# Machtentfaltung im virtuellen Raum

*Das freie Internet gehört der Vergangenheit an*

Die Staaten zeigen bei der Regulierung des globalen Kommunikationsnetzwerks wachsende Durchsetzungskraft. Die Entwicklung ihrer Cyber-Kapazitäten wächst stärker als die Möglichkeiten zu ihrer Kontrolle.

*Myriam Dunn Cavelty*

Cyber-Gefahren nehmen an Bedeutung zu. Daher wollen Staaten die Entwicklung und Regulierung des Cyberspace nicht mehr nur nichtstaatlichen Akteuren überlassen. Durch Normenbildung versuchen sie, Stabilität zu generieren; zugleich sind sie jedoch auch die grösste Bedrohung für die Stabilität.

Aufsehenerregende Vorfälle im Cyberspace sind heute an der Tagesordnung. Sie sind ausgetüftelter, kostspieliger und gravierender als je zuvor. Zum einen liegt das an der zunehmenden Verwundbarkeit der gesamten Informationsinfrastruktur. Zum anderen ist die Professionalisierung der Cyberkriminalität so weit fortgeschritten, dass sie längst nicht mehr nur ein kostspieliges Ärgernis für Individuen und die Privatwirtschaft darstellt. Auch Staaten mischen mit: Sie engagieren sich in einem eskalierenden «Rüstungswettlauf», indem sie Instrumentarien entwickeln, mit denen ihre Streitkräfte in der virtuellen Domäne verdeckte «Kriege» führen und gewinnen sollen. Und nicht zuletzt wird gezielt eingesetzte, technisch ausgeklügelte Schadsoftware für politische und wirtschaftliche Spionage verwendet.

## Staatliche Regulierung

Optimisten des Informationszeitalters sprachen Staaten jahrelang die Fähigkeit ab, ihre Macht im virtuellen Raum zu entfalten. Zu hierarchisch, langsam und unflexibel seien diese althergebrachten Gebilde, hiess es. Die jüngsten Entwicklungen zeigen jedoch, dass das Gegenteil zutrifft: Staaten reagieren auf den zunehmenden Druck, das globale Informations- und Kommunikationsnetzwerk im Namen der nationalen Sicherheit zu regulieren, mit wachsender Durchsetzungskraft. Da die Cyber-Domäne zu 100 Prozent menschengemacht ist, kann sie vollständig politischen Wünschen unterworfen werden. Die Spielregeln, inklusive der technologischen Aspekte des virtuellen Raums, werden gegenwärtig einseitig von Staaten verändert.

Trotz beträchtlichen Unterschieden zwischen herkömmlichen Sicherheitsproblemen und den neueren Herausforderungen der Cyber-Sicherheit setzen Staaten auf traditionelle Werkzeuge der Diplomatie. Während des Kalten Krieges entwickelte Instrumente werden verwendet, um politische Interaktion in und durch den Cyberspace zu stabilisieren und gleichzeitig das Eskalationspotenzial von Cyber-Konflikten zu verringern. Der Schwerpunkt liegt auf dem Aufbau von vertrauensbildenden Massnahmen im Rahmen der OSZE sowie der Ausgestaltung von völkerrechtlichen Normen für kriegerische Auseinandersetzung im Cyberspace. Darüber hinaus wird vor allem in amerikanischen Regierungskreisen aktiv darauf hingearbeitet, die alte Abschreckungslogik zumindest teilweise auf den Cyberspace auszuweiten.

## Mehr Unsicherheit

Zum einen haben diese internationalen Bemühungen eine positive Wirkung. Insgesamt ist ein sicherer und offener Cyberspace ohne die Beteiligung von Staaten nicht möglich. Zwischen Staaten können Verhaltensregeln aufgebaut werden, was mittelfristig zu mehr Stabilität führen wird. Paradoxerweise führen diese staatlichen Stabilitätsbemühungen zum andern auch zu mehr Unsicherheit in der virtuellen und in der Folge auch in der realen Welt.

Erstens mangelt es an Lösungsvorschlägen, wie bei der gegenwärtig stattfindenden Festlegung von Normen nichtstaatliche Akteure gewinnbringend einbezogen werden können. Einer der Hauptunterschiede zu traditionellen strategischen Themen ist, dass der Cyberspace seit je von verschiedenen Akteuren für ganz unterschiedliche, alltägliche Aktionen genutzt wird. Nach Sicherheit strebende staatliche Interventionen, die diesen Raum nun einer Logik der nationalen Sicherheit unterwerfen wollen, kollidieren daher häufig direkt mit ganz anderen Vorstellungen, wie der Cyberspace in Zukunft ausgestaltet werden soll.

Dies verursacht beträchtlichen Widerstand gegenüber nationalen Regulierungsversuchen, mit hohen Kosten für alle Beteiligten. Konkret führt die Bereitschaft von Staaten, Sicherheitsbedürfnisse über andere Bedürfnisse zu stellen, dazu, dass staatliche Kontrolle über Informationsflüsse und Bestrebungen, nationale Cyberräume zu bauen, sprunghaft zugenommen haben. Autoritäre Regime begrüssen dies, um ihre Macht weiter zu festigen. Auch in demokratischen Staaten gibt es mehr staatliche Überwachung und Zensur als je zuvor. Das «freie» Internet gehört der Vergangenheit an.

## Suspekte Nachrichtendienste

Zweitens kreiert die weitverbreitete Stärkung von Nachrichtendiensten und Militär in der Cyber-Sicherheit ganz spezifische Probleme. Die rasante Entwicklung von militärischen und geheimdienstlichen Cyber-Kapazitäten wächst gegenwärtig stärker als das zivile Verständnis und die Möglichkeiten zu ihrer Kontrolle. Während Nachrichtendienste oft das Budget wie auch die nötigen technologischen Ressourcen besitzen, um auf Cyber-Bedrohungen zu reagieren, löst ihre Rolle nicht erst seit Edward Snowdens Enthüllungen öffentliches Unbehagen aus.

Solches Unbehagen ist nicht unbegründet. Die gegenwärtigen Stabilitätsbemühungen der Staatenwelt sind fast ausschliesslich gegen zerstörerische Cyber-Attacken gerichtet. Diese Form von Cyber-Aggression könnte in der Tat verheerend sein, indes ist die Eintrittswahrscheinlichkeit sehr gering. Das weitaus grösste Problem für die Cyber-Sicherheit ist neben der Computerkriminalität das heimliche Einschleusen von Schadsoftware für Spionagezwecke, durch die Nachrichtendienste, aber auch durch Akteure aus der Industrie.

Nachrichtendienstliche Ausnutzung von Schwachstellen im Cyberspace untergräbt jene Stabilität, die durch Festlegung von Normen eigentlich erst noch erreicht werden soll. Diese Schwachstellen im globalen Cyberspace reduzieren die Sicherheit des gesamten Systems – für jedermann. Es kann keinen strategisch nutzbaren virtuellen Raum voller Schwachstellen und einen sicheren und robusten Cyberspace geben.

Wenn das Ziel ein sicherer und robuster Cyberspace ist, dann sind aktive politische Anstrengungen erforderlich, um strategisch ausnutzbare Schwachstellen im Cyberspace zu reduzieren. Dies ist ein Kompromiss, den Staaten eingehen müssen. Wenn ein solcher Kompromiss nicht erreicht wird, wird das Streben nach mehr nationaler Sicherheit durch die strategische Ausnutzung des Cyberspace zu immer weniger Sicherheit im globalen Kommunikationsnetzwerk führen. Im computerisierten Zeitalter ist dies dann wiederum gleichbedeutend mit weniger nationaler Sicherheit.

**Myriam Dunn Cavelty** ist Stellvertreterin für Forschung und Lehre am Center for Security Studies, ETH Zürich.