Eine zuverlässige globale Cybermacht: Deutschlands Nationale Sicherheitsstrategie für den Cyberraum

Weber, Valentin

Veröffentlichungsversion / Published Version
Stellungnahme / comment

Empfohlene Zitierung / Suggested Citation:
Weber, V. (2022). *Eine zuverlässige globale Cybermacht: Deutschlands Nationale Sicherheitsstrategie für den Cyberraum.* (DGAP Policy Brief, 32). Berlin: Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V.. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-85174-7

Nr. 32
Oktober 2022

DGAP POLICY BRIEF

Eine zuverlässige globale Cybermacht

Deutschlands Nationale Sicherheitsstrategie für den Cyberraum

Dr. Valentin Weber
Research Fellow,
Programm Technologie
und Außenpolitik

Deutschlands wichtigste Verbündete haben ihre Rollen bei der Gestaltung des Cyberraums definiert. Die USA betrachten sich als demokratische, werteorientierte Cybermacht, die bereit sind, gegen Gegner hart vorzugehen. Großbritannien will als verantwortungsvolle Cybermacht rücksichtsloses Verhalten unterbinden. Frankreich will sich als stabilisierende Kraft böswilligen Akteuren entgegenstellen. Und Deutschland? In seiner ersten Nationalen Sicherheitsstrategie könnte es Ideen für künftige Aktivitäten im Cyberraum entwickeln, indem es den Fokus auf Zuverlässigkeit und die Abstimmung mit Partnern richtet. Dafür sollte die Bundesregierung die im Folgenden genannten Schritte angehen.

– **Länder verteidigen, die sich um deutsche Unterstützung bemühen, und die Kapazitäten für eine solche Hilfe ausbauen.**

– **sich konsequent für eine starke und transparente Cybersicherheit einsetzen, um auch Partner im Ausland zu einem solchen Vorgehen zu bewegen.**

– **klarer auf seine eigenen offensiven Cyberfähigkeiten und seine Bereitschaft verweisen, diese Kapazitäten zu Verteidigungszwecken im Einklang mit dem Völkerrecht einzusetzen.**

– **seine offensiven Cyberfähigkeiten in Krisensituationen auf Ersuchen auch vertrauenswürdigen Partnern zur Verfügung zu stellen.**

EINLEITUNG

Mit dem Einmarsch Russlands in die Ukraine erhält Deutschland die einzigartige Gelegenheit einer Positionierung im globalen Cyberspace. Es reicht nicht mehr aus, bei Cyberoperationen auf die Einhaltung des Völkerrechts zu drängen und den Kapazitätsaufbau weiter voranzutreiben. Derartige allgemeingültige Erklärungen haben für die deutschen Verbündeten vor allem in Krisenzeiten keinerlei Wert. Die deutsche Regierung muss stattdessen eine konkrete Strategie für ihr weiteres Vorgehen entwickeln. Kurzum: Das Land muss sich als (Cyber)-Macht positionieren und von seinem Ruf als unzuverlässiger Partner befreien.

Innerhalb der Allianz der Westmächte hat sich Deutschland stets als vorbildlicher Partner gesehen. Inzwischen vertreten jedoch immer mehr deutsche Politiker*innen die Auffassung, dass das Land aus der Masse hervortreten, eine Führungsrolle übernehmen und angesichts seiner Wirtschaftskraft angemessene Militär- und Sicherheitskapazitäten aufbauen muss. Zu diesem Zweck muss es als *zuverlässige* Cybermacht auftreten, die ihre schutzbedürftigen europäischen Nachbarn unterstützt. Auf nationaler Ebene muss es zielgerichtete politische Strategien verfolgen, die sich auch auf internationaler Ebene umsetzen lassen. Seine offensiven Cyberfähigkeiten müssen zudem die Fähigkeiten anderer großer Cybermächte ergänzen. Dazu gehören Verteidigungswerkzeuge, die auch in Friedenszeiten schädigende Cyberoperationen unterbinden.[1] Im Mittelpunkt derartiger Strategien steht weniger die Abschreckung (der Iran führt z. B. regelmäßig Cyberangriffe gegen die USA durch, die bekannter- und erwiesenermaßen über offensive Fähigkeiten verfügen), sondern vielmehr ein transparentes demokratisches Vorgehen im Dienste der Bürgerinnen und Bürger. Russland hat seine offensiven Cyberfähigkeiten bisher weder offiziell bestätigt, noch hat es näher erläutert, unter welchen Umständen sie zum Einsatz kommen.

Vor allem aber kann sich Deutschland keine weitere Nabelschau leisten, was den Stellenwert der Zeitenwende und ihre Folgen für die Identitätsbildung nach dem Kalten Krieg betrifft. Das Land benötigt endlich eine Nationale Sicherheitsstrategie mit allen Merkmalen einer „Großstrategie“ und einem eindeutigen Narrativ, um die deutsche Gesellschaft zu informieren und zu mobilisieren. In die Ausarbeitung dieser NSS müssen auch die Cybermaßnahmen der deutschen Verbündeten und gegebenenfalls deren Defizite einfließen. Dafür ist es zunächst einmal sinnvoll, die verschiedenen Positionen im Cyberspace näher zu definieren.

GROSSBRITANNIEN: DIE VERANTWORTUNGSVOLLE CYBERMACHT

In einem umfassenden Bericht zu Fragen der Sicherheit, Verteidigung, Entwicklung und Außenpolitik (*Integrated Review of Security, Defence, Development and Foreign Policy*) aus dem Jahre 2021 bezeichnet sich Großbritannien selbst nicht nur als führende, sondern auch als verantwortungsvolle Cybermacht.[2] Folglich stehen britische Cyberoperationen im Einklang mit dem Völkerrecht und mit nationalem Recht. Darunter fällt auch das Gesetz über die Nachrichtendienste (*Intelligence Services Act*) von 1994, gemäß dem nationale Nachrichtendienste einer parlamentarischen Kontrolle unterliegen. Darüber hinaus bezeichnet der Bericht die britischen Cyberfähigkeiten als angemessen und zielgerichtet. Die damit verbundenen Beschränkungen sind Teil des unbeugsamen britischen Einsatzes gegen „verantwortungslose“ Cyberaktivitäten. Der Bericht nennt Russland als Beispiel für ein solches Verhalten, weil es keinen Wert auf die Rechtmäßigkeit seiner Cyberoperationen mit weitreichenden, wenn nicht sogar globalen Kollateralschäden legt.[3] Als verantwortungsvolle Cybermacht bekennt sich Großbritannien offen zu seinen Offensivfähigkeiten. „Wir werden auch weiterhin (…) auf unsere nuklearen und offensiven Cyberfähigkeiten zur Verteidigung gemäß unseren Bündnisverpflichtungen aus Artikel 5 [des Nordatlantikvertrags] verweisen.“[4]

1 Valentin Weber, “Rethinking European Cyber Defense Policy,” Deutsche Gesellschaft für Auswärtige Politik (April 2022): <https://dgap.org/sites/default/files/article_pdfs/dgap-policy%20brief-2022-08-en.pdf> (Zugriff am 30. September 2022).

2 The Cabinet Office, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, (16. März 2021): <https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy> (Zugriff am 30. September 2022).

3 Monica Kaminska, James Shires, and Max Smeets, “Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far),” European Cyber Conflict Research Initiative (Juli 2022): <https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf> (Zugriff am 30. September 2022).

4 *The Cabinet Office, Global Britain in a Competitive Age*, S. 20.

FRANKREICH: DIE STABILISIERENDE CYBERMACHT?

Frankreich bezeichnet sich in seiner neuen Cyberstrategie von 2021 als stabilisierende Kraft des Friedens und der Sicherheit. Im Dokument heißt es außerdem, dass Frankreich einen wirksamen Multilateralismus befürwortet, der Menschenrechte, Grundfreiheiten und demokratische Grundsätze achtet.[5] Das Land engagiert sich gegen destabilisierende Kräfte wie Russland, das mit nuklearen Marschflugkörpern und interkontinentalen nuklearen Torpedos über „ungewöhnliche" Waffen verfügt.[6] Darüber hinaus will Frankreich sogar in Regionen mit dringendem politischen Reformbedarf eine Vorreiterrolle im Bereich internationaler Stabilisierungsbemühungen übernehmen. Aus französischer Sicht erfordert die Sicherung der Stabilität auch eine Reaktion auf Cyberangriffe.[7] In dieser Hinsicht nimmt das Land eine ähnliche Haltung wie Großbritannien ein: Beide befürworten Normen für ein verantwortungsbewusstes Staatenverhalten. Außerdem will Frankreich vertrauensbildende Maßnahmen zur Stabilitätssicherung durchführen, um eine Eskalationsdynamik bei Cyberangriffen zu verhindern.

USA: DIE DEMOKRATISCHE CYBERMACHT

Die USA positionieren sich als werteorientierter Verfechter demokratischer Normen. In dieser Rolle legen sie das Völkerrecht – in Abhängigkeit von ihren jeweiligen geopolitischen Zielsetzungen – bei Bedarf etwas großzügiger aus. Mit Blick auf das Souveränitätsprinzip[8] stellen die USA fest, dass „Cyberoperationen auf Computern oder anderen Netzwerkgeräten, die sich auf dem Hoheitsgebiet eines anderen Staates befinden, nicht *per se* eine Verletzung" der Souveränität darstellen.[9] Frankreich hat hier beispielsweise eine strengere Rechtsauffassung, denn es betrachtet „jedes unzulässige Eindringen eines anderen Staates in ein französisches System oder *jedwedes* Einwirken auf französischem Staatsgebiet mit digitalen Mitteln" als Verletzung der eigenen Souveränität".[10]

Das Selbstverständnis der USA als Cybermacht zeichnet sich auch durch die Bereitschaft aus, entschlossen gegen seine Gegner vorzugehen. Diese Strategie ist Teil der „Persistent-Engagement-Theorie", die das aktuelle Vorgehen der USA im Cyberspace bestimmt:

„*Mit einer möglichst zielgerichteten offensiven Verteidigung gegen gegnerische Aktivitäten verfügen wir über einen größeren Spielraum, um die Schwächen unserer Gegner zu erkennen, ihre Absichten und Fähigkeiten zu ermitteln und zielgerichtet auf Angriffe zu reagieren. Durch unser kontinuierliches Engagement können wir unsere Gegner taktisch und strategisch schwächen und dazu zwingen, ihre Ressourcen auf die Verteidigung und Verhinderung von Angriffen umzuleiten.*"[11]

Das Außergewöhnliche an der Nationalen Sicherheitsstrategie 2021 von US-Präsident Joe Biden ist auch ihre klare Werteorientierung. Nach Maßgabe dieser Strategie sind alle Formen von Cyberbedrohungen, und auch andere Bedrohungen, letztendlich gegen eine Gemeinschaft von Demokratien gerichtet.[12]

5 Verteidigungsministerium, *Strategic Update*, (2021), p. 45: <https://www.stjornarradid.is/library/03-Verkefni/Almannaoryggi/Thjodaroryggismal/France%20-%20Strategic%20Review%202021.pdf> (Zugriff am 30. September 2022).

6 Ebd.

7 Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), *Revue stratégique de cyberdéfense* [Strategische Überprüfung der Cyberabwehr], (12. Februar 2018), S. 86-87: <http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf> (Zugriff am 30. September 2022).

8 Zum Völkerrecht und zum Souveränitätsprinzip im Cyberraum siehe Isabella Brunner, Erich Schweighofer und Jakob Zanol, "Malicious Cyber Operations, 'Hackbacks' and International Law: An Austrian Example as a Basis For Discussion on Permissible Responses," *Masaryk University Journal of Law and Technology* 14, no. 2, (23. September 2020): <https://journals.muni.cz/mujlt/article/download/13187/11652> (Zugriff am 30. September 2022).

9 Generalversammlung der Vereinten Nationen, *Official Compendium of Voluntary National Contributions On The Subject of How International Law Applies to the Use Of Information and Communications Technologies by States Submitted by Participating Governmental Experts in The Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266* (13. Juli 2021), S. 140: <https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf> (Zugriff am 30. September 2022).

10 Verteidigungsministerium, *Droit International Appliqué Aux Opérations Dans Le Cyberespace* [Anwendung des Völkerrechts auf Operationen im Cyberraum], (2019): <https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf> (Zugriff am 30. September 2022).

11 U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," (2018), S. 6: <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf> (Zugriff am 30. September 2022).

12 "We will stand with our allies and partners to combat new threats aimed at our democracies, ranging from cross-border aggression, cyberattacks, disinformation, and digital authoritarianism to infrastructure and energy coercion." [Wir kämpfen an der Seite unserer Verbündeten und Partner gegen neue Gefahren, von grenzüberschreitender Aggression, über Cyberangriffe, Desinformationen und digitalen Autoritarismus bis hin zum Einsatz von Infrastrukturen und Energie als Druckmittel], The White House, "Interim National Security Strategic Guidance," (März 2021), S. 19: <https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf> (Zugriff am 30. September 2022).

DREI PROBLEMFELDER

Aus den Positionierungen dieser drei Mächte ergeben sich drei Probleme. Erstens sind sie weniger koordiniert, als es zunächst erscheinen mag. Denn auch wenn sich die Formulierungen in den Strategiedokumenten häufig gleichen, werden sie in den einzelnen Ländern unterschiedlich ausgelegt. Beispielsweise sind sich alle drei zwar einig über die allgemeine *Anwendbarkeit* des Völkerrechts auf Cyberoperationen, doch sie haben sehr unterschiedliche Auffassungen davon, *wie* dieses Recht zur Anwendung kommt. Dies zeigt auch das im Vorangehenden aufgeführte Beispiel zur Definition des Souveränitätsbegriffs.

Zweitens überschätzen die drei Mächte häufig die Faktoren, die ihrer Einheit zugrunde liegen, sei es mit Blick auf internationale Normen oder als Wertegemeinschaft. Sie können sich also miteinander verbunden fühlen, obwohl sich ein Land aus Sicht der anderen „verantwortungslos“ oder „destabilisierend“ verhält. Beispielsweise haben die USA Malware in die kritische Infrastruktur und die Raketensysteme eines gegnerischen Staates eingeschleust, um seine Offensiv- und Defensivkapazitäten zu schwächen. Dies wiederum könnte den Gegner zu Gegenmaßnahmen bewegen.[13] Disruptive Angriffe auf das Staatsgebiet von Bündnispartnern könnten ebenfalls als Rechtsverletzung gewertet werden.[14]

Drittens definieren die einzelnen Mächte ihre eigene Rolle häufig aus einem negativen Blickwinkel auf das, was sie nicht sind. Frankreich verhält sich nicht wie eine terroristische Vereinigung, weil solche Gruppen zerstörerisch und destabilisierend vorgehen. Die USA sind nicht wie China, weil beide Länder über vollkommen unterschiedliche Wertesysteme verfügen. Großbritannien verhält sich nicht wie das verantwortungslose Russland. Selbst positive Glaubenssätze werden häufig nicht eindeutig formuliert. Großbritannien spricht von „verantwortungsvollen offensiven Cyberoperationen“, wenn es darum geht, schädliche Akteure im Cyberspace für ihre Taten zur Rechenschaft zu ziehen.[15] Allerdings hat der Verfasser dieses DGAP Policy Briefs bereits in einem anderen Artikel darauf verwiesen, dass sich „verantwortungsvolle“ offensive Cyberoperationen nur schwer definieren und durchführen lassen.[16]

DEUTSCHLAND ALS ZUVERLÄSSIGE CYBERMACHT

Die vorangehende Analyse macht deutlich, dass sich die Strategien der deutschen Verbündeten im Cyberspace in ihren wesentlichen Zielsetzungen gleichen. Doch es gibt auch Unterschiede, was die Anwendbarkeit des Völkerrechts und die Durchführung von Cyberoperationen betrifft. Die USA führen mit Abstand die disruptiven Angriffe durch unter den westlichen Staaten – als Beispiele waren Stuxnet und die Sabotage des nordkoreanischen Raketenprogramms zu nennen. Das Vorgehen Frankreichs und Großbritanniens ist dagegen weitaus gemäßigter oder zumindest weniger offensichtlich.[17] Dieser wahrgenommene Unterschied muss sich auch in den nationalen Strategien niederschlagen. Deutschland muss in seiner Nationalen Sicherheitsstrategie die vielen Gemeinsamkeiten mit seinen Verbündeten, aber auch die eigene besondere Position als zuverlässige Cybermacht unterstreichen. Wie könnte Deutschland dies erreichen?

Im Inland...

Die deutsche Nationale Sicherheitsstrategie und Innenpolitik müssen zuverlässig und konsequent auf Transparenz und eine Stärkung der Cybersicherheit ausgerichtet werden, um auch andere Länder zu Maßnahmen mit ähnlichen Schwerpunkten zu bewegen. Zurzeit hat Deutschland mit der Offenlegung von Sicherheitslücken und der Verschlüsselung einen anderen Weg gewählt. Das Bundesinnenministerium (BMI) setzt in seiner aktuellen Cybersi-

13 Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare* (London, 2022).

14 Chris Bing, “Command and Control: A Fight for the Future of Government Hacking,” *Cyberscoop*, 11. April 2018: <https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight> (Zugriff am 3. Oktober 2022).

15 The Cabinet Office, *Global Britain in a Competitive Age*, p. 42. Ein weiteres Problem besteht darin, dass der britische Bericht mehrere Beispiele für verantwortungsvolle defensive Cyberoperationen enthält. Diese betreffen jedoch nur Maßnahmen gegen nichtstaatliche Akteure und stellen damit kein Alleinstellungsmerkmal einer demokratischen Cybermacht dar. Denn auch Russland und China könnten ähnliche Maßnahmen wie Demokratien gegen Terroristen oder die Täter von Kindesmissbrauch ergreifen. In diesem Dokument bezieht sich das einzige Beispiel für staatliches Handeln auf Verteidigungsfähigkeiten, die darauf abzielen, den Einsatz von Waffensystemen gegen die britische Luftwaffe abzuwehren. (S. 42) Darüber hinaus enthält der Bericht keine weiteren Beispiele, dass Großbritannien bei der Durchführung offensiver Cyberoperationen gegen andere *staatliche Akteure* als verantwortungsbewusste Cybermacht auftritt.

16 Valentin Weber, “The Illusion of ‘Responsible’ Cyber Offense,” Deutsche Gesellschaft für Auswärtige Politik (27. Oktober 2021): <https://dgap.org/en/research/publications/illusion-responsible-cyber-offense> (Zugriff am 30. September 2022).

17 Jon R. Lindsay, “Stuxnet and the Limits of Cyber Warfare,” *Security Studies* 22, no. 3 (2013), S. 365–404: <https://doi.org/10.1080/09636412.2013.816122> (Zugriff am 30. September 2022); David E. Sanger und William J. Broad, “Trump Inherits a Secret Cyberwar Against North Korean Missiles,” *The New York Times*, 4. März 2017: <https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html> (Zugriff am 30. September 2022)

cherheitsagenda auf die innerstaatliche Rolle der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) bei der Entwicklung offensiver Cybertools, um die Abhängigkeit von vergleichbaren Instrumenten aus dem Ausland zu reduzieren.[18] Allerdings geht Deutschland im Unterschied zu den USA und Großbritannien weder transparent noch offen mit dem Einsatz derartiger Tools um.[19] Ohne einen solchen Rahmen, gemeinhin als „Schwachstellenmanagement-Prozess" bekannt, kann es sich und andere nicht schützen, wenn es selbst auf Intransparenz setzt.

Auch die deutsche Verschlüsselungspolitik wird den Ansprüchen an eine verlässliche und um mehr Sicherheit bemühte Cybermacht nicht gerecht. Die aktuelle Strategie „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" zeigt die ganze Widersprüchlichkeit des deutschen Vorgehens.[20] Die fortgesetzte Ende-zu-Ende-Verschlüsselung wird durch den Einbau von Hintertüren für Behörden untergraben. Mit einer solchen Strategie macht sich Deutschland anfällig für Cyberbedrohungen und legitimiert darüber hinaus das Handeln autoritärer Staaten, die Verschlüsselungsstandards zum Zweck der Inlandsüberwachung systematisch abgebaut haben.

... und im Ausland

Deutschland muss seine Vision für den Cyberraum mit seinem Selbstverständnis als Cybermacht oder, anders gesagt, mit seinen übergeordneten strategischen Zielen abgleichen.[21] Aktuell sind seine strategischen Prioritäten darauf ausgerichtet, eine größere Rolle in der europäischen Verteidigung zu übernehmen und in diesem Bereich für schwächere Nachbarstaaten als verlässlicher Partner aufzutreten. Tatsächlich hat sich Deutschland in jüngster Zeit aktiver um die Kontrolle des ost- und südosteuropäischen Luftraums bemüht und patrouilliert vor allem über den Staatsgebieten von Polen und Rumänien, die unmittelbar von Russland bedroht sind.[22]

Deutschland muss sich ähnlich aktiv in der Verteidigung der ost- und südosteuropäischen Flanken des Cyberraums zeigen und dieses Engagement mit anderen EU-Mitgliedstaaten koordinieren. Zu diesem Zweck muss das Land seine internationalen Kapazitäten ausbauen und *Best Practices* mit seinen Partnern austauschen. Jüngste Cyberangriffe auf Albanien (die nach Angaben des Landes vermutlich vom Iran ausgingen) verdeutlichen die Notwendigkeit einer Unterstützung der regionalen Cyberabwehr[23], die im Anschluss an die Cyberangriffe vor allem aus den USA kam.[24] Montenegro, ebenfalls Zielscheibe schädigender Cyberaktivitäten, hat Unterstützung vom US *Cyber Command* bei der zusätzlichen Sicherung seiner Netze gegen Cyberangriffe erhalten.[25] Doch auch deutsche Expertise ist gefragt. Kurz vor dem russischen Einmarsch in die Ukraine war ein Besuch von Mitarbeitenden des Bundesamts für Sicherheit in der Informationstechnik geplant, um das Land bei Maßnahmen zur Cybersicherheit zu unterstützen. Auch wenn die Reise aus Sicherheitsgründen abgesagt wurde, ist eine solche Unterstützung unter sicheren Bedingungen zu befürworten.

Die deutsche Stellungnahme zu den eigenen offensiven Fähigkeiten findet sich versteckt im Glossar auf Seite 133 der Cybersicherheitsstrategie von 2021. In der neuen Nationalen Sicherheitsstrategie muss die Regierung noch deutlicher darauf verweisen, dass Deutschland über offensive Cyberfähigkeiten verfügt und diese im Einklang mit dem Völkerrecht auch einsetzen wird. Offensive Cyberoperationen sollte das Land nur als Reaktion auf schädigende Aktivitäten

18 Bundesministerium des Innern und für Heimat, "Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat", (Juni 2022): <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4> (Zugriff am 30. September 2022).

19 Deutscher Bundestag, "IT-Schwachstellenmanagement der Bundesregierung", 25. Januar 2022: <https://www.bundestag.de/presse/hib/kurzmeldungen-879150> (Zugriff am 30. September 2022); Government Communications Headquarters, "The Equities Process," 29. November 2018: <https://www.gchq.gov.uk/information/equities-process> (Zugriff am 30. September 2022).

20 Bundesministerium des Innern, für Bau und Heimat, "Cybersicherheitsstrategie für Deutschland 2021" (August 2021): <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=C6B367B55F7F2C0AD403FB31F2C5A9CA.2_cid322?__blob=publicationFile&v=2> (Zugriff am 30. September 2022).

21 Valentin Weber, "Linking Cyber Strategy with Grand Strategy: The Case of the United States," *Journal of Cyber Policy*, August 17, 2018.

22 Bundeswehr, „Luftpatrouillen über Polen und Rumänien", 2. März 2022: <https://www.bundeswehr.de/de/organisation/luftwaffe/aktuelles/luftpatrouillen-ueber-polen-und-rumaenien-5364382> (Zugriff am 30. September 2022).

23 Fjori Sinoruka und Vladimir Karaj, "New Cyber-Attacks on Albania Cause Border Chaos," *Balkan Insight* (Blog), 12. September 2022: <https://balkaninsight.com/2022/09/12/new-cyber-attacks-on-albania-cause-border-chaos/> (Zugriff am 30. September 2022).

24 Mariam Baksh, "White House Attributes Attack on Albania's Critical Infrastructure to Iran," *Nextgov*, 7. September 2022: <https://www.nextgov.com/cybersecurity/2022/09/white-house-attributes-attack-albanias-critical-infrastructure-iran/376800/> (Zugriff am 30. September 2022).

25 U.S. Cyber Command, "US, Montenegro Work Together to Defend Against Malicious Cyber Actors," 30. Oktober 2019: <https://www.cybercom.mil/Media/News/News-Display/Article/2002939/us-montenegro-work-together-to-defend-against-malicious-cyber-actors/https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F2002939%2Fus-montenegro-work-together-to-defend-against-malicious-cyber-actors%2F> (Zugriff am 30. September 2022).

und zur Verhinderung disruptiver Angriffe durchführen.[26] Es sollte auf das Einschleusen logischer Bomben in die kritische Infrastruktur seiner Gegner verzichten, sofern keine unmittelbaren feindlichen Handlungen vorliegen oder drohen.[27] Das Eindringen in gegnerische Netze zum Zweck des Erkenntnisgewinns und der Aufklärung wäre weiterhin möglich. Trotz gelegentlicher Zweifel an Deutschlands offensiven Cyberfähigkeiten ist es der Bundeswehr 2016 gelungen, in die afghanische Mobilfunkinfrastruktur einzudringen und Informationen im Zusammenhang mit einer Geiselnahme zu erlangen.[28]

Als verlässliche Cybermacht muss Deutschland seine offensiven Cyberfähigkeiten auch vertrauenswürdigen EU-Mitgliedstaaten, Nato-Verbündeten oder Partnern im Ausland zur Verfügung stellen, um im Krisenfall auf Ersuchen Unterstützung zu gewähren. Mit bilateralen und multilateralen Vereinbarungen ließe sich sicherstellen, dass die Kapazitäten ausschließlich mit Ländern geteilt werden, die Cyberoperationen im Einklang mit dem Völkerrecht durchführen. In derartigen Vereinbarungen könnten auch die bereitzustellenden Fähigkeiten und die Umstände für eine solche Bereitstellung näher definiert werden.[29]

Ein beschränkter Einsatz der offensiven Cyberfähigkeiten Deutschlands stünde im klaren Gegensatz zu den Cyberaktivitäten der USA, die sogar täglich auf feindliche Infrastrukturen abzielen[30], um die Angriffsfähigkeiten ihrer Gegner zu schwächen.[31] Das aktuelle Vorgehen der USA geht auf den Krieg gegen den Terror zu Beginn des 21. Jahrhunderts zurück, als die Eliminierung von Terroristen gängige Praxis war. Doch diese taktischen Angriffe haben die Welt vermutlich nicht sicherer gemacht.[32] Und die Schädigung der feindlichen Infrastrukturen für Cyberangriffe könnte sich als ebenso wirkungslos erweisen. Die Blockade der Website eines russischen Propagandasenders während der Midterms in den USA wäre für die Behörden vermutlich mit einem Einsatz von Mitteln verbunden, die sie besser und nachhaltiger in den Ausbau der Cyberresilienz oder in strategische Cyberoperationen investieren könnten.[33] Und die langfristige Wirkung aller täglichen taktischen Aktivitäten, auf die die USA ihr anhaltendes Engagement stützen, ist womöglich eher begrenzt – was auch auf die Mehrzahl der russischen Cyberoperationen zutrifft.

Deutschland muss seine Position als globaler Akteur im Cyberkapazitätsaufbau weiter ausbauen, um seine Rolle als zuverlässige Cybermacht zu festigen. Obwohl sich die Regierung schon heute an zahlreichen Initiativen zum Cyberkapazitätsaufbau beteiligt, muss sie ihr diesbezügliches Engagement erweitern und noch stärker in ihre strategische Vision einfließen lassen.

26 Brunner, Schweighofer und Zanol, "Malicious Cyber Operations, 'Hackbacks' and International Law: An Austrian Example as a Basis for Discussion on Permissible Responses."

27 David E. Sanger und Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, 15. Juni 2019: <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html> (Zugriff am 30. September 2022).

28 Matthias Gebauer, "Bundeswehr: Hacker knackten Mobilfunknetz in Afghanistan", *Der Spiegel*, 23. September 2016: <https://www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html> (Zugriff am 30. September 2022).

29 Jan Kallberg, Todd Arnold, and Stephen S. Hamilton, "Sharing Cyber Capabilities Within the Alliance - Interoperability Through Structured Pre-Authorization Cyber," West Point Research Papers (Sommer 2022): <https://digitalcommons.usmalibrary.org/cgi/viewcontent.cgi?article=1707&context=usma_research_papers> (Zugriff am 30. September 2022).

30 U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command."

31 Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, "Persistent Engagement in Cyberspace Is a Strategic Imperative," *The National Interest*, 6. Juli 2022: <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/persistent-engagement-cyberspace> (Zugriff am 1. Oktober 2022).

32 Brian Michael Jenkins, "Five Years After the Death of Osama Bin Laden, Is the World Safer?," *The Rand Blog*, 2. Mai 2016: <https://www.rand.org/blog/2016/05/five-years-after-the-death-of-osama-bin-laden-is-the.html> (Zugriff am 30. September 2022).

33 Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *The Washington Post*, 27. Februar 2019: <https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html> (Zugriff am 30. September 2022).

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

Die Deutsche Gesellschaft für Auswärtige Politik e.V. (DGAP) forscht und berät zu aktuellen Themen der deutschen und europäischen Außenpolitik. Dieser Text spiegelt die Meinung der Autorinnen und Autoren wider, nicht die der DGAP.

Die DGAP ist gefördert vom Auswärtigen Amt aufgrund eines Beschlusses des deutschen Bundestages.

Herausgeber
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Übersetzung Kathrin Hadeler

Redaktion Jana Idris

Layout Luise Rombach

Design Konzept WeDo