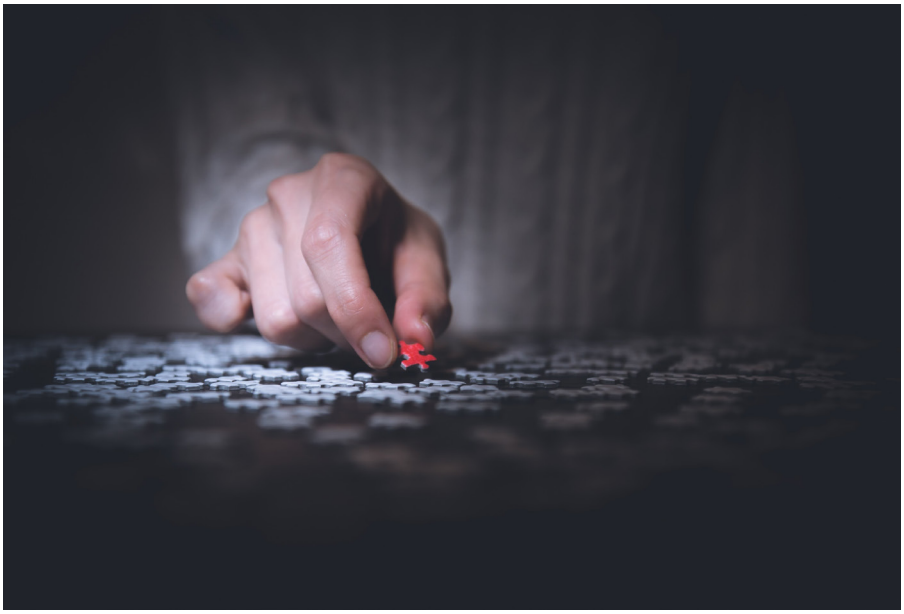
Nr. 244, Mai 2019, Herausgeber: Fabien Merz

Öffentliche Attribution von Cybervorfällen

Cybervorfälle werden vermehrt Verursachern öffentlich zugeschrieben. Diese Attributionen sind aber meist wenig transparent und nachvollziehbar. Zugängliches Wissen über Verursacher eines Cybervorfalls ist aber wichtig für die demokratische Willensbildung und für die internationale Stabilität. Es braucht internationale institutionelle Mechanismen und das Engagement von Staat, Wirtschaft und Gesellschaft, um das Vertrauen in öffentliche Attributionen zu stärken.

Von Florian J. Egloff und Andreas Wenger



Attributionsprozesse sind vielschichtige und meist langwierige Spurensuchen, mit dem Ziel herauszufinden, wer dahintersteckt. *Ryoji Iwata / Unsplash*

Wer steckt hinter einem Cybervorfall? Lange galt die Beantwortung dieser Frage als eine der technisch schwierigeren Herausforderungen – dem ist immer noch so. Das Internet ist so konstruiert, dass eine gewisse technische Anonymität bei Cybervorfällen relativ einfach erreichbar ist. Dies gibt Angreifern einen Vorteil, weil die betroffene Partei zunächst oft nicht weiss, wer den Vorfall verübt hat. Die vielschichtige und meist langwierige Spurensuche nach den Verursachern bezeichnet man als Attributionsprozess. Wenn die betroffene Partei glaubt, den Täter zu kennen, muss sie sich entscheiden, ob und wie sie auf den Cybervorfall reagieren will. Eine Handlungsoption, über die sie dabei verfügt, ist die öffentliche Attribution: die Verantwortung für einen Cybervorfall wird öffentlich einem spezifischen Verursacher zugeschrieben.

Seit einigen Jahren häufen sich die öffentlichen Zuschreibungen von Cybervorfällen durch Staaten und Unternehmen. Auf staatlicher Seite sind die USA sehr aktiv im Bereich der öffentlichen Attribution. Der Akt der Zuschreibung kann dabei in unterschiedlichen Formen erfolgen und reicht von öffentlichen Stellungnahmen über Gerichtsverfahren bis hin zu gemeinsamen Erklärungen mit Koalitionspartnern. Auf Unternehmensseite sind es vor allem Cybersicherheitsfirmen, die in öffentlich zugänglichen Berichten Cybervorfälle einzeln oder in Gruppen gewissen Verursachern zuweisen. Einige dieser Firmen ordnen diese Verursachergruppen zudem direkt der Verantwortung gewisser Staaten zu.

Beide Arten öffentlicher Attribution sind insbesondere für Demokratien politisch bedeutungsvoll. Öffentliches Wissen über digitale Interaktionen zwischen Angreifern und Opfern ist eine Voraussetzung für die demokratische Willensbildung und damit für die politische Legitimität der zur Verfügung stehenden Handlungsoptionen – von Versicherungsfragen über strafrechtliche Verfahren bis hin zu Fragen von Krieg und Frieden – auf nationaler und internationaler Ebene. Mangelnde Transparenz und Rechenschaftspflicht lässt die Gesellschaften darüber im Dunkeln, wie und warum Staaten und Cybersicherheitsfirmen zu ihren öffentlichen Schlüssen kommen. Vorschläge zur internationalen

Gouvernanz und Vertrauensbildung über Attributionsprozesse zeigen, dass Beiträge von Staaten, Unternehmen und Zivilgesellschaft – darunter auch von Universitäten – gefordert sind, um Cybervorfällen effektiver begegnen zu können.

Politische Legitimität

Die politische Legitimität in Demokratien basiert darauf, dass staatliches Handeln nachvollziehbar ist. Transparentes Regierungshandeln im Cybersicherheitsbereich setzt deshalb ein Mindestmass an öffentlicher Attribution voraus. Zwar können präventive und passive Gegenmassnahmen zugunsten der eigenen Cybersicherheit auch ohne Kenntnisse über mögliche Verursacher getroffen werden. Sobald jedoch Gegenmassnahmen gegen spezifische Angreifer ergriffen werden sollen, braucht es die Fähigkeit zu bestimmen, wer hinter dem Vorfall steckt. Sind diese gegeben, stellt sich die Frage, ob die gewonnenen Erkenntnisse öffentlich kommuniziert werden sollen.

Unterschiedliche politische Systeme werden diese Frage unterschiedlich beantworten. Innenpolitisch werden Demokratien öfters als Autokratien Transparenz schaffen müssen, um gewisse Gegenmassnahmen in Form von Zwangsmassnahmen (Strafrecht, Krieg) legitimieren zu können. Allerdings werden auch Demokratien keine Öffentlichkeit schaffen, solange Cyberkonflikte als Teil einer primär nachrichtendienstlichen Auseinandersetzung wahrgenommen werden. Die Janusköpfigkeit aller staatlicher Akteure im Bereich der Cybersicherheit – als Beschützer und als Täter – macht die öffentliche Attribution von Cybervorfällen zu einer politisch höchst umstrittenen Angelegenheit. Die Unterschiede in den innenpolitischen bedrohungspolitischen Auseinandersetzungen verschiedener politischer Systeme bieten wiederum potentielle Angriffsflächen gerade für autoritäre Staaten – aufgrund der Vernetzung der technischen Systeme allerdings nur mit schwer kontrollierbaren strategischen Auswirkungen für alle Beteiligten.

Die beobachtbare strategische Zurückhaltung staatlicher Akteure mit Blick auf den bewussten Einsatz von Cyberoperationen zur Zwangsausübung ist vor diesem Hintergrund zu sehen. Auf der internationalen Ebene geht es einerseits darum, ein Mindestmass an strategischer Stabilität aufrechtzuerhalten. In diesem Zusammenhang sind Attributionsfähigkeiten bei Cybervorfällen entscheidend, denn ohne sie werden herkömmliche Sicherheitsmechanismen in Frage gestellt. Abschreckung und Eskalationskontrolle beruhen darauf, dass die verantwortlichen Täter identifiziert und Gegenmassnahmen eingeleitet werden können. Andererseits ist eine öffentlich nachvollziehbare Attribution auch Voraussetzung für internationale Kooperation im Cyberraum. Wenn Cybernormen den Rahmen geben sollen für verantwortungsvolles Handeln im Cyberraum, setzt dies voraus, dass deren Einhaltung oder Missachtung von anderen Akteuren erkannt werden. Öffentliche Attribution kann in einer solchen Situation als ein Mittel eingesetzt werden, um solche Normenbrüche zu ächten.

> Eine öffentlich nachvollziehbare Attribution ist Voraussetzung für internationale Kooperation im Cyberraum.

Wissensasymmetrie

Öffentliche Attributionen von Cybervorfällen haben in den letzten Jahren zugenommen. Auf staatlicher Ebene ist Cybersicherheit zu einem Kernthema der Sicherheitspolitik geworden. Staaten haben ihre Nachrichtendienste vermehrt auf dieses Thema ausgerichtet und in Attributionsfähigkeiten investiert. Gleichzeitig ist die Handlungsoption der öffentlichen Attribution Teil des Instrumentariums im Bereich der Aussen- und Sicherheitspolitik geworden. Auch auf der Ebene der Unternehmen haben sich die Attributionsfähigkeiten rasch weiterentwickelt. Neue technische Möglichkeiten im Bereich der Cyberforensik und neue Methoden zur Täterbestimmung wurden entwickelt. Heute publizieren Firmen im Cybersicherheitsbereich regelmässig Berichte über sogenannte *Advanced Persistent Threats* (APTs), also professionelle Hackergruppen, die kontinuierlich und mit hoher Ressourcenintensität gezielt gegen ihre Opfer vorgehen.

Allerdings verfügen nur wenige staatliche und private Akteure über professionelle Attributionsprozesse und -fähigkeiten, mit denen sie die politisch verantwortlichen Akteure hinter Cybervorfällen identifizieren können. Es sind dies vor allem Länder mit leistungsfähigen Fernmelde- und Elektronischen Aufklärungssystemen (SIGINT) und einige wenige Unternehmen, die eigene globale Sensornetzwerke betreiben oder durch ihr Geschäftsmodell in globale Datenströme Einsicht haben. Die meisten anderen staatlichen und privaten Akteure besitzen weder die Fähigkeit, Attributionsprozesse zu betreiben, noch das Geld, sich dieses Wissen einzukaufen. Mit Blick auf die Frage der politischen Legitimität des Wahrheitsanspruchs von öffentlichen Attributionen ist diese Wissensasymmetrie problematisch. Wissen, das nicht unabhängig überprüft werden kann, ist politisch manipulierbar – und zwar sowohl von den Wissenden als auch von den Unwissenden.

Mangelnde Transparenz

Die öffentlichen Attributionen von Cybervorfällen durch Staaten und Cybersicherheitsfirmen sind meistens nicht sehr transparent. Auf der Basis der veröffentlichten Informationen sind die Schuldzuweisung nicht im Detail überprüfbar. Dies wiederspiegelt einerseits das Fehlen anerkannter internationaler Standards im Bereich der Attribution. International anerkannte forensische Techniken befinden sich erst im Aufbau. Andererseits besteht auf Eben der Expert*innen oft grössere Einigkeit, als öffentlich sichtbar ist. Dies wiederum ist auf strukturelle Ursachen zurückzuführen, die Staaten und Firmen dazu verleiten, nicht alle vorhandenen Informationen in der Öffentlichkeit transparent darzulegen.

Staaten wägen in der Cybersicherheitspolitik mehrere Interessen gegeneinander ab: Sie verfügen über offensive und defensive Mittel und sie handeln in Unsicherheit über die Motive und Fähigkeiten ihrer Konkurrenten. Trotz strategischer Zurückhaltung sind sie für einen Grossteil der Offensivaktivitäten im Cyberraum direkt oder indirekt verantwortlich. Aufgrund strukturellen Anreize ist die Geheimhaltung von technischen Fähigkeiten und Quellen die Standardantwort von Staaten auf Cybervorfälle. Öffentliche Attributionen dagegen bleiben die Ausnahme. Werden Cybervorfälle öffentlich spezifischen Verursachern zugeschrieben, hat dies immer auch vielschichtige politische Gründe. Viele der bisherigen öffentlichen Attributionen scheinen dabei vor allem aussen- und sicherheitspolitischen Interessen zu dienen. In einem Mindermass werden damit auch innenpolitische Ziele verfolgt.

Die Cybersicherheitsfirmen wiederum haben ein Interesse daran, eine eigenständige Analysefähigkeit öffentlich unter Beweis zu stellen. Ihre Berichte haben einen wichtigen Werbeeffekt in einem Wachstums-

markt. Gleichzeitig haben sie gute strukturelle Gründe, nicht alle ihre Datenquellen offenzulegen. Erstens ist die Datenbasis eines Cybersicherheitsunternehmens ein Geschäftsgeheimnis mit beträchtlichem Marktwert. Zweitens werden die besten Daten oft von Kundennetzwerken gewonnen, die Geheimhaltungsvereinbarungen unterliegen. Drittens haben Cybersicherheitsunternehmen nur eine begrenzte Einsicht in Cyberkonflikte, definiert durch die Technologien, die sie anbieten und die Märkte, in denen sie tätig sind. Dies bedeutet insgesamt, dass Cybersicherheitsfirmen über detailliertes Wissen hinsichtlich einiger Akteure verfügen, wobei nur eine Teilmenge dieses Wissens an die Öffentlichkeit dringt.

Der Prozess der Attribution

Attribution ist eine inhärent interdisziplinäre Aufgabe. Im Falle von Cybervorfällen braucht es dazu ein Fundament an computerwissenschaftlichem Wissen, vor allem in den Bereichen Forensik, Netzwerksicherheit und Schadsoftwareanalyse. Aber auch andere Wissensgebiete, insbesondere Politik-, Ökonomie-, Psychologie-, Verwaltungs- und Rechtswissenschaften, haben wichtige Beiträge sowohl zum Attributionsprozess als auch zum Verständnis von öffentlichen Attributionen beizutragen.

Im Attributionsprozess wird Wissen über den Ursprung eines Cybervorfalls generiert. Dieser Prozess kann analytisch in drei Ebenen gegliedert werden. Auf einer taktischen Ebene wird ermittelt, was genau geschehen ist und wie dabei vorgegangen wurde. Auf der operationellen Ebene werden zusätzliche Erkenntnissen über die Täterschaft hinzugefügt, indem alle nachrichtendienstlichen Quellen beigezogen werden. Auf der strategischen Ebene wird der Vorfall politisch bewertet. Dabei geht es unter anderem darum, die Ursachen des Vorfalls im Kontext weiterer Vorfälle zu erkennen. Am Schluss des Prozesses steht die Entscheidung, ob und welche politischen Konsequenzen aus dem Vorfall gezogen werden sollen. Öffentliche Attribution ist dabei eine von vielen möglichen Handlungsoptionen.

Auf den drei Ebenen sind jeweils verschiedene Akteure involviert. Auf der taktischen Ebene beauftragen Staaten, Firmen oder Einzelpersonen Cybersicherheitsfirmen, die sich auf Vorfallsbewältigung spezialisieren. Behörden werden vor allem dann relevant, wenn es einen Bezug zur nationalen Sicherheit oder zu einem sich anbahnenden Gerichtsfall gibt. Auf der operationellen Ebene sind Attributionsprozesse meist in den Nachrichtendiensten angesiedelt, können aber im Kontext von Gerichtsermittlungen auch bei der Polizei respektive der Staatsanwaltschaft liegen. Auf der strategischen Ebene werden die Handlungsoptionen meist von nationalen Sicherheitsstäben erarbeitet. Dabei werden die Cybervorfälle in einem breiteren aussen- und sicherheitspolitischen Kontext umfassend bewertet. Die Handlungsoptionen sind dementsprechend auch nicht an den Cyberraum gebunden und beinhalten die ganze Bandbreite an politischen Instrumenten.

Institutionelle Mechanismen

Auf internationaler Ebene gibt es keinen institutionalisierten Mechanismus der öffentlichen Attribution im Cybersicherheitsbereich. Neuerdings steigt die Zahl der Stimmen, die einen solchen Mechanismus fordern. Noch zeichnet sich kein Konsens hinsichtlich der Frage ab, welche Akteure sich wie in einen internationalen Attributionsprozess einbringen sollen. Dabei gehen die Vorschläge hinsichtlich dem Grad der Beteiligung von Staaten, Unternehmen und Zivilgesellschaft, der Art und dem Kontext der Cybervorfälle sowie der Organisationsform und der Verbindlichkeit der Regulierung teilweise weit auseinander. Entscheidend hinsichtlich der Glaubwürdigkeit der öffentlichen Attribution ist dabei, welche Akteure – die Industrie, die Staaten oder die Zivilgesellschaft – im Zentrum der vorgeschlagenen Mechanismen stehen.

> Auf internationaler Ebene gibt es keinen institutionalisierten Mechanismus der öffentlichen Attribution.

Industrie-zentrierte Ansätze konzentrieren sich auf die Attribution staatlich gesponserter Cybervorfälle, da diese den Interessen global tätiger Firmen entgegenlaufen können. Bereits 2017 schlug beispielsweise *Microsoft* die Gründung einer unabhängigen Organisation vor, die die Zusammenarbeit zwischen Technologiefirmen im Bereich der Attribution ermöglichen soll. Das primäre Ziel einer solchen Organisation soll eine politisch neutrale Identifizierung und Einordnung von Staaten ausgehender Cybervorfälle sein. Durch die internationale Zusammenarbeit von Cybersicherheitsexpert*innen und die Transparenz über die Daten und Schlussfolgerungen erhofft sich *Microsoft* eine Überbrückung des Vertrauensdefizits, das momentan gegenüber öffentlichen Attributionen besteht.

Auch staaten-zentrierte Ansätze konzentrieren auf die Attribution von staatlichen Cyberkonflikten. Ein Beispiel dafür ist die Anregung einer russischen Denkfabrik, die ein unabhängiges internationales Cyber-(Schieds-)Gericht für Cyberkonflikte zwischen Staaten vorschlägt. Ähnlich sieht das die US-amerikanische Denkfabrik *Atlantic Council*, die einen multilateralen Cyber-Adjudikationsrat für Cybervorfälle empfiehlt, die die Gewaltschwelle eines bewaffneten Konflikts überschreiten. Staaten mit fortgeschrittenen Attributionsfähigkeiten würden diese dem Forum zur Verfügung stellen, während Staaten ohne solche Fähigkeiten ihre Fälle vor das Forum bringen könnten. Das Forum würde Beweise und Empfehlungen an internationale oder regionale Sicherheitsgremien weitergegeben, die über allfällige Sanktionen befinden würden.

Auch einige zivilgesellschafts-zentrierte Ansätze sind bereits lanciert worden. *AccessNow* kritisiert, dass zu viel Gewicht auf die Gründung von Organisationen gelegt werde. Stattdessen schlägt die NGO vor, der Entwicklung von Leitfäden und Beweisstandards mehr Aufmerksamkeit zu

Weiterführende Literatur

Deibert, R. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs, 32* (4), 411–424. Zudem forscht das *CitizenLab* zum Thema der gezielten Cyber Angriffen auf die Zivilgesellschaft.

Grindal, K., Kuerbis, B., Badiei, F., & Mueller, M. (2018). Is it time to institutionalize cyber-attribution? *Internet Governance Project White Paper.*

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies, 38* (1–2), 4–37.

Schulzke, M. (2018). The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty. *Perspectives on Politics, 16* (4), 954–968.

Die USA hat eine gewisse Transparenz über ihre Attributionsmethodologie geschaffen in: Office of the Director of National Intelligence (ODNI) (2018). "A Guide to Cyber Attribution". *U.S. Office of the Director of National Intelligence Publication.*

schenken. Der Direktor des *CitizenLab* in Toronto, Ronald J. Deibert, wiederum bringt ein Netzwerk von universitären Instituten in die Debatte, die verteilte, transparente und durch die Wissenschaft begutachtete Forschung zu Cybervorfällen betreiben. Nochmals anders sieht dies die US-Denkfabrik *RAND Corporation,* die ein ständiges globales Konsortium nichtstaatlicher Akteure empfiehlt, das sich auf Attribution der wichtigsten Cybervorfälle konzentriert.

Alle diese Empfehlungen versuchen die Wissensasymmetrie im Bereich der öffentlichen Attribution abzubauen und dem damit verbundenen Misstrauen gegenüber öffentlichen Attributionen entgegen zu wirken. Alle Vorschläge gehen davon aus, dass öffentlichen Attributionen dann vertraut wird, wenn sie durch ein internationales Expertennetzwerk transparent begutachtet werden. Allerdings macht es aus politischer Perspektive einen Unterschied, ob es sich um staatlich gesponserte Vorfälle handelt oder nicht. Bei staatlichen Cyberkonflikten braucht es für die politische Reaktion zwingend den Einbezug öffentlicher Akteure, bei nichtstaatlichen Vorfällen hingegen lediglich den Austausch mit Staaten. Daraus lässt sich ableiten, dass es ein Netzwerk internationaler Mechanismen braucht, im dem sich staats-, industrie- und zivilgesellschaftszentrierte Ansätze wechselseitig ergänzen. Die Attributionsfähigkeiten werden dezentral aufgebaut und basieren auf nationalen und regionalen, staatlichen und nichtstaatlichen Vertrauensstrukturen. Mit Blick auf die politische Reaktion, die Sanktionsfrage und die internationale Stabilität müssen diese dezentralen Strukturen allerdings zwingend an bestehende regionale und globale Sicherheitsinstitutionen angedockt werden.

> Universitäten können eine wichtige vertrauensbildende Rolle übernehmen.

Die Rolle der Universitäten

Die Entwicklung eines tragfähigen Governanz-Rahmens für die öffentliche Attribution von Cybervorfällen braucht das Engagement von Staat, Wirtschaft und Gesellschaft. Auch Universitäten können in diesem Zusammenhang eine wichtige vertrauensbildende Rolle übernehmen. Sie erarbeiten und geben öffentliches, transparentes und begutachtetes Wissen weiter und können damit auch der skizzierten Wissensasymmetrie im Bereich der öffentlichen Attribution von Cybervorfällen entgegenwirken. Zwei unterschiedliche Beiträge – Forschung und Netzwerkbildung – können dabei unterschieden werden.

Einerseits können Universitäten interdisziplinäre und begutachtete Forschung zur Attributionsproblematik betreiben. Die Erforschung der Prozesse der öffentlichen Attribution erfordert eine Integration von technischer, organisatorischer und politischer Expertise. Grundlagenforschung kann das Fundament liefern, auf dem internationale Beweisstandards aufgebaut und verifiziert werden. Forschung kann erklären, wie Beweisstandards und Normen in der praktischen Attributionsarbeit entstehen. Forschung kann ferner auch zur Beantwortung der Frage beitragen, wie internationale Mechanismen der öffentlichen Attribution und damit verbundene Gouvernanz-Netzwerke konkret ausgestaltet werden können.

Andererseits können Universitäten auch zur Erforschung von digitalen Konflikten beitragen. Universitäre Labs, die über eine eigenständige interdisziplinäre Attributionsexpertise und eine eigenständige Datenbasis verfügen, könnten die vielschichtigen Realitäten von Cyberkonflikten erforschen. Als Konsortium könnte ein Netzwerk von universitären Institutionen, die eigenständig Cyberkonflikte erforschen, wesentlich zur Erweiterung des öffentlichen Wissens in diesen gesellschaftlich und politisch wichtigen Fragen beitragen. Der Aufbau von interdisziplinärem Wissen im Bereich der Attribution und die Verankerung dieses Wissens in der Ausbildung der nächsten Generation von Analyst*innen ist für ein besseres Verständnis digitaler Konflikte unerlässlich.

Dr. Florian J. Egloff ist Senior Researcher in Cybersecurity am Center for Security Studies (CSS) der ETH Zürich und Research Associate am Centre for Technology & Global Affairs an der Universität Oxford.

Prof. Dr. Andreas Wenger ist Professor für Internationale und Schweizer Sicherheitspolitik an der ETH Zürich und leitet das Center for Security Studies (CSS) an der ETH Zürich.

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

Herausgeber: Lisa Watanabe, Fabien Merz, Benno Zogg
Lektorat: Benno Zogg
Layout und Infografiken: Miriam Dahinden-Ganzoni
ISSN: 2296-0236; DOI: 10.3929/ethz-b-000340834

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

Zuletzt erschienene CSS-Analysen:

Komplexität aufschlüsseln im ukrainischen Friedensprozess Nr. 243
Der Ukrainekrieg und westliche Militärstrategie Nr. 242
PESCO-Rüstungskooperation: Potenzial und Bruchlinien Nr. 241
Die Koreas nähern sich an: Chancen und Hürden Nr. 240
Mehr Kontinuität als Wandel im Kongo Nr. 239
Militärtechnologie: Mythos Imitation Nr. 238