Entkoppelung von China

CSIS Multilateral Cyber Action Committee: The Two Technospheres. Western-Chinese Technology Decoupling: Implications for Cybersecurity. Washington, D.C.: Center for Strategic & International Studies (CSIS), März 2022

Besprochen von **Stefan Steinicke**, Berlin;
E-Mail: s.steinicke@googlemail.com

https://doi.org/10.1515/sirius-2022-3013

Die Entkopplung der westlichen und chinesischen Technologiesphären schreitet voran. Gründe hierfür sind der sich zuspitzende Systemwettbewerb und die zentrale Rolle von neuen Technologien für die zukünftige Machtverteilung in der internationalen Ordnung. Diese Entkopplung hat vielfältige Auswirkungen auf die Cybersicherheit. Das Misstrauen zwischen beiden Seiten nimmt in dem Maße zu, in dem die Separierung der Sphären voranschreitet und der direkte Austausch abnimmt. Der Westen und China versuchen sich, in der digitalen Weltordnung in eine vorteilhafte Position zu bringen, um die eigene Sphäre zu schützen und zu erweitern. Damit drohen ein technologisches Wettrüsten und eine Destabilisierung des Cyberraumes.

Das *CSIS Multilateral Cyber Action Committee* analysiert in seinem Report, dass sich durch das Entkoppeln der Sphären vier Cybersicherheitsimplikationen für den Westen ergeben:

1. Westliche Firmen in China seien mit zunehmenden Cybersicherheitsrisiken konfrontiert. Neue Regularien erlaubten den chinesischen Behörden umfassende Zugriffsrechte. Westliche Unternehmen, die sich mit Cybersicherheitsmaßnahmen vor diesem aufdringlichen Verhalten schützen wollen, würden verstärkt zur Zielscheibe für Cyberzwischenfälle.

2. Neue Datenregulierungen in China sähen vor, dass alle Datenströme in das Land rein und wieder raus durch von offiziellen Stellen kontrollierte Knotenpunkte laufen müssen. Dadurch entstünden hohe Kosten für westliche Unternehmen, die einerseits chinesische Regularien erfüllen und gleichzeitig die Integrität und Sicherheit von Datenströmen gewährleisten müssen. Dieser Zielkonflikt sei immer schwieriger aufzulösen.

3. Es gäbe ein wachsendes Potenzial für chinesische Dominanz in jenen Staaten, die nicht eindeutig der westlichen Technologiesphäre zugeordnet werden. Sollten sich diese Staaten der chinesischen Sphäre anschließen, wären westliche Firmen in vielen aufstrebenden Ländern und ihren sich rasant entwickelnden Märkten großen Cybersicherheitsrisiken in Form chinesischer Technologieinfrastruktur (Hard- und Software) ausgeliefert. Dem Wachstumspotenzial westlicher Unternehmen in den *„in between"*-Staaten wäre damit Grenzen gesetzt.

4. Es werde zunehmend schwierig, globale Cybersicherheitsnormen zu etablieren und durchzusetzen. Stattdessen gäbe es in beiden Technologiesphären eigene Normen, Regulierungen und Rechtsprechungen. Dadurch werde es immer problematischer, Cyberkriminellen in der jeweils anderen Sphäre habhaft zu werden, wodurch noch mehr Unsicherheit im Cyberraum entstehe.

Die Autorinnen und Autoren der Studie skizzieren im Weiteren daher eine westliche Strategie, die dazu dienen soll, die Cybersicherheit der eigenen Technologiesphäre zu erhöhen und im digitalen Systemwettbewerb zu bestehen:

1. Internationale Cybersicherheitsnormen sollten gestärkt werden, indem man mehr Transparenz herstellt und jenen Akteuren hohe Kosten auferlegt, die gegen diese Normen verstoßen. Um dies zu erreichen, sollte eine neue *Governance* geschaffen werden, die das Monitoring von Fehlverhalten und die Identifikation der verantwortlichen Akteure übernimmt. Diese Art des *Trackings* sollte in Form von *Public-Private-Partnerships* zwischen Regierungen und Unternehmen stattfinden. Die neu zu schaffende Institution könnte sich am *International Observatory of Human Rights* oder dem *Enforcement*-Mechanismus für Nichtverbreitung der Internationalen Atomenergiebehörde orientieren.

2. Der Westen sollte für globale Standards bei Datenkonnektivität werben, um grenzüberschreitende Datenflüsse zu ermöglichen, die gleichzeitig Sicherheit und Wahrung der Privatsphäre gewährleisten. Dazu sollte eine neue Organisation geschaffen werden, die operative Prozesse und Maßnahmen zwischen westlichen Staaten institutionalisiert und angleicht. Das Ergebnis könnte dann als Grundlage für eine weltweite Anwendung dienen.

3. Außerdem gehe es für den Westen darum, ein Umfeld zu erschaffen, in dem eine Führungsposition in neuen Technologien, wie 6G, KI oder Quantencomputing ermöglicht wird. Um Chinas Langfriststrategie zur Technologieführerschaft zu kontern, müsse der Westen eigene Initiativen zur Stärkung der Wettbewerbsfähigkeit starten. Nötig hierbei sei eine enge Zusammenarbeit zwischen Regierungen und Unternehmen.

4. Auf operativer und technischer Ebene müsse die Cybersicherheitskollaboration zwischen westlichen Regierungen und Unternehmen gestärkt werden, um böswillige Akteure in ihrem Handeln abzuschrecken. Daher sollten gemeinsame *Public-Private-Partnership*-Zentren gegründet und betrieben werden, um Daten, Analysen und Erkenntnisse zusammenzuführen sowie das Fehlverhalten dieser Akteure zu verfolgen und zu unterbinden.

5. Der Westen sollte einen Fokus auf Technologie-Transparenz legen. Diese könnte zu einem zentralen Wettbewerbsvorteil gegenüber China in jenen Staaten werden, die sich bisher noch keiner der Technologiesphären angeschlossen haben. Transparenz ließe sich stärken, indem Staaten und Unternehmen Produktteile (Hardware und Code) zur Evaluierung an multilaterale Organisationen übergeben, die deren Unversehrtheit und Sicherheit beurteilen. Darüber könne Vertrauen in die Integrität der Produkte hergestellt werden.

https://www.csis.org/analysis/two-technospheres