3 // 2024

spotlight

SEGMENTIERUNG DES CYBERSPACE?

Chinas und Russlands Decoupling-Bestrebungen und ihre Konsequenzen

Seit einigen Jahren zeichnet sich ein besorgniserregender Trend ab: Autoritär geprägte Staaten entkoppeln sich zunehmend von den globalen Internet-Infrastrukturen durch den Aufbau eigener IT-Systeme und -Infrastrukturen. Mittelfristig könnte diese Entwicklung zu einer Aufteilung des Cyberspace in unabhängig voneinander funktionierende Teile führen. Eine solche *Segmentierung* kann Bestandteil strategisch-außenpolitischer Interessensdurchsetzung sein. Damit wird die ohnehin brüchige Stabilität des Cyberraums nachhaltig untergraben und das Risiko schwerwiegender Cyberattacken erhöht.

Moskau: Ein Serverraum für Russlands leistungsstärksten Supercomputer Christofari im Rechenzentrum Skolkovo der Sberbank. Foto: © picture alliance/dpa/TASS | Mikhail Tereshchenko.

VON THOMAS REINHOLD

Der Cyberspace ist eine Ansammlung unzähliger miteinander verbundener IT-Netzwerke, die auf Grundlage global einheitlicher, verbindlicher technischer Vorgaben – sog. *Protokolle* – funktionieren, die sämtliche technischen Abläufe der Datenübertragung im Internet regeln. Diese Verfahren wurden und werden durch internationale besetzte und partizipativ organisierte zivilgesellschaftliche Gremien, wie der Internet Engineering Task Force (IETF) sowie der Internet Corporation for Assigned Names and Numbers (ICANN) entwickelt und gemeinsam verwaltet. Aufgrund des stark in den USA und in Westeuropa angesiedelten Ursprungs des Cyberspace sind dabei in gewissem Maße auch Werte abgebildet, die nicht von allen Staaten geteilt werden, wie der freie Zugang zu Informationen, Anonymität im Cyberspace und der Schutz vor Überwachung. Insbesondere autokratisch geprägte Staaten sehen damit ihre nationale Souveränität untergraben und bauen seit einigen Jahren parallele Infrastrukturen auf.

Ein Beispiel dafür sind die umfangreichen IT-Systeme für die DNS-Namensauflösung sowie die Steuerung des nationalen Datenverkehrs (das sog. *Routing*), die in China für die Kontrolle der Informationsverbreitung und des Zugangs zum weltweiten Internet aufgebaut worden sind und kontinuierlich weiterentwickelt werden.[1] Gleichzeitig propagiert China seit einigen Jahren vor allem im Rahmen der International Telecommunication Union (ITU), einer UNO-Sonderorganisation, eine von Huawei konzipierte und als „IPv6+“ oder auch „New IP“ bezeichnete Weiterentwicklung des weltweiten Standards für die Datenübertragung im Internet, die unter anderem eine Durchsetzung nationaler Informationsbeschränkungen ermöglicht.

Parallel weitet China seinen Einflussrahmen im Cyberspace mit der Finanzierung neuer Internet-Glasfaser-Anbindungen und der unternehmerischen Kontrolle über dafür benötigte IT-Infrastrukturen im Zuge der „Digitalen Seidenstraße“[2] auf Schwellen- und Entwicklungsländer aus. Diese verfügen oftmals nicht über ausreichende Anbindungen an den globalen Cyberspace,[3] um den Verlust von Übertragungskapazitäten durch Störungen einzelner Kabel zu kompensieren (die sog. *Redundanz*).

Beijing, 10. Juli 2018: Auf der China Internet Conference 2018 informieren sich die Teilnehmenden über die Möglichkeiten der IPv6 Einführung. Foto: © picture alliance / Xinhua News Agency | Li Xin.

Als weiteres Beispiel kann Russland angesehen werden, das mit „RuNET“[4] seit einigen Jahren unabhängige Infrastrukturen aufbaut. Diese Bestrebungen sind nach Russlands Angriff auf die Ukraine erheblich intensiviert worden,[5] sowohl im Rahmen der nationalen Informationskontrolle, aber auch dezidiert als Reaktion auf internationale Sanktionen,[6] um beispielsweise unabhängig vom global verwalteten DNS-System zu werden.[7]

IMPLIKATIONEN FÜR DIE ARCHITEKTUR DES CYBERSPACE UND DESSEN REGULATION

Beiden Fallbeispielen ist gemeinsam, dass in einem ersten Schritt global verwaltete, aber innerhalb der staatlichen Jurisdiktion befindliche Infrastrukturen und Internet-Dienstleistungen durch national kontrollierte und ausschließlich national verwaltete Systeme ersetzt werden. Diese bereits feststellbaren Tendenzen schaffen die Voraussetzungen dafür in einem weiteren Schritt innerhalb des national kontrollierten Cyberspace globale Protokolle abzulösen und durch eigene technische Vorgaben zu ersetzen. Da eine solche Umstellung aufgrund funktioneller Zusammenhänge und technischer Abhängigkeiten in aller Regel weitere IT-Systeme betrifft, könnten so in den nächsten ein bis zwei Jahrzehnten[8] innerhalb des globalen Cyberspace „Segmente“ entstehen, die von den globalen Funktionsprinzipien und Diensten entkoppelt sind. Gleichzeitig sorgt diese Konzentration auf die Nutzung nationaler IT-Dienste dafür, dass mehr und mehr Daten nur noch ausschließlich innerhalb des Segmentes übertragen werden, und mindert die Erfordernisse, das betreffende Segment weiterhin eng mit dem Rest des Cyberspace zu verbinden. Dies gefährdet die Redundanz von Datenverbindungen als eine der wesentlichsten infrastrukturellen Stärken des Cyberspace, während die Abhängigkeiten von den verbleibenden Verbindungen zunimmt.[9]

Bislang wurde der Cyberspace weitestgehend als globales Gemeingut betrachtet, an dem alle Staaten partizipieren und von dessen geregelter Nutzung sie auf Grundlage gemeinsamer Vereinbarungen profitieren. Der daraus resultierende, implizite Schutz dieses Raumes verliert jedoch an Wirksamkeit, je unabhängiger einzelne Segmente werden und je mehr unterschiedliche Werteauffassungen ohne negative Konsequenzen durchgesetzt werden können. Dieser Trend nationaler Sonderwege behindert die Weiterentwicklung global wirksamer Normen für den Cyberspace und erschwert zusätzlich die bereits ohnehin schwierige Ausgestaltung verbindlicher Regeln für staatliches Verhalten im Cyberspace. Divergierende technische Verfahren stehen des Weiteren einer einheitlichen globalen Regulierung der Funktionsprinzipien im Wege und können zu einem „Flickenteppich“ an potentiell inkompatiblen technischen Protokollen führen, die durch aufwendige „Übersetzungsprotokolle“[10] konvertiert werden müssten, um den Datenaustausch über Segmentgrenzen hinweg zu ermöglichen. Die Herausbildung unabhängiger Segmente, deren technische Infrastrukturen sich immer weiter voneinander entfernen, könnte auch die international weitestgehend gefestigte Auffassung[11] untergraben, was kritische Infrastrukturen im Cyberspace sind, und den Konsens gefährden, solche IT-Systeme nicht durch absichtliche oder unabsichtliche Aktivitäten im Cyberspace zu gefährden.

Perspektivisch besteht außerdem die Herausforderung, dass Segmente und deren Protokolle zum Bestandteil staatlicher *Power Projection* werden können, etwa im Rahmen strategischer Wirtschaftsförderungsprojekte und der damit verbundenen globalen Expansionsbestrebungen. Gerade Schwellen- und Entwicklungsländer könnten vor die Frage gestellt werden, ob sie sich beispielsweise im Zuge der Unterstützung beim immens kostenintensiven Aufbau und Betrieb von IT-Systemen und -Infrastrukturen dem Segment des unterstützenden Staates anschließen und dessen Protokolle übernehmen. Staaten, die diese Zuordnung nicht eingehen wollen, müssten unterschiedliche Übersetzungssysteme implementieren, um mit ver-

schiedenen Segmenten sowie dem Rest des Cyberspace interagieren zu können.

IMPLIKATIONEN FÜR DIE ZUKUNFT DES CYBERWAR

Bisher bot der Umstand, dass sich schadhafte Aktivitäten eines Akteurs im Cyberspace schnell auch zu seinen eigenen Ungunsten entwickeln können, einen Anreiz, von allzu offensiven Maßnahmen mit ungewissem Eskalations- und Ausbreitungspotential abzusehen. Obgleich die Herausbildung unterschiedlicher technischer Funktionsprinzipien aus Sicht des einzelnen Segments oberflächlich betrachtet eine Verbesserung der Resilienz darstellt, erodiert diese Entwicklung jedoch massiv den Schutz des Cyberspace vor schwerwiegenden und großflächigen Cyberattacken. Während schadhafte Aktivitäten bislang auch deswegen maßgeschneidert werden, damit ihre Wirkung auf das intendierte Ziel begrenzt bleibt und sich nicht unkontrolliert ausbreitet,[12] muss ein Akteur, dessen IT-Systeme vom Rest der Welt entkoppelt sind, nicht mehr das unbeabsichtigte Übergreifen auf diese befürchten. Mit dem Fortschreiten dieser Entwicklung könnten auch die globalen IT-Infrastrukturen, die das technische Rückgrat des Cyberspace bilden, zum Ziel von Cyber-Angriffen oder auch physischen Zerstörungen werden, wenn ein angreifender Akteur von deren Funktion nur noch begrenzt oder gar nicht mehr abhängt. Dadurch wird die Herausforderung des physischen Schutzes der global verteilten Datenübertragungs-Infrastrukturen weiter verschärft. Diese beruhen zu großen Teilen auf unterseeischen Glasfaserverbindungen, von denen ca. 80% in einer Tiefe liegen, die nicht mehr effektiv durch direkte physische oder technische Maßnahmen geschützt werden kann.[13] Debatten um Abschreckungsmaßnahmen und Vergeltungsandrohungen bei Angriffen auf diese Systeme könnten dadurch Auftrieb erhalten.

Im Gegenzug kommt dem Schutz der Segment-eigenen Infrastrukturen eine enorme Relevanz zu. Dies gilt insbesondere für Staaten, die einem Segment zugehörig sind, von dessen „Kern-Infrastruktur" sie aber geographisch weit entfernt sind. Inselstaaten im Pazifik sind beispielsweise bereits jetzt infrastrukturell von eingeschränkten, zum Teil singulären Zugriffsmöglichkeiten auf den Cyberspace abhängig. Mit Blick auf derartige „Segment-Inseln" steigt für feindliche Akteure der Anreiz, die Schwachpunkte der fehlenden oder unzureichenden Redundanzen auszunutzen und anzugreifen. Es wird massiver Investitionen bedürfen, um redundante Strukturen – entweder auf Basis bestehender Glasfasertechnologie oder durch alternative Versorgungswege per Satellit – aufzubauen und gegen Angriffe und Störungen abzusichern.

Neben dieser Entwicklung in Bezug auf offene gewalttätige Konflikte werden mutmaßlich auch in Friedenszeiten die verdeckten Cyber-Aktivitäten in fremden Segmenten zunehmen, um diese zu überwachen und nach ausnutzbaren Fehlern in den technischen Protokollen und den IT-Systemen zu suchen. Diese Schwachstellen werden benötigt, um Handlungsmöglichkeiten für Wirtschaftsspionage, nachrichtendienstliche Bedarfe oder militärische Operationen zu etablieren.

Neben diesen Formen von offensiven Cyberangriffen werden mutmaßlich auch informationsbasierte, hybride Angriffe weiter zunehmen – als Ausdruck der politischen Konfrontation sowie als Mittel der Delegitimierung, Destabilisierung und Störung. Ebenso ist zu erwarten, dass auch die schadhaften Aktivitäten zwischenstaatlicher Akteure im Cyberspace, wie sie insbesondere im Zuge des russischen Angriffskrieges gegen die Ukraine zu Tage getreten sind,[14] weiter zunehmen werden, entweder in klarer politischer Zuordnung zu einem Segment oder in Form Segment-übergreifender, opportunistischer Akteure.

FAZIT UND HANDLUNGSEMPFEHLUNGEN

Die zunehmenden Entkopplungsbestrebungen einzelner Staaten können dazu führen, dass sich innerhalb des Cyberspace Segmente entwickeln bis hin zu einer Herausbildung divergierender und mutmaßlich inkompatibler Infrastrukturen und Funktionsprinzipien. Die Verringerung der globalen Abhängigkeit vom Cyberspace erodiert den impliziten Schutz dieser Domäne vor großflächig angelegten, schad-

CNTR-PROJEKT

Das Cluster Natur- und Technikwissenschaftliche Rüstungskontrollforschung (CNTR) erforscht militärisch relevante Neue Technologien und Entwicklungen in den Naturwissenschaften aus interdisziplinärer Perspektive. Die Wissenschaftler*innen des Clusters untersuchen Auswirkungen auf die internationale Sicherheit, ordnen diese wissenschaftlich fundiert ein und entwickeln auf dieser Grundlage Handlungsempfehlungen zur Stärkung der Rüstungskontrolle.

Das Projekt wird über eine Laufzeit von vier Jahren (Januar 2023 bis Dezember 2026) vom Auswärtigen Amt gefördert.

ZUM AUTOR

Dr. Thomas Reinhold ist wissenschaftlicher Mitarbeiter im CNTR-Projekt. Er forscht zur Militarisierung des Cyberspace, KI und Möglichkeiten zur Rüstungsbegrenzung, -kontrolle und Abrüstung dieser Technologien.

KONTAKT
reinhold@prif.org

PRIF, Baseler Str. 27–31, 60329 Frankfurt am Main
PVst, DPAG 43853, Entgelt bezahlt, ISSN-2512-627X

haften Aktivitäten einzelner Akteure. Damit rücken kritische, teilweise nur schwer zu schützende IT-Infrastrukturen in den Fokus von Cyberangriffen und Störungsversuchen. Gleichzeitig wird fraglich, welche gemeinsamen Interessen staatlicher Akteure den friedlichen Fortbestand eines funktionierenden, globalen Datennetzes ermöglichen können.

Von diesen Überlegungen ausgehend ergeben sich folgende Handlungsempfehlungen:

- Globale IT-Infrastrukturen sollten weiter gestärkt und deren Rolle für das Funktionieren des Cyberspace international hervorgehoben werden. Deren Schutz und Unverletzlichkeit sollte explizit in internationalen Normen und nationaler Rechtsprechung verankert und Cyberoperationen in fremden Netzwerken sollten vermieden werden.
- Die Verwaltung des Cyberspace sollte weiterhin durch eine möglichst breite internationale Basis aus Staaten, Wirtschaft und Zivilgesellschaft auf Grundlage partizipativer Entscheidungsfindung erfolgen. Die Eingliederung bestehender Verwaltungsgremien unter dem Dach der Vereinten Nationen sollte als Maßnahme für deren Legitimierung geprüft werden.
- Verwundbarkeiten durch Engpässe der globalen Infrastrukturen sollten durch den Aufbau von Redundanzen ausgeglichen werden. Schwellen- und Entwicklungsländer sollten weiterhin beim Aufbau von Verbindungen zu den globalen Cyberspace-Infrastrukturen auf multilateraler Basis unterstützt werden.
- Initiativen zur Verbesserung der Cybersicherheit sollten durch den weiteren Ausbau multilateraler Kooperationen massiv gestärkt werden, um insbesondere kritische Infrastrukturen abzusichern. Technologische Abhängigkeiten von Herstellern aus Staaten die sich zu diesem Schutz nicht verpflichten, sollten evaluiert und nach Möglichkeit reduziert und vermieden werden.

PRIF SPOTLIGHT: Das Peace Research Institute Frankfurt (PRIF) ist das größte Friedensforschungsinstitut in Deutschland. PRIF analysiert die Ursachen gewaltsamer internationaler und innerer Konflikte, erforscht die Bedingungen des Friedens und arbeitet daran, den Friedensgedanken zu verbreiten.

V.i.S.d.P.: Elisabeth Waczek, Öffentlichkeitsarbeit (PRIF), Baseler Straße 27–31, Frankfurt am Main, Telefon (069) 959104-0, info@prif.org, www.prif.org. Design: Anja Feix · Layout: PRIF · Druck: Druckerei Spiegler

Fußnoten und weiterführende Links:
prif.org/spotlight0324-fn
DOI 10.48809/prifspot2403

Peace Research Institute Frankfurt
Leibniz-Institut für Friedens- und Konfliktforschung

Leibniz Gemeinschaft