Nr. 313, November 2022

Normen vs. Realitäten: Die Cyberthematik bei der UNO

Nach dem Einmarsch Russlands in die Ukraine geriet die Debatte über Cybernormen bei der UNO in eine Sackgasse. Spannungen zwischen den USA und Russland haben substanzielle Fortschritte blockiert, besonders zu Fragen des Verhaltens im Cyberraum während bewaffneten Konflikten. Andererseits ist der Umstand, dass die UNO-Arbeitsgruppen weiterhin bestehen, zwar nur ein kleines, aber doch ein positives Signal für die Zukunft, genauso wie die zahlreicher werdenden Foren zur Normendebatte ausserhalb der UNO.

Von Taylor Grossman

Als Folge der weltweiten Ausbreitung von Informations- und Kommunikationstechnologien (IKT) in den 1980er und 1990er Jahren standen die Staaten grundlegend neuen regulatorischen Fragen gegenüber: Wie soll dieser Bereich bezüglich nationaler Sicherheit, staatlicher Souveränität, Kriminalitätsbekämpfung und anderen zentralen Gebieten mit staatlichem Vorrechtsanspruch behandelt werden? In diesen frühen Jahren gab es noch keine Abkommen über die Anwendung des Völkerrechts im Cyberraum. Manche Internet-Pioniere der ersten Stunde scheuten staatliche Eingriffe. Der Cyber-Bürgerrechtler John Perry Barlow verfasste 1996 in der Schweiz eine Unabhängigkeitserklärung des Cyberraum. Andere begannen sich mit der Frage zu beschäftigen, ob der Cyberraum ein komplett neues Set von Verhaltensnormen braucht (Vgl. CSS Cyberdefense Report: One, Two, or Two Hundred Internets?).

Fotografisches Porträt einer UN-Flagge auf einem Computer-Motherboard, Oktober 2022.
Entworfen von Kevin Kohler und generiert mit DALL-E OpenAI.

Wegen dieser Ungewissheit bot sich die UNO als wichtige Anlaufstelle für die Entwicklung von Cybernormen an. Im Verlaufe der letzten zwei Jahrzehnte hat die UNO dazu beigetragen, den IKT-Bereich in die bestehenden internationalen Normen und Gesetze, auch in ihre Gründungscharta, zu integrieren und für ein gewisses Mass an Kontinuität des verantwortungsvollen staatlichen Verhaltens in verschiedenen Bereichen gesorgt, indem der Cyberraum in die völkerrechtlichen Bestimmungen zur See, auf dem Land und in der Luft eingebunden wurde. Die UNO bemühte sich insbesondere um gemeinsame Mindestnormen, um die Gefahr zu reduzieren, dass vom Cyberspace Instabilität, Eskalation und Schaden – insbesondere für die

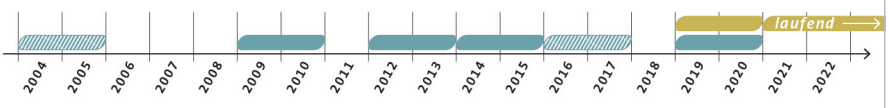
Zivilbevölkerung – ausgeht. Die Schweiz hat bei diesen Anstrengungen eine zentrale Rolle gespielt, von ihrem Engagement für Genf als «Hauptstadt der digitalen Gouvernanz» über ihre Funktion als Vorsitzende früherer Gesprächsrunden über diese Normen im Rahmen der UNO und bis zu ihrem Interesse an Neutralität im Cyberraum (vgl. CSS Cyberdefense Report: The Law of Neutrality in Cyberspace).

Doch trotz dieser ambitionierten Voraussetzung haben die beiden durch die UNO geführten Prozesse – die sechs Gruppen von Regierungssachverständigen (GGEs), die zwischen 2004 und 2021 tagten, und die beiden Offenen Arbeitsgruppen (OEWGs), die seit 2019 tagen – ausser hehren Formulierungen nur wenig erreicht. Grossmächte wie Russland, China und die USA sind in der Regel davor zurückgeschreckt, bei der Formulierung von Cybernormen in spezifische Details zu gehen. Während China manchmal mit Vertretern anderer Staaten zusammengearbeitet hat, um seine eigenen Standpunkte zu fördern, spielte Russland bei beiden UNO-Prozessen eine zentrale Rolle, oft jedoch nur als Störfaktor. Bislang haben sich die Staaten auf die allgemeine Anwendbarkeit des Völkerrechts auf den Cyberraum geeinigt, doch die meisten Staaten haben zu bestimmten Rechtsfragen bisher nicht Position bezogen. Beim humanitären Völkerrecht (HRV) – auch als Kriegsvölkerrecht bekannt – besteht noch weniger Übereinstimmung. Abgesehen von einem allgemeinen Verweis auf seine potenzielle Relevanz im GGE-Konsensbericht von 2021 ist es den UNO-Verhandlungen nicht gelungen, weitere praktische Erkenntnisse zu erarbeiten. Nichtstaatliche Akteure haben inzwischen versucht, eine dominantere Rolle im Normendiskus zu spielen und sich dabei häufig für strengere normative Beschränkungen von staatlichem Verhalten eingesetzt.

Der Krieg, den Russland in der Ukraine führt, hat die fragilen, konsensbasierten UNO-Foren der Normendiskussion noch zusätzlich geschwächt, wie die verfahrenstechnischen und inhaltlichen Hindernisse zeigen, die bei den letzten Sitzungsrunden der Arbeitsgruppen in New York aufgetaucht sind. Die Frühlings- und Sommersitzungen der OEWG über die Sicherheit der IKT und deren Verwendung waren nur dem Namen nach substanziell: Die Arbeitsgruppen haben zwar einen Konsensbericht über Fortschritte erstellt, aber über konkrete Fortschritte lässt sich darin kaum etwas finden. Dieser insgesamt glanzlose Leistungsausweis unterstreicht die wachsende Kluft zwischen der Normendebatte und der Realität internationaler Politik, zumal diese Plattformen sehr wenig unternommen haben, um die aktuelle Situation in der Ukraine zu bewältigen. Der wichtigste Aspekt der Arbeitsgruppen ist aber letztlich, dass sie nach wie vor als Anknüpfungspunkt für Engagement und als Anregung für andere Plattformen der Umsetzung von Normen existieren. Die Schweiz hat sich weiterhin für einen robusten, durch die UNO geführten Prozess eingesetzt und auch mitgeholfen, die Liste der Arbeitsgruppenteilnehmer zu erweitern, was zu einem vielversprechenden Anstieg von Aktivitäten zur Einführung von Normen ausserhalb der UNO geführt hat.

UN-Normenprozesse im Überblick

	Gruppe von Regierungssachverständigen (GGE)	Offene Arbeitsgruppe (OEWG)
Zeitlicher Umfang	~2 Jahre	~2–4 Jahre
Teilnehmende	Mitgliedsstaaten	Mitgliedsstaaten, Nichtregierungsorganisationen
Auswahl der Teilnehmenden	UNO-Generalsekretär	Offen
Anzahl der Teilnehmenden	15–25	100+
Mitgliedschaft	Fest	Flexibel



Konsensbericht
Kein Konsensbericht

Quelle: Angepasst von Reaching Critical Will und DigiWatch

Eine Geschichte von zwei Prozessen

1998 schlug die russische UNO-Delegation einen vorläufigen Tagesordnungspunkt zu IKT vor mit dem Hinweis auf die negativen Auswirkungen, die diese neuen Technologien sowohl auf die internationale Stabilität als auch auf die innerstaatliche Sicherheit haben könnte. Der Erste UNO-Ausschuss für Abrüstung und Internationale Sicherheit (DISEC) bildete schliesslich eine Arbeitsgruppe von Regierungssachverständigen (GGE), mit dem Auftrag, die Frage zu untersuchen – ein heute beliebter Mechanismus für die Prüfung von neuen Themenfeldern durch die Bildung einer konkreten Plattform, auf der Sachverständige zusammenkommen und Handlungsempfehlungen erarbeiten, ohne dass Staaten an verpflichtende Resolutionen gebunden werden. Sechs Arbeitsgruppen von Regierungssachverständigen (GGEs) tagten schliesslich zwischen 2004 und 2021 mit unterschiedlichem Erfolg. Während die erste GGE keinen Konsensbericht zustande brachte, gelang es späteren GGEs, sich vorsichtig voranzutasten. Insbesondere der GGE-Bericht von 2013 hat die Anwendbarkeit des Völkerrechts auf die Verwendung von IKT durch Staaten bekräftigt, und der Bericht von 2015 hat elf unverbindliche Normen für staatliches Verhalten skizziert. Diese GGEs hatten einen eng gefassten Auftrag: Er konzentrierte sich eher auf politische und militärische Fragen als auf technische Aspekte von Cybertechnologien. So schlägt der Bericht von 2015 beispielsweise eine Norm vor, wonach die Staaten davon Abstand nehmen, die kritische Infrastruktur anderer Staaten ins Visier zu nehmen, ohne spezifische Bestimmungen festzulegen bezüglich technischer Methoden oder der Ausnützung von Sicherheitslücken, die gegen kritische Infrastruktur eingesetzt werden könnte.

Nach diesen scheinbaren Durchbrüchen begann sich der GGE-Prozess jedoch auseinander zu entwickeln. Mit den immer komplexer werdenden Fragen konfrontiert, wie die zwei Jahre zuvor formulierten freiwilligen Normen umgesetzt werden könnten, war die GGE von 2017 nicht in der Lage, einen Konsensbericht vorzulegen. Inzwischen schuf Russland eine separate Plattform für die Cybernormdebatte mittels einer neuen Offenen Arbeitsgruppe (OEWG). Die OEWG wurde vordergründig errichtet, um eine stabilere und gleichberechtigtere Teilnahme zu ermöglichen. Doch trotz der angeblichen Vorteile dieses neuen Forums innerhalb der UNO ist der russische Vorstoss diesbezüglich eher als Versuch zu werten, den ohnehin schon heiklen Prozess zu verkomplizierten und zum Scheitern zu bringen. Manche Staaten befürchteten, die OEWG könnte konkurrenzierende, widersprüchliche normative Rahmenbedingungen schaffen, welche

die Wirkung der nichtbindenden GGE-Berichte zusätzlich verwässern würden.

Der GGE-Prozess findet in beschränkter Zusammensetzung statt: Der Generalsekretär wählt die Teilnehmenden zu Beginn aus, wobei die Mitgliederzahl des Gremiums auf wenige Vertreter von Staaten (15-25) limitiert ist. Die Zusammensetzung bleibt zudem während der Tagungsdauer jeder GGE unverändert. Die OEWG dagegen kann schnell einmal zu einem schwerfälligen Gremium werden, da ihm alle 193 Mitgliedstaaten angehören. Die Teilnehmenden müssen nicht an jeder Sitzung teilnehmen und können sich irgendwann im Arbeitsprozess der Arbeitsgruppe nach eigenem Gutdünken einbringen. Die OEWG steht auch Nichtregierungsorganisationen (NGOs) offen: Zivilgesellschaftliche Organisationen und Vertretungen von Wissenschaft und Industrie können eine Mitgliedschaft beantragen und während des Prozesses Feedbacks geben. Akkreditierte Organisationen können als Beobachtende an OEWG-Sitzungen teilnehmen und sich während des gesamten Prozesses an informellen Beratungen beteiligen.

Staaten sind keine monolithischen Akteure im Cyberraum. Die Mehrheit der weltweiten IKT wird privat betrieben.

Die russischen Interessen im Zusammenhang mit Förderung staatlicher Souveränität und innerer Sicherheit stehen zunehmend im Widerspruch zur Stossrichtung der GGEs im Hinblick auf die internationale Beschränkung staatlicher Aktivitäten im Cyberraum. Russlands Fokus auf innerer Sicherheit war beim Vorschlag von 1998 von Anfang an offensichtlich, und auch spätere Äusserungen legten die Betonung mehr auf «Informationssicherheit», einschliesslich der sich aus dem Cyberraum ergebenden «politischen und ideologischen» Bedrohungen, als auf «Cybersicherheit» im engeren, technischen Sinne. Konkret umfasst die Informationssicherheit Fragen zur Moderation und Beschränkung von Inhalten, die ein expliziteres Eingreifen des Staates beim Zugang zu Informationen zulassen im Interesse der Aufrechterhaltung der innenpolitischen Stabilität. Die UNO-Normfindungsprozesse haben in der Regel unverfängliche Begriffe wie «IKT-Sicherheit» benutzt, um dieses Problem zu umgehen, doch die zugrunde liegenden Spannungen zwischen einem offeneren Cyberraum und einem Cyberraum, der erhöhter staatlicher Überwachung unterliegt, behindern Fortschritte in New York und Genf nach wie vor.

Jüngste Entwicklungen

Trotz anfänglicher Vorbehalte gegenüber dem zweigleisigen Prozess im Rahmen der UNO endete das Jahr 2021 mit einem überraschenden Erfolg für Cybernormen. Die sechste GGE schloss mit einem Konsensbericht, der einen vorsichtigen Schritt vorwärts im Bereich des HVR und seiner potenziellen Anwendbarkeit auf die staatliche Verwendung der IKT enthält. Die Schweiz hat sich stark für die Ausweitung des HVR auf Cyberaktivitäten eingesetzt und in Verbindung mit dem GGE-Bericht ein Positionspapier veröffentlicht, das über die Feststellungen des Ersteren hinausgeht und die Haltung vertritt, dass das HVR das hauptsächliche Regelwerk für Cyberoperationen in einem bewaffneten Konflikt darstellt. Die erste OEWG unter dem Vorsitz von Jürg Lauber, dem UNO-Botschafter der Schweiz, hat ebenfalls einen Konsensbericht vorgelegt, der die Feststellungen früherer GGE übernommen und die Wichtigkeit der durch die UNO geführten Debatte über Cybertechnologien im Zusammenhang mit internationaler Sicherheit bekräftigt hat. Botschafter Lauber war zudem federführend beim Versuch, kleinere, regionale Organisationen für die Mitarbeit in der OEWG zu gewinnen, um ein breiteres Spektrum an Fachwissen miteinbeziehen zu können. Im Dezember 2021 wurde eine zweite OEWG eingerichtet, die ihre Arbeit 2025 abschliessen soll.

Russland und die USA haben auch Schritte unternommen, um ihr diplomatisches Engagement im Cyberraum zu festigen. Im Juni 2021 trafen sich der amerikanische Präsident Joe Biden und der russische Präsident Wladimir Putin in Genf zu einem Gespräch über die Möglichkeiten, Spannungen abzubauen und Cyberattacken auf ihre jeweiligen Staaten einzudämmen. In den folgenden Monaten schien die Zahl der Cyberattacken etwas zurückzugehen, und die USA und Russland schlossen eine neue vorläufige Vereinbarung ab, um gegen böswillige Hacker vorzugehen, die auf ihrem Territorium operierten. Im Oktober legten Russland und die USA dem Ersten Ausschuss der UNO-Vollversammlung einen gemeinsamen Vorschlag vor, der die Verpflichtung beider Staaten gegenüber den OEWG- und GGE-Prozessen und den resultierenden Konsensberichten unterstreicht. Fünfzig Staaten haben die Resolution mitunterstützt, worauf sie Anfang November ohne Abstimmung angenommen wurde.

Fast ein Jahr später mutet eine solche Resolution wie ein Relikt aus einer längst vergangenen Zeit an. Der Einmarsch Russlands in die Ukraine im Februar 2022 verursachte grössere Beeinträchtigungen der internationalen Diplomatie, die sich zwangsläufig auch auf den Bereich der Cybernormen auswirken. Das gespannte Verhältnis zwischen den USA und Russland hat Fortschritte im Hinblick auf die November-Resolution nahezu unmöglich gemacht und die Fronten in der laufenden OEWG verhärtet. Der Cyberbereich hat auf den Kriegsschauplätzen in der Ukraine eine wichtige unterstützende Rolle gespielt, auch beim anfänglichen Versuch Russlands, Kiew einzunehmen und beim neuartigen Konzept der ukrainischen IT-Armee. In den Tagen vor dem Einmarsch im Februar griff Russland die Versorgungskette an, was Störungen der Satellitenkommunikation auf dem gesamten Gebiet der Ukraine verursachte. Der Kreml ist auch für die Mehrzahl von *Distributed-Denial-of-Service*-Attacken (DDoS)-und Datenvernichtungskampagnen gegen den ukrainischen Staat und dessen Bevölkerung verantwortlich. Die IT-Armee der Ukraine hat ihrerseits koordinierte Angriffe zur Unlesbarmachung und Überlastung russischer Webdienste, in der Regel durch DDoS-Attacken, durchgeführt. Während der strategische Wert dieser Operationen noch unklar ist, hat die IT-Armee offen Teilnehmer von ausserhalb der Ukraine, einschliesslich in der EU und in NATO-Mitgliedsstaaten rekrutiert. (Vgl. CSS Cyberdefense Report: The IT-Army of Ukraine). Diese Entwicklungen stellen die Schlussfolgerungen früherer Konsensberichte infrage und werfen ein Schlaglicht auf die Sorgfaltspflichten zum Schutz kri-

Weiterführende Literatur

Duncan Hollis, **«A Brief Primer on International Law and Cyberspace»,** *Carnegie Endowment for International Peace,* 14.06.2021.

Camino Kavanagh, **«Ukraine: Cyber Operations and Digital Technologies»,** *Directions Blog,* 22.03.2022.

Louise Marie Hurel, **«The Rocky Road to Cyber Norms at the United Nations»,** *Council on Foreign Relations*, 06.09.2022.

tischer Infrastruktureinrichtungen und zur Klassifikation von Teilnehmenden an bewaffneten Konflikten im Cyberraum.

Rückschritte in der OEWG

Allerdings ist die UNO kaum in der Lage, Fortschritte bei der Bewältigung der Realität des Konflikts durch ihren Normendiskurs zu erzielen. Vielmehr leidet die OEWG unter verfahrenstechnischem Gezänk und thematischem Stillstand. Die Ablehnung der Kandidatur von 32 zivilgesellschaftlichen Organisationen für die Teilnahme an den Sitzungen im Juli in New York machte die Politisierung der Teilnahme an diesem Prozess besonders deutlich. Die meisten Ablehnungen gingen von Russland aus. Das Land hat zwar keine öffentliche Begründung für seine Entscheide gegeben, aber die meisten Organisationen, denen die Teilnahme verweigert wurde, haben einen westlichen Hintergrund. Auch die Ukraine hat eine kleine Anzahl von Organisationen abgelehnt, mit der Begründung, sie seien zu stark mit dem russischen Staat verbunden und könnten somit nicht als nichtstaatliche Teilnehmer im eigentlichen Sinne gelten.

Wegen der Ablehnung von NGOs im Juni verliert der OEWG-Prozess einen entscheidenden Vorteil, der in seiner Offenheit liegt. Der Aufbau der Arbeitsgruppe ermöglicht eine flexiblere und umfassendere Beteiligung von Akteuren an der Normendebatte. Staaten sind keine monolithischen Akteure im Cyberraum. Die Mehrheit der weltweiten IKT ist in privaten Händen und wird privat betrieben; auch die kritische Infrastruktur ist zunehmend nicht mehr in staatlicher Hand. NGOs spielen bereits eine wichtige Rolle bei der faktischen Verwaltung des Cyberraum, von zivilgesellschaftlichen Organisationen, die bedeutendes Fachwissen und erhebliche Kapazitäten für den Umgang mit der Behandlung von Sicherheitsvorfällen und deren Behebung beisteuern, bis zu multinationalen Unternehmen, die einen Grossteil des Internets betreiben. Der Ausschluss dieser Organisationen von der Formulierung und Umsetzung von Normen ist kurzsichtig, da Organisationen wie *Cyber Tech Accords* (ein Konsortium, das bedeutende Interessen des amerikanischen und europäischen Privatsektors im IKT-Bereich vertritt) und FIRST (ein Netzwerk globaler Computersicherheitsreaktionsteams) auch weiterhin eine wichtige Rolle im Cyberraum spielen werden, unabhängig von ihrer Präsenz bei den Sitzungen in New York.

Inhaltlicher Stillstand

Darum wundert es nicht, dass die OEWG sogar noch weniger unternommen hat, um inhaltliche Differenzen zu beseitigen. Selbst im Bereich der vertrauensbildenden Massnahmen – Aktivitäten und Prozesse, die dazu dienen sollen, Spannungen oder Misstrauen zwischen Staaten abzubauen und damit das Eskalations- und Konfliktpotenzial einzudämmen – steckt die OEWG in einer Sackgasse. In früheren Sitzungen wurde eine Cyberkrisen-Hotline nach dem Vorbild des berühmten heissen Drahts zwischen Moskau und Washington zur Vorbeugung von Atomkriegen im Kalten Krieg vorgeschlagen. Doch die OEWG konnte hinsichtlich eines spezifischen Umsetzungsplanes keine Fortschritte erzielen. Selbst eine Empfehlung, die Zusammenarbeit von Computerkrisenreaktionsteams zu vertiefen, wurde aus dem abschliessenden Fortschrittsbericht entfernt. Wenn es der OEWG nicht einmal gelingt, Fortschritte in derart unstrittigen Bereichen zu erzielen, wo kann sie dann noch auf eine gemeinsame Grundlage hoffen?

Die OEWG scheiterte auch bei der Frage des HVR und dessen Anwendbarkeit im Cyberraum. Speziell im Zusammenhang mit dem Krieg Russlands gegen die Ukraine wurde das HVR zu einem wesentlichen Streitgegenstand. Frühere GGEs und die derzeitige OEWG waren ausserstande, über die schwammigsten Verweise auf HVR-Grundsätze hinauszugehen, wie etwa die Erwähnung, dass die Verhältnismässigkeit und das Treffen von Unterscheidungen im Cyberraum relevant sein könnten. Hinsichtlich spezifischer Anwendungen bleiben die Konsensberichte auffällig stumm. Unabhängig von dieser Pattsituation finden Cyberoperationen jedoch immer mehr ihren Platz in bewaffneten Konflikten. Grundsätze des HVR stehen hier eindeutig zur Debatte und Fragen, die sich darum drehen, wer als Kämpfer zu betrachten ist und welche Handlungsweisen verhältnismässig sind, werden irgendwann auch andere Foren der völkerrechtlichen Auseinandersetzung beschäftigen. Im heutigen Klima scheinen Fortschritte bei diesen Fragen jedoch genauso unwahrscheinlich wie sie dringend wären.

Ausblick

Die Stagnation der OEWG ist ein Anzeichen der weiteren Zersplitterung des geopolitischen Umfelds angesichts steigender Spannungen zwischen Russland und dem Westen. Trotz des beschränkten Fortschritts, den sie in diesem Jahr erzielen konnte, betonen einige Mitglieder der Gruppe, dass allein schon deren Weiterbestehen eine vertrauensbildende Massnahme sei. Multilaterale UNO-Foren bleiben wichtige Anlaufstellen für Debatten, besonders wenn man berücksichtigt, dass andere diplomatische Kanäle im Verlaufe des letzten Jahres zusammengebrochen sind. Nur schon die Tatsache, dass sich Russland, die Ukraine, die USA und die EU im März und im Juli dieses Jahres in New York getroffen haben, um über Cybernormen zu reden, mutet wie ein kleines Wunder an. Für die Schweiz ist die Fortsetzung des UN-Normendiskurses ein Zeichen dafür, dass manche Staaten ein beständiges Interesse an einem stabilen, beherrschbaren Cyberraum haben.

Während die Aussichten auf wesentliche Fortschritte kurz- und mittelfristig nicht vielversprechend sind, hat die Schweiz ein klares Interesse an einem glaubwürdigen und offenen UNO-Prozess. Die Schweiz hat sich für eine bedeutsame Einbeziehung von NGOs in den UNO-Prozess eingesetzt; und nicht zuletzt der Schweizer Fürsprache ist es zu verdanken, dass die OEWG auch Normendebatten auf regionaler Ebene und in Nichtregierungsforen ausgelöst hat, die hoffentlich fruchtbarere Resultate hervorbringen werden. Diese Fülle kleinerer Foren der Normendebatte ist ein willkommenes Signal dafür, dass – während der Westen und Russland sich in einem längeren Patt gegenüberstehen – andere Staaten versuchen, sich schrittweise vorwärtszubewegen.

Für mehr zu Perspektiven Cybersicherheitspolitik, siehe CSS Themenseite.

Taylor Grossman ist Senior Researcher im Team Risiko und Resilienz am Center for Security Studies (CSS) der ETH Zürich.

Die **CSS Analysen zur Sicherheitspolitik** werden herausgegeben vom Center for Security Studies (CSS) der ETH Zürich. Das CSS ist ein Kompetenzzentrum für schweizerische und internationale Sicherheitspolitik. Jeden Monat erscheinen zwei Analysen auf Deutsch, Französisch und Englisch.

Herausgeberin: Névine Schepers
Lektorat: Julian Kamasa, Kevin Kohler
Layout und Grafiken: Miriam Dahinden-Ganzoni

Feedback und Kommentare: analysen@sipo.gess.ethz.ch
Weitere Ausgaben und Abonnement: www.css.ethz.ch/cssanalysen

ISSN: 2296-0236; DOI: 10.3929/ethz-b-000578694