Deutscher Bundestag **Drucksache 19/29615**

19. Wahlperiode 12.05.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Roman Müller-Böhm, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/28426 –

Völkerrecht des Netzes

Vorbemerkung der Fragesteller

Die Vereinten Nationen sind mit dem Inkrafttreten der UN-Charta am 24. Oktober 1945 gegründet worden. Seit dieser Zeit hat sich im Hinblick auf die Digitalisierung ein nie geglaubter Wandel und eine enorme Entwicklung vollzogen. Gerade die Entwicklung des Internets ist zum Zeitpunkt der Gründung der Vereinten Nationen nicht erwartbar oder absehbar gewesen. Entsprechend ist die Digitalisierung bei der Schaffung der rechtlichen Regelungen noch nicht berücksichtigt worden. In der sogenannten Digitalen Agenda 2014–2017 der Bundesregierung (https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda.pdf?__blob=publicationFile&v=3) hieß es noch: „Wir wollen Klarheit über das anwendbare Völkerrecht des Netzes schaffen, um die geltenden Grund- und Freiheitsrechte auch in der digitalen Welt wirksam zu schützen und die Chancen für eine demokratische Teilhabe am weltweiten Kommunikationsnetz zu verstärken.“ Somit wird die Erarbeitung eines „Völkerrechts des Netzes“ festgeschrieben. Vor diesem Hintergrund stellt sich die Frage, was von der Planung geblieben ist oder aber was konkret durchgeführt wurde. Auch für den Bereich der Menschenrechte stellt sich die Frage, wie den neuen Herausforderungen begegnet wird und wie sie verarbeitet werden, insbesondere unter der Bedingung der globalen digitalen Kommunikationsnetze. Auch vor dem Hintergrund des Vertrags des UN-Menschenrechtsrates „UNHRC Resolution on The Promotion, Protection and Enjoyment of Human Rights on the Internet (A/HRC/32/L.20)“, wonach Menschenrechte online wie auch offline Geltung finden, gebietet sich nach Ansicht der Fragesteller eine genaue Überprüfung des derzeitigen Status quo der rechtlichen Ausgestaltung von Verträgen betreffend die digitale Entwicklung.

1. Inwiefern gibt es aus Sicht der Bundesregierung heute ein „Völkerrecht des Netzes“?

Unter dem Begriff „Völkerrecht des Netzes“ lässt sich die Gesamtheit völkerrechtlicher Normen und Rechtsprinzipien verstehen, die Rechte und Pflichten für Völkerrechtssubjekte im und in Bezug auf den Cyberraum begründen. Dazu zählen nach Auffassung der Bundesregierung sowohl allgemeine Regelungen

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Auswärtigen Amts vom 11. Mai 2021 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

des Völkerrechts, die nicht nur, aber auch auf Cybersachverhalte Anwendung finden (beispielsweise grundlegende Bestimmungen der Charta der Vereinten Nationen, VN), als auch „Cyber-spezifische“ völkerrechtliche Regelungen, etwa das Übereinkommen über Computerkriminalität des Europarates vom 23. November 2001, die sogenannte Budapest-Konvention (abrufbar unter https://www.coe.int/de/web/conventions/full-list/-/conventions/rms/090000168 00 8157a).

Mit dem „Völkerrecht des Netzes“ eng verknüpft sind darüber hinaus die Normen und Standards, die nicht den klassischen Völkerrechtsquellen zugeordnet werden können. Dazu gehören unter anderem die nicht rechtlich verbindlichen Normen verantwortungsvollen Staatenverhaltens, wie sie etwa durch die VN-Arbeitsgruppen zu Cyber und Sicherheit („Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security” – GGE und „Open-ended Working Group on developments in the field of information and telecommunications in the context of international security” – OEWG) erarbeitet wurden.

a) Inwiefern bedarf es aus Sicht der Bundesregierung eines „Völkerrechts des Netzes“?

Die internationale Vernetzung ist im Cyberraum so hoch wie in kaum einem anderen Gesellschaftsbereich: Die grenzüberschreitende, enge Verflechtung von Netzwerken, Technologien und Cyberprozessen hat Gesellschaften und Einzelpersonen aus aller Welt näher zusammenrücken lassen und neue Möglichkeiten der Zusammenarbeit eröffnet. Zugleich sind Staat und Gesellschaft zunehmend auf die Funktionsfähigkeit von IT-Infrastrukturen angewiesen. Dies birgt auch Risiken. Nach Einschätzung der Bundesregierung ist das Völkerrecht als rechtlich verbindlicher normativer Rahmen für das Verhalten von Staaten und anderen Völkerrechtssubjekten essentiell, um die Chancen und Risiken des Cyberraums als globales Phänomen zum Wohle aller in ein Gleichgewicht zu bringen und zu regeln.

b) Welche Maßnahmen hat die Bundesregierung seit 2017 ergriffen, um ein „Völkerrecht des Netzes“ zu schaffen?

Die Bundesregierung vertritt die Auffassung, dass das geltende Völkerrecht grundsätzlich auch auf Cyber-Sachverhalte Anwendung findet. Da der Cyberraum kein rechtsfreier Bereich ist, sieht die Bundesregierung keinen Bedarf einer umfassenden Neuregelung auf Völkerrechtsebene. Gleichwohl bringt sich die Bundesregierung in die laufende internationale Diskussion ein, wie das geltende Völkerrecht, beispielsweise die VN-Charta, das im Wesentlichen vor dem Cyberraum entstanden ist, Anwendung findet. Die Bundesregierung setzt sich auf VN-Ebene in den Arbeitsgruppen GGE und OEWG kontinuierlich und nachdrücklich dafür ein, dass die Rolle des Völkerrechts im Cyberraum gestärkt wird sowie die nicht rechtlich verbindlichen Normen verantwortungsvollen Staatenverhaltens im Cyberraum weiterentwickelt und ausdifferenziert werden.

Auch außerhalb des VN-Rahmens trägt die Bundesregierung zur Stärkung des Völkerrechts im Cyberraum bei. So hat sie am 5. März 2021 ein Positionspapier zur Anwendung des Völkerrechts im Cyberraum (abrufbar unter https://www.auswaertiges-amt.de/de/aussenpolitik/themen/internationales-recht/voelkerrecht-aktuelle-dokumente/2221614) veröffentlicht, das die Anwendung des geltenden Völkerrechts, darunter insbesondere auch der VN-Charta und des humanitären Völkerrechts, im Kontext transnationaler Cyberoperationen bestätigt. Das Papier erläutert ferner die Position der Bundesregierung zu den Modalitäten der Anwendung einer Auswahl völkerrechtlicher Kernnormen im Cyber-

Kontext. Hierzu zählen das Prinzip staatlicher Souveränität, das völkerrechtliche Interventionsverbot, das Gewaltverbot sowie wichtige Bestimmungen des humanitären Völkerrechts. Darüber hinaus setzt sich das Papier mit Rechtsfragen der Zurechnung sowie mit staatlichen Reaktionsmöglichkeiten auf cyberbezogene Völkerrechtsverletzungen auseinander. Das Papier fungiert als deutscher Beitrag zu den laufenden internationalen Diskussionen, fördert das Verständnis hinsichtlich der deutschen Rechtsposition und trägt somit zu Transparenz und Rechtssicherheit bei. Es untermauert damit auch Deutschlands Bekenntnis zu einer völkerrechtsbasierten Cyber-Außenpolitik.

Darüber hinaus hat sich die Bundesregierung für die Stärkung und Weiterentwicklung spezifischer Rechtsinstrumente zur Regelung von Cyber-Sachverhalten eingesetzt, darunter etwa im Bereich der Cyberkriminalität (Übereinkommen über Computerkriminalität des Europarates vom 23. November 2001, sog. Budapest-Konvention).

Die Bundesregierung unterstützt die Verhandlungen eines Zweiten Zusatzprotokolls zur Budapest Konvention. Dieses Protokoll, für das der Rat der Europäischen Kommission im Juni 2019 ein Verhandlungsmandat erteilt hat, dient einer verstärkten internationalen Zusammenarbeit bei der Sicherung elektronischer Beweismittel im Strafverfahren zum Zwecke einer effektiven Verfolgung von Computerkriminalität.

Darüber hinaus setzt sich die Bundesregierung derzeit für die Entwicklung eines verbindlichen völkerrechtlichen Rechtsinstruments für künstliche Intelligenz (KI) im Ad-hoc-Ausschuss des Europarats für künstliche Intelligenz (CAHAI) ein.

c) Wenn ja, wie und in welcher Form kann ein „Völkerrecht des Netzes“ in der derzeitigen völkerrechtlichen Ordnung eingesetzt werden?

Nach Auffassung der Bundesregierung ist das „Völkerrecht des Netzes“ ein untechnischer Sammel- und Oberbegriff für eine Vielzahl völkerrechtlicher Normen mit Relevanz für und Anwendbarkeit auf Cyber-Sachverhalte, die bereits Teil der existierenden Völkerrechtsordnung sind. Auf die Antworten zu den Fragen 1 bis 1b wird verwiesen.

2. Inwiefern verfolgt die Bundesregierung derzeit die Schaffung eines „Völkerrechts des Netzes“?

   a) Seit wann und mit welchen Maßnahmen verfolgt die Bundesregierung seit 2017 die Schaffung eines „Völkerrechts des Netzes“?

   b) Welche Erfolge konnten bislang erreicht werden?

   c) Welche Maßnahmen waren nicht erfolgreich, und woran scheiterten sie?

Die Fragen 2 bis 2c werden gemeinsam beantwortet.

Auf die Antwort zu Frage 1b wird verwiesen.

3. Wie sieht ein „Völkerrecht des Netzes“ aus Sicht der Bundesregierung derzeit konkret aus?

Auf die Antwort zu Frage 1 wird verwiesen.

4. Erwartet die Bundesregierung, dass einflussreiche Staaten ein „Völkerrecht des Netzes“ aus machtpolitischen Interessen verhindern, und wenn ja, inwiefern?

Aus Sicht der Bundesregierung findet das geltende Völkerrecht bereits im Cyberraum Anwendung. Insoweit wird auf die Antwort zu Frage 1 verwiesen. Gleichwohl stellen einige Staaten die umfassende Anwendbarkeit des Völkerrechts oder wichtiger Teilbereiche in Abrede, und es bestehen Forderungen nach der Verabschiedung einer umfassenden, neuen völkerrechtlichen Konvention zur Regelung des Cyberraums. Nach Einschätzung der Bundesregierung beruhen diese Positionen auf unterschiedlichen Motiven, darunter auch dem Bestreben, ein Agieren im Cyberraum nicht an rechtlich verbindlichen Verhaltensnormen auszurichten.

5. Welche Rolle spielen aus Sicht der Bundesregierung die Menschenrechte in einem solchen „Völkerrecht des Netzes“?

Die in verschiedenen internationalen Verträgen sowie im Völkergewohnheitsrecht verbrieften Menschenrechte sind online wie offline zu gewähren. Sie schützen den Einzelnen in Bezug auf seine Teilnahme am Internet und sein Handeln im Cyberraum, sie schützen ihn aber auch vor Cyber-basierten Übergriffen. Für die Freiheit der Internetkommunikation zentral sind internationale Verbürgungen der Meinungsfreiheit, wie sie insbesondere in Artikel 19 Absatz 2 des Internationalen Pakts über bürgerliche und politische Rechte (IPbpR) oder Artikel 10 der Europäischen Menschenrechtskonvention (EMRK) zu finden sind. Artikel 19 Absatz 2 IPbpR verweist ausdrücklich auf die Ausübung des Rechts auf Meinungsfreiheit „durch Mittel eigener Wahl“. Sowohl Artikel 19 Absatz 2 IPbPR als auch Artikel 10 EMRK schützen (aktive) Meinungsäußerungen im Internet, darunter etwa das Hochladen von Internetinhalten, als auch die (passive) Rezeption von Inhalten über das Internet. Auf der anderen Seite steht das Recht auf Privatheit, verbrieft insbesondere in Artikel 17 IPbpR und Artikel 8 EMRK. Schutzgut ist hier unter anderem die private Kommunikation. Staatliche Kontrolle über private Internetnutzung und deren Inhalte können daher einen Eingriff in die Privatsphäre darstellen. Darüber hinaus können auch andere Menschenrechtsgarantien Anwendung auf Cyber-Sachverhalte finden. Ob Eingriffe in den Schutzbereich menschenrechtlicher Garantien gerechtfertigt sind und Menschenrechte konkret verletzt sind, ist dabei auch im Kontext des Internets bzw. des Cyberraums eine Frage des Einzelfalls.

6. Inwiefern kann aus Sicht der Bundesregierung ein „Völkerrecht des Netzes“ die Integrität des Netzes legitim und effektiv schützen?

Unter der „Integrität des Netzes“ kann verstanden werden, dass das Netz frei ist von Nutzungen für rechtswidrige Zwecke, aber auch, dass es funktionsfähig ist. Völkerrechtliche Normen begründen Rechte und Pflichten von Staaten und anderen Völkerrechtssubjekten in Bezug auf den Cyberraum. Sie verbieten Übergriffe auf Cyber-Infrastrukturen und -prozesse fremder Staaten, aber auch auf nicht cyber-bezogene Güter fremder Staaten unter Nutzung von Cyber-Kapazitäten, sofern dadurch beispielsweise die Souveränität eines fremden Staates verletzt, in die inneren Angelegenheiten („domaine réservé“) eines fremden Staates mit Zwang eingegriffen (Interventionsverbot) oder das völkerrechtliche Gewaltverbot verletzt wird. Die Integrität des Internets und des Cyberraums wird durch das Völkerrecht darüber hinaus auch dadurch geschützt, dass in einem völkerrechtlichen Instrument wie der Budapest-Konvention strafrechtliche Maßnahmen zur Bekämpfung von Handlungen gegen die Vertrau-

lichkeit, Unversehrtheit und Verfügbarkeit von Computersystemen, Netzen und Computerdaten sowie des Missbrauchs solcher Systeme, Netze und Daten vorgesehen werden.

7. Welche Wirkung hat die Digitalisierung aus Sicht der Bundesregierung auf das Völkerrecht?

Die Digitalisierung ist ein vorrechtlicher, faktischer gesellschaftlicher Vorgang, der als solcher das existierende Völkerrecht und dessen Grundstrukturen (wie andere neuere gesellschaftliche Entwicklungen auch) nicht zu ändern oder in seiner Normativität zu beeinflussen vermag. Gleichwohl schafft die Digitalisierung das Erfordernis, existierendes Völkerrecht auf neue Sachverhalte im Cyber-Kontext anzuwenden und existierende völkerrechtliche Bestimmungen im Lichte der Besonderheiten des Cyberraums (hohes Maß grenzüberschreitender Verflechtungen, Immaterialität von Cybervorgängen, Anonymität, etc.) auszulegen. In einzelnen Bereichen ergab oder ergibt sich überdies Anlass und Raum für neue Regelungen, wie etwa bei der Koordinierung staatlicher Maßnahmen gegen die Cyberkriminalität mit der Budapest-Konvention, oder um spezifischen Risiken für Menschenrechte, Rechtsstaatlichkeit und Demokratie zu begegnen.

8. Hat die Bundesregierung anlässlich ihrer Zielvorstellungen für eine Weiterentwicklung des „Völkerrechts des Netzes“ den transnationalen Charakter des Internets völkerrechtlich betrachtet, und wenn ja, mit welchem Ergebnis?

Das für die geltende Völkerrechtsordnung zentrale Prinzip der Territorialität spielt nach Auffassung der Bundesregierung auch im Cyber-Kontext eine wichtige Rolle. Da sich alle Cyberaktivitäten letztendlich auf Handlungen von Menschen zurückführen lassen, die physische Infrastrukturen nutzen, ist der Cyberraum keine „deterritorialisierte“ Größe. Unter anderem gibt es nach Sicht der Bundesregierung völkerrechtlich auch keine eigenständigen, von den physischen Grenzen eines Staates abweichenden „Cybergrenzen“, die den territorialen Geltungsbereich der staatlichen Souveränität einschränkten oder unberücksichtigt ließen. Gleichwohl erkennt die Bundesregierung, dass der Cyberraum durch ein besonders hohes Maß grenzüberschreitender Interdependenzen zwischen Infrastrukturen und Kommunikationsprozessen gekennzeichnet ist. Dies erschwert die Abgrenzung von Hoheitsrechten einzelner Staaten in Bezug auf Cybervorgänge. Erschwert ist darüber hinaus die Zurechenbarkeit eines konkreten Verhaltens zu staatlichen wie nicht-staatlichen Akteuren. Die Bundesregierung setzt sich dafür ein, das Verständnis der Anwendung des geltenden Völkerrechts auf Cyber-Sachverhalte weiter zu fördern und auszubauen.

9. Sieht die Bundesregierung Anwendungsmöglichkeiten der Blockchain-Technologie, Algorithmen und Smart Contracts im Völkerrecht, und wenn ja, inwiefern?

Technologien im Sinne der Fragestellung können in den Anwendungsbereich existierender völkerrechtlicher Regelungen fallen, etwa im Bereich der Menschenrechte, wenn sie durch Staaten etwa zum Zweck der Strafverfolgung eingesetzt werden, oder im Bereich des Humanitären Völkerrechts, wenn KI-Technologie in der Kriegsführung eingesetzt wird. Davon abgesehen wird das gegenwärtige (Völker-)Recht teilweise nicht als ausreichend angesehen, um die

Chancen und Risiken neuartiger Technologien im Bereich künstliche Intelligenz umfassend zu regulieren. Auf die Antwort zu Frage 1b wird verwiesen.

10. Welche Staaten haben aus Sicht der Bundesregierung den größten Einfluss auf die Fortentwicklung eines digitalen Völkerrechts?

11. Welcher Staat ist aus Sicht der Bundesregierung ein Treiber auf dem Gebiet des digitalen Völkerrechts?

Die Fragen 10 und 11 werden gemeinsam beantwortet.

Als „Treiber auf dem Gebiet des digitalen Völkerrechts“ bzw. Staaten mit einem besonderen Einfluss können Staaten angesehen werden, die sich besonders engagiert an aktuellen Diskussionen zur Anwendung des Völkerrechts im Cyberraum und zu verantwortungsvollem Staatenverhalten beteiligen. Dazu gehören einige der 25 Staaten, die in der GGE vertreten sind, darunter Deutschland, und die in diesem Rahmen seit langem an der Konkretisierung des völkerrechtlichen Rahmens für verantwortliches Staatenverhalten im Cyberraum intensiv mitwirken. Darüber hinaus haben eine Reihe von Staaten in letzter Zeit nationale Positionspapiere zur Anwendung des Völkerrechts im Cyberraum vorgelegt oder sich in verschiedenen Kontexten zu dieser Thematik geäußert, darunter Australien, Estland, Finnland, Frankreich, Iran, Israel, Neuseeland, Niederlande, die Vereinigten Staaten von Amerika und die Bundesrepublik Deutschland.

12. Besteht aus Sicht der Bundesregierung aufgrund der Digitalisierung Anpassungsbedarf aktueller völkerrechtlicher Verträge?

    a) Wenn ja, inwiefern?

       Um welche Verträge handelt es sich dabei konkret?

    b) An welcher Stelle sollten die konkreten Verträge geändert werden und inwiefern?

Die Fragen 12 bis 12b werden gemeinsam beantwortet.

Aus Sicht der Bundesregierung ist das geltende Völkerrecht, darunter insbesondere auch wichtige völkerrechtliche Verträge wie die VN-Charta, internationale Menschenrechtsverträge oder die Genfer Konventionen zum Humanitären Völkerrecht, online wie offline anwendbar. Fragen der Anwendung dieser Verträge, die zeitlich vor der Verbreitung digitaler Technologien entstanden sind, in Bezug auf Cyber-Sachverhalte sind grundsätzlich mit den etablierten, in Artikel 31 ff. des Wiener Übereinkommens über das Recht der Verträge vom 23. Mai 1969 kodifizierten Methoden der Auslegung völkerrechtlicher Verträge zu lösen. Zu den Bemühungen, Klarheit darüber zu schaffen, wie bestehende Regeln auf Cyber-Sachverhalte anzuwenden sind, wird auf Antwort zu Frage 1b verwiesen.

13. Sieht die Bundesregierung die Notwendigkeit, eine eigenständige Kodifikation der Regelungen zu schaffen, die die Digitalisierung im Völkerrecht berücksichtigen?

Die Bundesregierung verfolgt nicht den Gedanken eines eigenständigen umfassenden völkerrechtlichen Vertrages zur Regelung des Cyberraums oder der Digitalisierung. Es würde der Eindruck entstehen, der Cyberraum sei ungeregelt. Letzteres ist nicht der Fall, da das existierende Völkerrecht auch auf den Cyber-

raum Anwendung findet. Auf die Antworten zu den Fragen 1 und 12 wird verwiesen.

14. Sieht die Bundesregierung politische Hindernisse, die einer formellen Vertragsveränderung zur Fortentwicklung völkerrechtlicher Verträge zum Zwecke des digitalen Völkerrechts entgegenstehen, und wenn ja, welche?

Aus Sicht der Bundesregierung ergibt sich nicht das Erfordernis einer umfassenden, systematischen Anpassung geltender völkerrechtlicher Verträge im Lichte der faktischen Besonderheiten des Cyberraums; auf die Antworten zu den Fragen 12 und 13 wird verwiesen. Darüber hinaus ist eine Bewertung der politischen Rahmenbedingungen für die konkrete Änderung einzelner völkerrechtlicher Verträge von den Umständen des Einzelfalls abhängig und kann nicht pauschal erfolgen.

15. Inwieweit ist es aus Sicht der Bundesregierung in einer digitalisierten Welt möglich, weltweit Freiheit und Sicherheit in Einklang zu bringen, und inwieweit können völkerrechtliche Regelungen aus Sicht der Bundesregierung dazu zweckdienlich sein?

Die Bundesregierung vertritt die Auffassung, dass Freiheit und Sicherheit in einer digitalisierten Welt keine Gegensätze bilden, sondern sich gegenseitig bedingen. Eine freie Nutzung des Internets ist ohne Gewährleistung der Sicherheit seiner Nutzer nicht möglich. Gleichzeitig ist die Sicherheit des Einzelnen bedroht, wenn seine Freiheitsrechte nicht geschützt werden.

Die Durchsetzung der geltenden Regelungen des Völkerrechts ist eine Grundbedingung für die von der Bundesregierung angestrebte Wahrung und Förderung eines freien, offenen, sicheren und stabilen Cyberraums. Im Einzelnen bestehende Spannungsverhältnisse zwischen Freiheit und Sicherheit im digitalen Raum sind abhängig von den Umständen des Einzelfalls unter Beachtung des geltenden Rechts aufzulösen.

a) Teilt Bundesregierung die Ansicht der Fragesteller, dass das Internet als „globales öffentliches Gut“ betrachtet werden kann?

   Wer ist aus Sicht der Bundesregierung dazu befugt, dieses zu verwalten?

b) Welche Maßnahmen zum Schutz dieses Gutes plant die Bundesregierung?

Die Fragen 15a und 15b werden zusammen beantwortet.

Die Bundesregierung verwendet für die völkerrechtliche Beschreibung des Internets nicht den Begriff „globales öffentliches Gut“. Die Bundesregierung teilt insoweit die im sogenannten Tallinn Manual 2.0, einem Expertendokument zur Anwendung und Auslegung des Völkerrechts im Cyberraum (Michael N. Schmitt/Liis Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyberspace, Cambridge 2017, S. 12), geäußerte Ansicht, dass die Zuerkennung eines völkerrechtlichen Sonderstatus für das Internet im Sinne eines „global common“ den physischen Ursprung und damit die territoriale Radizierung des Cyberraums und seiner Komponenten (insbesondere Personen, die Cyberaktivitäten durchführen, auf dem Territorium eines Staates gelegene Hardware, die für bestimmte Datenverarbeitungsvorgänge genutzt wird, etc.) missachten könnte. Die Annahme eines derartigen Sonderstatus für das Internet könnte da-

mit in Konflikt zu völkerrechtlichen Kernnormen wie dem Prinzip der territorialen Souveränität geraten.

Die Bundesregierung setzt sich für die Achtung der Menschenrechte im Kontext des Internets ein und wendet sich gegen ungerechtfertigte Internetsperren oder „Shutdowns“, gerade wenn diese die legitime politische Arbeit in einem Staat beeinträchtigen oder einzelne Internetnutzer einschüchtern sollen. Mit ihren Maßnahmen zur Klärung der Anwendungsmodalitäten des Völkerrechts im Cyberraum (siehe die Antwort zu Frage 1) trägt die Bundesregierung darüber hinaus dazu bei, Rechtssicherheit bei der Nutzung von Cyberkapazitäten im internationalen Kontext zu schaffen.

16. Gibt es aus Sicht der Bundesregierung eine digitale Souveränität von Staaten?

    a) Wenn ja, woraus ergibt sich diese?

    b) Wenn ja, inwiefern plant die Bundesregierung Maßnahmen zum Schutz dieser Souveränität?

Die Fragen 16 bis 16b werden zusammen beantwortet.

Der völkerrechtliche Grundsatz der staatlichen Souveränität gilt für die Aktivitäten von Staaten im Cyberraum. Staatliche Souveränität bedeutet unter anderem, dass einem Staat das Recht zur Rechtsetzung, zur Rechtsdurchsetzung und Rechtsprechung (Jurisdiktion) sowohl in Bezug auf Personen, die an Cyberaktivitäten beteiligt sind, als auch in Bezug auf die Cyberinfrastrukturen in seinem Hoheitsgebiet (und unter bestimmten Voraussetzungen darüber hinaus) vorbehalten ist. Begrenzt wird dieses Recht nur durch die einschlägigen Regeln des Völkerrechts, einschließlich des humanitären Völkerrechts und der internationalen Menschenrechte. Staatliche Souveränität im Cyberraum bedeutet unter anderem auch, dass die politische Unabhängigkeit eines Staates und sein Territorium gegen (mit Cybermitteln) durchgeführte Übergriffe anderer Staaten geschützt sind. Die Bundesregierung ist der Auffassung, dass Staaten zurechenbare Cyberoperationen, die die Souveränität eines anderen Staates verletzen, völkerrechtswidrig sind.

Die Bundesregierung beobachtet gegen Deutschland bzw. deutsche Interessen sowie auch gegen andere Staaten gerichtete Cybermaßnahmen und prüft bei gegebenem Anlass, ob diese eine Verletzung des völkerrechtlichen Grundsatzes der Souveränität (oder anderer geltender Regeln des Völkerrechts) darstellen. Die Bundesregierung behält sich vor, gegen Cybermaßnahmen, die gegen Völkerrecht verstoßen, im Einklang mit den maßgeblichen völkerrechtlichen Regeln (z. B. Recht der Gegenmaßnahmen, Selbstverteidigungsrecht) zu reagieren.

17. Wer übt aus Sicht der Bundesregierung im Internet „virtuelle Kontrolle“ aus, und woraus ergibt sich die jeweilige Kontrollbefugnis?

Bei dem Begriff der „virtuellen Kontrolle“ handelt es sich nicht um einen allgemein gebräuchlichen oder gar definierten Begriff; im Übrigen ist der Begriffsteil der „Kontrolle“ mehrdeutig. Soweit hiermit rechtlich verfasste Kontrolle im Sinne staatlicher Hoheitsgewalt gemeint ist, ist darauf hinzuweisen, dass die Staaten gemäß ihrer jeweiligen Souveränität Hoheitsgewalt über die physischen bzw. physisch zuordenbaren Komponenten und Handlungen im Cyberraum (z. B. Hardware, auf der ein Internetinhalt abgespeichert ist, Schnittstellen/Knotenpunkte, über die bestimmte Internetinhalte „transportierende“ elektrische Impulse verlaufen) sowie über Personen, die an Cybervorgängen beteiligt

sind, ausüben. Anknüpfungspunkte sind dabei aus völkerrechtlicher Sicht die Regelungen über die Gebietshoheit bzw. sog. Jurisdiktion (Zuständigkeit für Rechtssetzung, Rechtsdurchsetzung und Rechtsprechung in Bezug auf einen konkreten Sachverhalt).

Es ist Aufgabe der staatlichen Behörden, sicherzustellen, dass auch nichtstaatliche Entitäten und Personen, die im Internet tätig sind bzw. Technologien und/oder Inhalte bereitstellen, im Einklang mit den jeweils für sie geltenden rechtlichen Bestimmungen handeln.

18. Sollte eine Kontrollbefugnis hinsichtlich einer „virtuellen Kontrolle“ aus Sicht der Bundesregierung völkerrechtlich geregelt sein, und wenn ja, inwiefern?

Das Völkerrecht regelt mit seinen Bestimmungen zur Begründung und Abgrenzung staatlicher Gebietshoheit bzw. Jurisdiktion die Ausübung von staatlicher Hoheitsmacht in Bezug auf den Cyberraum; insoweit wird auf die Antwort zu Frage 17 verwiesen. Auch mit Blick auf den transnationalen Charakter des Cyberraums kommt es hinsichtlich der Abgrenzung staatlicher Regelungs- und Rechtsdurchsetzungszuständigkeiten auf den konkreten Einzelfall an. Die Bundesregierung verfolgt keine Pläne zur allgemeinen Neuregelung des Völkerrechts der staatlichen Jurisdiktion mit Blick auf den Cyberbereich.

19. Welche Staaten sind der Bundesregierung bekannt, die Einfluss auf die Freiheit des Internets nehmen und versuchen Einfluss auf den Internetverkehr zu nehmen?

    a) Plant die Bundesregierung, dagegen Maßnahmen zu unternehmen, und wenn ja, welche?

    b) Welche Probleme ergeben sich aus Sicht der Bundesregierung daraus?

    c) Inwieweit kann aus Sicht der Bundesregierung durch das derzeitige Völkerrecht Einfluss darauf genommen werden?

Die Fragen 19 bis 19c werden zusammen beantwortet.

Eine systematische Erfassung von Staaten, die Einfluss auf die Freiheit des Internets und auf den Internetverkehr nehmen, findet nicht statt (s. auch Antwort der Bundesregierung zu Frage 3 der Kleinen Anfrage der Fraktion der FDP, Bundestagsdrucksache 19/18902). Davon abgesehen beobachtet die Bundesregierung mit Sorge einen anhaltenden globalen Trend der Einschränkung von Freiheitsrechten im Internet, der sich unter dem Vorwand der Bekämpfung der globalen Corona-Pandemie zum Teil noch verstärkt hat. Die Nichtregierungsorganisation Freedom House hat hierzu eine umfassende Studie „Freedom on the Net 2020“ veröffentlicht, abrufbar unter https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow. Beschränkungen der Freiheit des Internets haben zahlreiche negative Auswirkungen u. a. sozialer, wirtschaftlicher und menschenrechtlicher Natur. Insbesondere vulnerable und marginalisierte Gruppen, die für soziale Kontakte und Informationen auf das Internet angewiesen sind, können hierdurch stärker betroffen sein.

Die Verteidigung eines freien, offenen, sicheren und stabilen Cyberraums ist Leitlinie deutscher Cyberaußenpolitik. In diesem Rahmen ergreift die Bundesregierung eine Vielzahl von Maßnahmen auf der nationalen, europäischen und internationalen Ebene. Beispielsweise thematisiert sie die Beschränkung von Freiheitsrechten online in bilateralen Konsultationen, wirkt mit an internationalen Erklärungen und Resolutionen, z. B. zu sog. Internet Shutdowns, und för-

dert finanziell Projekte zum Schutz und zur Förderung von Menschenrechten online. Im Übrigen wird auf den 14. Bericht der Bundesregierung über ihre Menschenrechtspolitik (abrufbar unter https://www.auswaertiges-amt.de/de/aussenpolitik/themen/menschenrechte/menschenrechtsbericht/2422186) verwiesen.

20. Inwiefern und durch welche Maßnahmen konkret nimmt die Bundesregierung Einfluss auf den Internetverkehr?

Die Bundesregierung setzt sich für ein gemeinsames, freies, offenes, sicheres und stabiles globales Internet ein. Beispielsweise bringt sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) in internationalen Internetstandardisierungsgremien (u. a. der „Internet Engineering Task Force" – IETF) ein und veröffentlicht regelmäßig Empfehlungen für Telekommunikationsanbieter zum sicheren Betrieb des Internets (abrufbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unterneh-men/Weitere_regulierte_Unternehmen/Internet_Service_Provider/Internet-Service-Provider_node.html). Im Übrigen muss sich jeder Anbieter und Nutzer von Produkten und Dienstleistungen in Deutschland, so auch Internetanbieter und -nutzer, an das geltende Recht halten.

21. Inwiefern sieht die Bundesregierung Massenüberwachungsprogramme als Bruch der Menschenrechte im Sinne des Völkerrechts an?

Je nach Begriffsverständnis können bei Programmen im Sinne der Fragestellung entsprechend ihrer Ausgestaltung grund- und menschenrechtlich geschützte Rechtspositionen, etwa das Recht auf Privatheit sowie das Post- und Fernmeldegeheimnis, betroffen sein. Eine Bewertung etwa der Verhältnismäßigkeit entsprechender Maßnahmen kann nur in Betrachtung der Umstände des Einzelfalls erfolgen und nicht pauschal vorgenommen werden.

22. Inwiefern stellt offensives Hacking unter völkerrechtlichen Gesichtspunkten aus Sicht der Bundesregierung ein Problem dar?

Grundsätzlich können nach Auffassung der Bundesregierung Cybermaßnahmen durch Staaten den völkerrechtlichen Grundsatz der Souveränität verletzen, beispielsweise wenn diese zu nicht unerheblichen physischen Auswirkungen und Schäden im Hoheitsgebiet eines anderen Staates oder zu nicht unerheblichen Funktionsbeeinträchtigungen bei Cyberinfrastrukturen führen, die sich im Hoheitsgebiet eines anderen Staates befinden. Cybermaßnahmen können auch gegen das völkergewohnheitsrechtlich geltende und aus Artikel 2 Absatz 1 der Charta der Vereinten Nationen ableitbare Interventionsverbot, das eine Einmischung in die inneren Angelegenheiten (sog. „domaine réservé") eines anderen Staates unter Anwendung von Zwang verbietet, verstoßen. Eine völkerrechtliche Bewertung von Cybermaßnahmen, wie etwa offensives Hacking, ist unter anderem abhängig von der konkreten technischen Vorgehensweise, dem Ziel entsprechender Maßnahmen, ihren Auswirkungen und sonstigen Begleitumständen. Sie ist somit nur im Einzelfall, nicht pauschal vorzunehmen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333