen über Cybersicherheit zu führen.

Die **Internationale Fernmeldeunion (ITU)** ist eine spezialisierte Agentur der Vereinten Nationen, die sich auf die Entwicklung und Standardisierung von Informations- und Kommunikationstechnologien konzentriert. Sie unterstützt Länder weltweit bei der Verbesserung ▼

Die **Offene Arbeitsgruppe (OEWG)** für Cyberkriminalität, die durch Resolution 65/230 der Generalversammlung 2011 ins Leben gerufen wurde, ergänzt die Arbeit der GGE, indem sie eine Plattform für alle UN-Mitgliedsstaaten bietet. Insbesondere Entwicklungsländer erhalten hier die Möglichkeit, an der Erarbeitung von internationalen Normen im Cyberspace mitzuwirken. Dabei stehen Frieden, Stabilität, Kapazitätsaufbau und internationale Zusammenarbeit im Fokus.

Zusätzlich spielt die **Internationale Fernmeldeunion (ITU)** eine wichtige Rolle bei der Unterstützung von Ländern in der Sicherung ihrer digitalen Infrastruktur. Das **Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC)** fördert rechtliche und technische Unterstützung, um nationale Kapazitäten zur Bekämpfung von Cyberkriminalität zu stärken.

Das Budapester Übereinkommen ist der umfassendste internationale Vertrag zur Bekämpfung von Cyberkriminalität. Es schafft eine einheitliche Grundlage für nationale Gesetze, sodass diese miteinander kompatibel sind, und erleichtert so die grenzüberschreitende Zusammenarbeit bei der Verfolgung von Cyberkriminalität. Einige Länder, wie die Mitglieder der Shanghaier Organisation für Zusammenarbeit, setzten jedoch eigene Schwerpunkte und betonen die staatliche Souveränität über den Cyberspace.

Probleme und Lösungsansätze

Ein zentrales Problem ist die Zurechenbarkeit von Cyber-Angriffen, da es oft schwierig ist, Täter eindeutig zu identifizieren. Ohne klare Mechanismen zur Zuordnung können Staaten Angriffe leugnen und sich der Verantwortung entziehen. Eine mögliche Lösung wäre die Einrichtung eines internationalen Gremiums, das unabhängig Cyber-Angriffe untersucht und transparent über die Herkunft solcher Angriffe berichtet. Solche Mechanismen könnten durch technologischen Fortschritt, internationale Kooperation und den Einsatz von forensischen Methoden unterstützt werden.

Um Entwicklungsländer im Kampf gegen Cyberkriminalität zu stärken, ist der Kapazitätsaufbau entscheidend. Viele dieser Länder verfügen nicht über die technischen Ressourcen oder das Fachwissen, um sich gegen komplexe Cyber-Bedrohungen zu verteidigen. Lösungsansätze könnten technische Unterstützung durch internationale Institutionen, Schulungsprogramme und Technologietransfer umfassen. Ebenso könnten Partnerschaften zwischen entwickelten und weniger entwickelten Ländern den Wissenstransfer fördern und die Resilienz gegen Cyber-Angriffe erhöhen.

Außerdem stellt **Cyberterrorismus** eine ernsthafte Gefahr dar, weil nichtstaatliche Akteure gezielt den Cyberspace nutzen, um Terroranschläge zu planen oder wichtige Infrastrukturen zu destabilisieren. Hier sind bessere Mechanismen zur Überwachung und Bekämpfung terroristischer Aktivitäten im Internet notwendig. Internationale Zusammenarbeit von Strafverfolgungsbehörden und Geheimdiensten, verstärkte Informationsaustausche sowie die Entwicklung eines rechtlichen Rahmens, der die strafrechtliche Verfolgung von Cyberterrorist*innen ermöglicht, wären wichtige Schritte.

Zusätzlich sind die bestehenden internationalen Normen und Verträge, wie die Budapester Konvention, nicht ausreichend, um die neuen Formen von Cyberkriminalität und staatlich gesponserten Cyber-Angriffen zu bekämpfen. Um diesen Herausforderungen gerecht zu werden, könnten bestehende Abkommen erweitert werden, um **hybride Kriegsführung** und staatlich geförderte Angriffe besser zu regulieren. Gleichzeitig müssten die Normen klarer definiert und

(Forsetzung) ihrer digitalen Infrastruktur und bei der Förderung von Cybersicherheit. Die ITU spielt eine zentrale Rolle bei der technischen Zusammenarbeit und dem Kapazitätsaufbau, insbesondere in weniger entwickelten Ländern.

Das Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC) ist eine UN-Agentur, die sich mit der Bekämpfung von Drogenhandel, organisierter Kriminalität und Terrorismus beschäftigt. Im Bereich der Cybersicherheit unterstützt das UNODC Staaten durch rechtliche und technische Beratung sowie bei der Schaffung nationaler Kapazitäten zur Bekämpfung von Cyberkriminalität und grenzüberschreitenden Cyber-Bedrohungen.

Cyberterrorismus bezeichnet den Einsatz von Computern und Netzwerken durch terroristische Gruppen oder Einzelpersonen, um Angst zu verbreiten, staatliche oder zivile Infrastrukturen zu sabotieren oder politische Ziele durch Cyber-Angriffe zu erreichen.

Hybride Kriegsführung kombiniert konventionelle militärische ▼

Mechanismen zur Überwachung ihrer Einhaltung geschaffen werden.

Expert*innen zufolge ist ein globaler Rechtsrahmen zur Bekämpfung von Cyberkriminalität notwendig, um die zunehmenden Bedrohungen im digitalen Raum zu bewältigen. Die Herausforderung liegt jedoch darin, dass auf der internationalen Bühne Staaten mit unterschiedlichen politischen Systemen und Prioritäten aufeinandertreffen und koordiniert werden müssen. Diese Unterschiede erschweren die Zusammenarbeit. Eine Lösung könnte das Schaffen eines multilateralen Vertrags unter der Aufsicht internationaler Organisationen sein. Dieser Vertrag sollte flexibel genug sein, um den verschiedenen rechtlichen und kulturellen Ansätzen Rechnung zu tragen und gleichzeitig Mindeststandards für Cybersicherheit festzulegen.

Hinweise zur Recherche

Um die Position Ihres Landes zu ermitteln, sollten Sie zunächst prüfen, ob es Mitglied der Shanghaier Organisation für Zusammenarbeit oder des Budapester Übereinkommens ist. Es lohnt sich außerdem zu recherchieren, ob Ihr Land in den letzten Jahren Ziel von Cyber-Angriffen war oder möglicherweise selbst solche Angriffe unterstützt oder durchgeführt hat. Weiterhin ist es entscheidend, die Kapazitäten Ihres Landes zur Verteidigung seines eigenen Cyberspace zu analysieren. Länder mit geringen Cyber-Fähigkeiten könnten besonderes Interesse an einem Technologietransfer haben. Mit diesen Informationen können Sie die Position Ihres Landes fundiert einschätzen.

(Fortsetzung) Operationen mit unkonventionellen Mitteln wie Cyber-Angriffen, Desinformationskampagnen und wirtschaftlichem Druck, um Gegner*innen zu destabilisieren und ohne offene militärische Konfrontation strategische Ziele zu erreichen.

Inhaltlich stellen die Ergebnisse der Gruppe der Regierungs Expert*innen (GGE) und der Offene Arbeitsgruppe (OEWG), sowie der Shanghai Organisation für Zusammenarbeit und des Budapester Übereinkommens sicherlich die wichtigsten Dokumente dar.

Quellen

Council of Europe: Budapest Konvention. ETS No.185. 2001 — Diese Seite beschreibt das Budapester Übereinkommen, das als erster internationaler Vertrag zur Bekämpfung von Cyberkriminalität gilt. Besonders relevant für Länder, die grenzüberschreitende Cyberkriminalität angehen und eine internationale Zusammenarbeit aufbauen wollen. (Deutsch).

Cooperative Cyber Defence Centre of Excellence: Shanghaier Organisation für Zusammenarbeit . 2021. — Die Seite bietet Informationen zur Shanghaier Organisation für Zusammenarbeit und ihren Aktivitäten im Bereich Cybersicherheit. Wichtige Quelle für Staaten, die alternative Modelle zur Cyber-Regulierung verfolgen. (Englisch).

United Nations Office for Disarmament Affairs: Final Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. A/76/135. 2021. — In diesem Bericht werden die Ergebnisse der UN-Gruppe der Regierungs Expert*innen zu Normen für staatliches Verhalten im Cyberspace festgehalten. Besonders wichtig für die Entwicklung internationaler Cyber-Normen und Regeln. (Englisch).

United Nations Office on Drugs and Crime: Open-ended Intergovernmental Expert Group on Cybercrime. 2021. — Diese Seite beschreibt die Arbeit der offenen Expert*innengruppe zu Cyberkriminalität, die Strategien zur Bekämpfung globaler Cyberverbrechen erörtert. Hilfreich zur Analyse aktueller internationaler Diskussionen. (Englisch).

International Telecommunication Union: ITU Main Page. 2024. — Die ITU spielt eine Schlüsselrolle bei der globalen Cybersicherheit und technischen Standards. Diese Seite bietet umfassende Informationen über Cybersicherheitsinitiativen und die Unterstützung von Staaten. Nützlich, um ITU-Programme im Detail zu verstehen. (Englisch).

United Nations Office on Drugs and Crime: Cybercrime Prevention and Criminal Justice. 2021. — Diese Seite bietet Informationen über die Aktivitäten der UNODC zur Prävention und Bekämpfung von Cyberkriminalität, einschließlich Schulungsprogramme und internationaler Kooperation. Essentiell für Einblicke in internationale Cyberkriminalitätsprävention. (Englisch).

Sicherheitsrat
Gremientext für das Thema
Cyberkriminalität und internationale Sicherheit
Autor*in: Lars Kiehne

Model United Nations Schleswig-Holstein 2025
mun-sh.de

Projektleitung MUN-SH 2025
Tom Bergmann – Carl-Jobst Hülsmann – Frederik Schissler
projektleitung@mun-sh.de

Ein Projekt des Deutsche Model United Nations (DMUN) e.V.
Birkenweg 1, 24235 Laboe