

28. Juni 2021 – Isabel Serpa da Silva

## **Die Zukunft des Multilateralismus im Lichte der geopolitischen Vereinnahmung des Internets**

**Im Zuge der geopolitischen Vereinnahmung des Internets erwachsen multilaterale Foren zu einem Austragungsort des machtpolitischen Ringens um die Gestaltung von Cyber-Normen. Welche Form und Funktion kann und sollte der Multilateralismus einnehmen, um weiteren Fragmentierungserscheinungen des Cyberspace in der post-liberalen Ära entgegenzuwirken?**

Derzeit befindet sich der Cyberspace in einem fundamentalen Umwälzungsprozess, der sich maßgeblich durch die sicherheitspolitisch motivierte Praxis staatlicher Akteur\*innen vorangetrieben sieht. Charakteristisch für jenen Prozess, in dem sich sukzessiv eine neue Geographie des Internets herausbildet, erweist sich seine Emergenz entlang vierer, korrelierender Entwicklungslinien, die gekennzeichnet sind durch: (1) die Wahrnehmung von Interdependenz als Gefahr, (2) die Herausbildung eines Nebeneinanders von Cybermächten, (3) die Verstaatlichung der Internetpolitik und (4) dem Abtrennen von Interaktionsschnittstellen zu anderen Kulturräumen. Diese Entwicklungen stellen die multilaterale Zusammenarbeit vor neue Herausforderungen, die das Potential in sich tragen, sowohl die Form als auch die Funktion des Multilateralismus im Lichte einer neuen Geopolitik des Internets zu verändern.

Im Zuge des kürzlich erschienen „Weißbuch Multilateralismus“ hob die Bundesregierung (2021) dabei vor allem die Notwendigkeit zur inklusiven Öffnung der multilateralen Zusammenarbeit hervor, indem sie betonte, dass sich „die Legitimität multilateralen Handelns [zwar] [...] aus dessen Bindung an die regelbasierte internationale Ordnung [ergibt]. Legitimität beruh[e] allerdings ebenso auf Repräsentation und Teilhabe“ (S.24). Die Inklusion von Unternehmen, Nichtregierungsorganisationen und Expert\*innengemeinschaften zur Gestaltung von Cyber-Normen würde somit nicht nur die Legitimität multilateraler Entscheidungsfindungen und Vereinbarungen steigern, sondern sie würde „langfristig [auch] dazu beitragen, die Verantwortung für die internationale Ordnung

auf viele Schultern zu verteilen“ (ebd.). Ein interessanter Aspekt der bundesdeutschen Ambitionen zur Gestaltung des Cyberspace besteht somit darin, dass sich die Bundesregierung des staatszentrierten Souveränitätsverständnisses, das den Status Quo des Multi Stakeholder-Modells bisweilen auch unter westlichen Demokratien herausfordert, entledigt. Stattdessen betont sie die gewachsene Relevanz inklusiver multilateraler Lösungen, um die digitale Ordnung der Zukunft zu stabilisieren. Dass sich aus jener Ambition der inklusiven Öffnung des Multilateralismus zugleich eine notwendige Reformation des bestehenden Multi Stakeholder-Modells ableitet, bleibt hingegen gänzlich unterthematisiert. Nachdem der Beitrag einen Einblick in die Entwicklungslinien der geopolitischen Vereinnahmung des Internets sowie die divergierenden Souveränitäts-Konzeptionen als Herausforderung für die multilaterale Zusammenarbeit gegeben hat, soll daher erläutert werden, warum die im *Weißbuch Multilateralismus* vorliegende, *implizite These der genuinen Demokratiefreundlichkeit des Multi Stakeholder-Modells* ausgesprochen kritisch zu betrachten ist.

### **Entwicklungslinien einer neuen Geographie des Internets**

Derzeit erleben wir einen Wendepunkt sicherheitspolitischer Praxis, in dessen Kontext sich die Fähigkeit zur *Verteidigung digitalen Territoriums* zu einem immer normaleren Phänomen entwickelt, das sich in das gängige Repertoire moderner Staatlichkeit einreicht. Jene Entwicklung geht mit der wachsenden Fähigkeit sowohl staatlicher als auch nicht-staatlicher Akteur\*innen einher, digitale Tools zu nutzen, um Opponenten Schaden zuzufügen. Dabei eröffnen Cyber-Tools neue Dimensionen in der Bedeutung von Krieg, Kriegsführung und Gewalt, da sie sowohl vitale Infrastrukturen als auch Informationsressourcen in bisweilen unbekanntem, aber potentiell verheerendem, Ausmaße bedrohen, ohne physische Gewalt im herkömmlichen Sinne einzusetzen ([Reuter, 2019](#)). So sieht sich die Wahrnehmung vielzähliger staatlicher Akteur\*innen in nicht unwesentlichem Maße von „einer Schar global agierender Gruppierungen aus Spionen, Kriminellen, Bürgerwehren, Militäreinheiten, Terroristen und opportunistischen Angreifern geprägt, die versuchen, überall dort gewaltsam einzugreifen, wohin sich der Cyberspace erstreckt [Übersetz. D. Verf.]“ ([Demchak, 2011, S.275](#)).

Wenngleich eine erhebliche Lücke zwischen der wahrgenommenen Bedrohung aus dem Cyberspace und dem tatsächlichen Ausmaß gewaltsamer Cyber-Inzidenzen in der realpolitischen Praxis besteht, hält sich jene Erzählung des Cyberspace als Domäne der Kriegsführung hartnäckig. Zurückzuführen ist dies insbesondere auf die Strukturmerkmale des digitalen Raumes; so kreieren die immense Unsicherheit, Unvorhersehbarkeit, Komplexität, Interdependenz sowie der Mangel an Informationen und Fallbeispielen einen schier unüberblickbaren und nur schwer einzuschätzenden Kontext für staatliche Akteur\*innen, der sie dazu verleitet, Risiken, assoziiert mit der Bedrohung durch feindliche Dritte zu überschätzen ([Gomez/Villar, 2018, S.62-63](#)). Diese Verschränkung der Charakteristika des Cyberspace mit den individuellen kognitiven Prozessen menschlicher Akteur\*innen stieß wiederum eine Entwicklung los, nach der sich der Cyberspace, einst wahrgenommen als *das* Tool zur Demokratisierung und Liberalisierung, zu einer *Domain of Conquest* entwickelte, in der staatliche Akteur\*innen bisweilen sowohl um die Kontrolle kritischer Infrastrukturen (KRITIS) als auch die Deutungshoheit in der Ausgestaltung von Werten, Interessen, Normen und Ideen im Rahmen der Herausbildung einer neuen Geographie des Internets ringen.

Entgegen der einst klaren westlichen Prägung des Cyberspace sieht sich jener geopolitische Prozess durch ein Nebeneinander unterschiedlicher Kulturräume gezeichnet, welche aufgrund der Verschmelzung von Wirtschafts- und Sicherheitsinteressen allesamt darum bemüht sind, ihre Cybermacht stetig auszubauen. Insbesondere das Verständnis digitaler Souveränität erwuchs in diesem Rahmen zu einem umfassenden Wirtschaftskonzept, das darauf abzielt, die „Autonomie und Handlungsfähigkeit“ ([BmWi et al., 2014, S.4](#)) des Staates im Bereich der „Informations- und Telekommunikationstechnik“ (ebd.) zu erweitern, während Cyber-Tools zum Mittel zum Zweck wurden, um kritische Infrastrukturen (KRITIS) und Informationsressourcen vor Disruptionen durch feindliche Dritte zu schützen. Die fortschreitende „Digitalisierung der Kriegsführung“ ([Schörnig/Werkner, 2019](#)) muss somit als Symptom eines ordnungspolitischen Wandels, der nunmehr auch beginnt, den digitalen Raum zu vereinnahmen, begriffen werden. Der digitale Grenzziehungsprozess, der aus jenem ordnungspolitischen Wandel resultiert, geht dabei jedoch zugleich mit einem normativen Wandel in der Wahrnehmung des Cyberspace einher, der bedingt, dass sich die Designmerkmale des Internets –

Offenheit, Hierarchiefreiheit, Dezentralität und Anonymität – in zunehmenden Maße zugunsten des Strebens nach nationaler Sicherheit herausgefordert sehen.

So sei darauf verwiesen, dass, wenn unter staatlichen Akteur\*innen gemeinhin akzeptiert wird, dass kritischen Systemen nicht mehr vertraut werden kann, sofern sie, jenseits des ihnen zugewiesenen Territoriums an das offene, globale Netz angebunden sind, diese beginnen, einen Weg zu finden, um potentiellen Bedrohungen des nationalen Territoriums durch den Cyberspace zu begegnen. Dies bedingt wiederum, dass staatliche Akteur\*innen in zunehmenden Maße Federführung in der Gestaltung von Cyber Security übernehmen, um die Interaktionsschnittstellen zu anderen kulturellen Räumen, die als potentielle Bedrohung wahrgenommen werden, neu zu organisieren oder gar abzutrennen. Was zunächst skurril erscheinen mag, konstituiert historisch betrachtet jedoch keine unübliche Reaktion, *um souveräne Kontrolle, als das Kennzeichen funktionierender Staatlichkeit*, zu erhalten ([Demchak, 2011, S.276](#)).

### **Konkurrierende Konzeptionalisierungen des Souveränitätsbegriffs als Herausforderung für die multilaterale Zusammenarbeit**

Wie bereits [Müller \(2017, S.3\)](#) hervorhob, übersetzt sich der Konflikt um Internet Governance in der post-liberalen Ära somit in einen komplexen, multidimensionalen Machtkampf, der insbesondere die Frage nach der Zukunft nationaler Souveränität in Zeiten der Digitalisierung in sein Zentrum stellt. Der multilaterale Prozess zu Cyber Security erwuchs so zu einem zentralen Element des machtpolitischen Ringens um Deutungshoheit in der Gestaltung des Internets. Dabei verfolgen divergierende Cybermächte (USA, EU, China, Russland) das Ziel Normen zur Autonomie des Staates in Zeiten der digitalen Vernetzung zu etablieren, wobei sie nach je unterschiedlichen Ordnungsprinzipien agieren, die eine multilaterale Konsensfindung erschweren.

Die chinesische Konzeption von Internet-Souveränität zentriert sich dabei um die Idee, territoriale Grenzen im digitalen Raum durch staatliche Kontrollmechanismen wie Filter- und Zensurmaßnahmen sowie dem Aufbau eines nach außen abgegrenzten digitalen Ökosystems zu verwirklichen. In diesem Sinne handelt es sich jedoch nicht nur um eine nach innen gewandte Konzeption; vielmehr zeichnete sich gerade in den letzten Jahren eine Entwicklung ab, nach der Peking immer

stärker darauf abzielt, Normen zu exportieren, um die digitale Ordnung der Zukunft nach dem chinesischen Bilde zu formen. Dies zeigt sich insbesondere in der Beförderung des chinesischen Modells von Internet Governance in Foren der multilateralen Auseinandersetzung (bspw. UN GGE, Internet Governance Forum, ITU). Dabei erfüllt das Konzept der Internet-Souveränität für Peking zugleich eine doppelte Funktion: einerseits zur Einflussnahme auf sich etablierende Cyber-Praktiken sowie die Bedeutung von Staatlichkeit im Zuge der digitalen Revolution, andererseits zur Erhöhung der Legitimität der Kommunistischen Partei, die sich vor allem dadurch gestärkt sieht, dass sich Regierungen des Globalen Südens in zunehmendem Maße dem chinesischen normativen Rahmenwerk anschließen ([Chen et al., 2017, S.452-453](#)).

Ähnlich wie China propagiert auch Russland eine autoritäre Konzeption von Internet-Souveränität, die darauf abzielt, technische Möglichkeiten zu nutzen, um einen Informationsraum zu schaffen, der sich vom globalen Geschehen abkoppeln lässt. Die Logik der russischen Strategie zur Versicherheitlichung des Internets ist dabei in signifikantem Maße an die Definition der Begriffe ‚Information‘ und ‚Informationssicherheit‘ gekoppelt, in deren Kontext der digitale Informationsraum als Teil des physischen Territoriums betrachtet wird. Hieraus folgt wiederum, ähnlich dem chinesischen Modell, dass sich die Konzepte von Souveränität und territorialer Integrität inhärent mit der Regulation digitaler Informationsflüsse verbunden sehen ([Kovaleva, 2018, S.141-142](#)). Auf der internationalen Bühne resultierte jene Konzeption wiederum in der Akzentuierung völkerrechtlicher Prinzipien zur Erhaltung staatlicher Souveränität im Cyberspace. In der Diskussion stand dabei bspw. das Prinzip der Nichteinmischung (non-intervention), das es nach russischem Bilde von der physischen in die digitale Sphäre zu übertragen galt ([Claessen, 2020, S.146](#)). Hierin zeichnet sich vor allem das innenpolitische Bestreben Moskaus ab, die Autorität und die Verantwortung des Staates vor Entwicklungen aus dem Information Space zu bewahren, um „die Stabilität der konstitutionellen Ordnung sowie die Souveränität und die territoriale Integrität der russischen Ökonomie und Politik zu garantieren, sodass eine wechselseitig wertvolle internationale Kooperation erhalten bleibt [Übersetz. D. Verf.]“ (Doctrine for Information Security, 2000, zitiert nach [Claessen, 2020, S.146](#)).

Wenngleich nicht vorzuenthalten ist, dass Facetten der Konzeption von Internet-Souveränität durch Russland und China variieren, kann man an dieser Stelle zumindest festhalten, dass sie in ihrem Streben nach Abschottung vielzählige semantische Deutungsmuster und strategische Ziele einen, die bedingen, dass beide Staaten multilaterale Foren nicht nur allein, sondern auch gemeinsam nutzen, um ihren Machtradius zu erweitern. Ihr Ziel besteht dabei darin, die Forderung nach mehr staatlicher Handlungsfähigkeit im digitalen Raum zu untermauern, indem sie Reformvorschläge unterbreiten, die die Hegemonie des Multi Stakeholder-Modells unterminieren, um eine diskursive Umdeutung zu initiieren, die bereits bedingt, dass sich das (westliche) Bild des Internets als freies und globales Informations- und Kommunikationsmedium in einem Prozess der Auflösung befindet. Signifikant erweist sich in diesem Zuge nicht nur, dass sowohl Russland als auch China bestehende Foren der multilateralen Zusammenarbeit strategisch nutzen, sondern zugleich selbst neue Foren initiieren, bspw. die *World Internet Conference* (WIC) sowie die *Shanghai Cooperation Organization* (SCO), die über einen *exklusiv zentral-asiatischen Charakter* verfügen ([Deutsche Gesellschaft für die Vereinten Nationen e.V., 2019, S.2](#)).

Blickt man nun in die Riegen westlicher Demokratien, so fällt bereits anhand der Begrifflichkeiten ‚Digitale Souveränität‘ und ‚Cybersicherheit‘, im Gegensatz zu ‚Internet-Souveränität‘ und ‚Informationssicherheit‘, auf, dass wir mit einem divergierenden außenpolitischen Vokabular konfrontiert sind, dessen Bedeutungsgehalte je spezifische Zukunftsvisionen des digitalen Raumes abbilden, die im Rahmen einer globalen digitalen Ordnung nur schwer vereinbar erscheinen. So stützt sich die in Deutschland und anderen westlichen Ländern insbesondere seit 2013 geführte Debatte um Digitale Souveränität zwar auf einige Elemente, die auch die chinesische und russische Konzeption teilen (bspw. Autonomie und technologische Souveränität), indes wird sie jedoch unter komplett anderen Vorzeichen geführt. Vordergründig erweist sich dabei vor allem die *diskursive Verknüpfung des Souveränitäts- und Cybersicherheitsbegriffes mit dem Streben nach der Verwirklichung von Menschen- und Grundrechten*, welche sich bspw. auch in der Charta der Europäischen Union zu Cybersicherheit im digitalen Raum widerspiegelt (European Commission, 2013). Fokussiert wird in diesem Rahmen also ein außenpolitischer Ansatz, nach dem die Etablierung von Normen, Regeln und

Prinzipien, die ein verantwortungsbewusstes Handeln von Staaten im Cyberspace ermöglichen, an erster Stelle steht ([Claessen, 2020, S.152](#)).

Für die multilaterale Praxis staatlicher Akteur\*innen bedeutet dies nun konkret, dass sich das Feld durch divergierende Konzeptualisierungen des Souveränitätsbegriffs geprägt sieht; dabei steht einerseits das Prinzip der Nicht-Einmischung und der Kontrolle des Staates über den Informationsraum, andererseits die Notwendigkeit zur kollektiven Verantwortungsübernahme in der Gestaltung einer sicheren und resilienten Cybersicherheitsarchitektur im Vordergrund ([Barrinha/Renard, 2020, S.757-758](#)). Jener Dissens spiegelt sich nicht nur darin wider, dass sich *die verbindliche Kooperation in Cybersicherheitsbelangen, wenngleich ein allgemeiner Konsens zur Notwendigkeit multilateraler Lösungen besteht, bisweilen auf der bilateralen Ebene abspielt*. Auch institutionell manifestieren sich jene semantischen Disparitäten bereits in der Entwicklung zweier separater Working Groups innerhalb der UN: (1) der UN Group of Governmental Experts (UNGGE), welche das Prinzip des verantwortungsbewussten kollektiven Handelns staatlicher Akteur\*innen in seinen Kern stellt und im Wesentlichen durch die USA geführt wird und (2) die Open Ended Working Group (OEWG), die sich, wenngleich ihr offiziell eine andere Funktion zukommt, um die Verwirklichung des Souveränitätsgedankens im Cyberspace zentriert und unter russischer Führung steht.

### **Multilateralismus neu denken, Multi Stakeholder-Governance reformieren?**

Neben dem Wettbewerb divergierender Konzeptualisierungen des Souveränitätsbegriffs erweist sich für den geopolitischen Prozess, in dem sich eine neue Geographie des Internets herausbildet, zudem eine Narrativ-Verschiebung in der Bedeutung internationaler Zusammenarbeit signifikant. Diese leitet sich daraus ab, dass staatliche Akteur\*innen immer mehr Kontrolle im Bereich der Internet Governance übernehmen, indem sie Debatten über die Ausgestaltung sicherer und stabiler Infrastrukturen in die Riegen intergouvernementaler oder bilateraler Vereinbarungen verlagern. Das bisweilen vorherrschende *Multi Stakeholder-Modell*, dass zivilgesellschaftlichen und industriellen Akteur\*innen die Möglichkeit vermittelt, eine Rolle in der Gestaltung von Internet Governance einzunehmen, *sieht sich im Lichte jener neuen Entwicklungen somit immer stärker durch cyberdiplomatische Dialoge ersetzt oder verdrängt*.

*Der Trend, nach dem das Streben nach staatlicher Kontrolle in der Gestaltung des Cyberspace dem Denken und Handeln autoritärer Staaten zuzusprechen ist, befindet sich demgemäß in Auflösung, da bisweilen auch immer mehr westliche Regierungen den Status Quo des Multi Stakeholder-Systems herausfordern ([Barrinha/Renard, 2020, S.759](#)). Diese Entwicklungen müssen wiederum ausgesprochen kritisch betrachtet werden, wenn man bedenkt, dass sich das Zusammenwirken von staatlichen und nicht-staatlichen sowie technischen und policy-orientierten Expert\*innen-Netzwerken essentiell erweist, um einen offenen und inklusiven digitalen Raum zu erhalten, der sich dazu im Stande sieht, weiteren Fragmentierungserscheinungen zu begegnen ([Liaropoulos, 2016, S.22-23](#)).*

Die Einbindung nicht-staatlicher Akteur\*innen in den multilateralen Prozess zur Entwicklung von Cyber-Normen ist auch insofern erforderlich, da ein normatives Rahmenwerk, das ausschließlich unter staatlichen Akteur\*innen verhandelt wird, auch ausschließlich auf die Bedürfnisse und Praktiken eben jener Akteur\*innen ausgerichtet und nicht explizit darauf zugeschnitten ist, die Handlungen von Unternehmen und zivilgesellschaftlichen Akteur\*innen in der Konfrontation mit Bedrohungen aus dem Cyberspace zu leiten. Gerade Unternehmen sehen sich jedoch in immer höherem Maße durch Cyberkriminalität und Cyberspionage bedroht, während insbesondere die größeren Player (bspw. Microsoft) auch über die Möglichkeit verfügen, jenen Bedrohungen direkt oder indirekt zu begegnen ([Butler/Lachow, 2012, S.3](#)). In dem Prozess, in dem sich Normen zu Verhaltensweisen im Cyberspace herausbilden, gilt es den privaten Sektor somit in einer Art und Weise zu integrieren, die seiner unbestreitbar bedeutenden Rolle in und Verflechtung mit globalen Cyber-Belangen Rechnung trägt.

Eine derartige Integration nicht-staatlicher Akteur\*innen in die multilaterale Kooperation zur Entwicklung von Cyber-Normen würde jedoch zugleich, insbesondere mit Blick auf den Unternehmensektor, eine Entwicklung erforderlich machen, nach der man die naive Vorstellung von Multi Stakeholder-Governance als inhärent demokratiefreundliches System final fallen lässt. Vielmehr bedürfe es einer kritischen Auseinandersetzung unter Theoretiker\*innen und Praktiker\*innen, die den Gebrauch des Begriffs ‚multi stakeholderism‘ in ihr Zentrum stellt, da dieser nur allzu häufig als rhetorisches Mittel genutzt wird, um bestehende Machtasymmetrien im Policy-Prozess zu legitimieren und zu verfestigen. Des Weiteren müsste sich die



Forschung im Kontext einer konstitutionellen Reformation von Multi Stakeholder-Governance auch explizit mit der Gefahr einer Depolitisierung des Normbildungsprozesses zugunsten von Unternehmensinteressen und damit einhergehenden Entwicklungen eines sich digitalisierenden Neoliberalismus auseinandersetzen ([Palladino/Santaniello, 2021, S.153](#)).

Die Erweiterung multilateraler Kooperation um nicht-staatliche Akteur\*innen würde demgemäß eine Vielzahl neuer Fragen für Politik und Wissenschaft aufwerfen, die sich nicht nur um neue Formen oder Funktionen des Multilateralismus, sondern zugleich um einen damit einhergehenden erforderlichen Strukturwandel von Multi Stakeholder-Governance zentrieren würden. In diesem Zuge gelte es wiederum nicht nur neue Prozeduren zu entwickeln, sondern gleichsam kritisch zu hinterfragen, inwiefern sich jene neuen Prozeduren auch noch dazu im Stande sehen, demokratischen Werten der Gleichheit, Partizipation und Inklusion gerecht zu werden, statt sie zu unterminieren.

Klar wird also, dass es sich hierbei um ein schwieriges Unterfangen handelt; angesichts der disruptiven Transformationsprozesse, die der digitale Raum derzeit erlebt, kann es allerdings auch keine einfache Lösung sein, die seiner stetigen Fragmentierung und Polarisierung entgegenwirkt. Im Zuge der multilateralen Zusammenarbeit zur Gestaltung von Internet Governance sollte das Multi Stakeholder-Modell demgemäß nicht allzu schnell entwertet, sondern vielmehr *in einen demokratischeren Kontext gesetzt werden, der neue Akteur\*innen sowie zukünftige demographische Trends in der Entwicklung des Cyberspace inkludiert*. Insbesondere mit Blick auf die derzeitige Diversifizierung von Cybermächten und die schwindende Monopolstellung des globalen Nordens gilt es jenen Aspekt nochmals hervorzuheben. So bedarf es einer Reform partizipativer Verfahren, einer Einbindung von nicht-staatlichen Akteur\*innen sowie eines gewachsenen Willens auch Regierungen des Globalen Südens in Cyber diplomatische Verhandlungen einzubeziehen, wenn man ein inklusives Governance-Modell anstrebt, dass derzeitigen Tendenzen in der Versicherheitlichung der internationalen Cybersicherheitspolitik entgegenwirken kann.

Derzeit erscheint es also umso dringlicher inklusive, multilaterale Lösungen zu finden, die sowohl staatliche als auch nicht-staatliche Akteur\*innen einbinden, um ein verbindliches Rahmenwerk von Normen und vertrauensbildenden Maßnahmen

zu entwickeln, die ein „post-liberales Internet-Governance-System“ ermöglichen. Angesichts der bestehenden Macht-Antagonismen zwischen denjenigen Partizipanten, die über die Autorität und die Ressourcen verfügen, um eine Bandbreite an Aktivitäten im Cyberspace zu regulieren, den Staaten, erscheint eine derartige Vision eines inklusiven post-liberalen Internet-Governance-Systems derzeit allerdings nahezu utopisch. Das sich abzeichnende Bild deutet vielmehr in Richtung einer ‚multi order governance‘ ([Barrinha/Renard, 2020, S.765](#)), in deren Kontext die multilaterale Zusammenarbeit als Brückenbilder zwischen unterschiedlichen Blöcken fungiert, die sich über Zeit ihr je eigenes System des Internet Governance angeeignet haben.