G | G A Focus | GLOBAL

Julia Grauvogel und Christian von Soest

# Cybersanktionen: Zunehmende Anwendung eines neuen Instruments

GIGA Focus | Global | Nummer 3 | April 2021 | ISSN 1862-3581

Am 15. April 2021 hat US-Präsident Joe Biden umfangreiche Sanktionen gegen Russland wegen Cyberangriffen in Kraft gesetzt. Unter anderem wurden zehn russische Diplomaten ausgewiesen und 38 Organisationen, Unternehmen und Personen direkt sanktioniert. Die Regierung wirft ihnen vor, in die US-Wahlen eingegriffen und weitere Hackerangriffe (sogenannte SolarWinds-Hacks) ausgeführt zu haben. Im Vergleich dazu setzt die EU das Instrument der Cybersanktionen noch zurückhaltend ein.

- Im Jahr 2020 verhängte die EU erstmals Kontensperrungen und Einreisebeschränkungen gegen Individuen und Organisationen, die an Cyberangriffen auf Firmen, Behörden und den Deutschen Bundestag beteiligt waren.

- Eine zentrale Voraussetzung für die Anwendung von Cybersanktionen ist die *technische Zurechnung* eines Cyberangriffs, d.h. die Ermittlung der Täterinnen und Täter. Zunehmend handeln diese offensichtlich auch im Auftrag von Staaten wie Nordkorea oder Russland. Die EU betont jedoch, dass die *politische Zuschreibung* staatlicher Verantwortung weiter die souveräne Entscheidung eines jeden einzelnen EU-Mitgliedsstaates bleibt.

- Die Cybersanktionen zielen auf die für Hackerangriffe verantwortlichen Personen und sollen als Strafe, aber auch als weithin sichtbares Signal nach außen wirken. Dagegen ist zweifelhaft, ob Cybersanktionen bei den Täterinnen und Tätern zu einer Verhaltensänderung führen. Dies wird als zentrales Ziel für traditionelle Sanktionen formuliert.

- Die Koordination mit internationalen Partnern wie den USA, die bereits seit dem Jahr 2015 über ein Cybersanktionsregime verfügen, oder auch den Vereinten Nationen verläuft nur schleppend.

## Fazit

*Cybersanktionen dienen auch zur Abschreckung zukünftiger Cyberangriffe. Daher können Hackerangriffe auf Drittstaaten oder internationale Organisationen ebenfalls sanktioniert werden. Es fehlt jedoch innerhalb der EU, vor allem aber im globalen Süden, an technischen Voraussetzungen, um die immer häufiger werdenden Angriffe aufspüren und zuordnen zu können. Die EU sollte daher in die Stärkung eigener technischer Kapazitäten für die Prävention und Reaktion (und in „Cyberentwicklungszusammenarbeit“) investieren.*

**Dr. Julia Grauvogel**
Senior Research Fellow
julia.grauvogel@giga-hamburg.de

**Dr. Christian von Soest**
Lead Research Fellow
christian.vonsoest@giga-hamburg.de

**German Institute for Global and Area Studies (GIGA)**
Leibniz-Institut für Globale und Regionale Studien
Neuer Jungfernstieg 21
20354 Hamburg

www.giga-hamburg.de/de/publikationen/giga-focus/

## Die wachsende Bedrohung durch Cyberangriffe

Hackerangriffe werden ein immer größeres Problem: Die Europäische Arzneimittelbehörde EMA wurde Ende des Jahres 2020 Opfer eines Cyberangriffs. Nach Angaben der Pharma-Hersteller BioNTech und Pfizer konnten sich die Hackerinnen und Hacker dabei Zugriff auf Dokumente zum Coronavirus-Impfstoff der beiden Unternehmen verschaffen. Zu Beginn des Jahres 2021 gab es in Thüringen einen Cyberangriff auf die Internetplattform des Landes zur Vergabe von Impfterminen.

Cybersicherheit wurde in Deutschland erstmals infolge der Angriffe der „Fancy Bear"-Hackergruppe auf den Deutschen Bundestag im Jahr 2015 in einer breiteren Öffentlichkeit diskutiert. Im März 2021 attackierten Hackerinnen und Hacker durch gefälschte E-Mail-Nachrichten (Phishing-E-Mails) die Konten von mindestens sieben Bundestagsabgeordneten. Es wird vermutet, dass der russische Geheimdienst GRU hinter dem Angriff steckt (*Spiegel* 2021). Die jüngsten Cyberangriffe auf IT-Infrastruktur im medizinischen Bereich, aber auch die oftmals abrupte Umstellung auf digitales Arbeiten infolge der Pandemie haben die Cybersicherheitsprobleme weiter verschärft. Dabei zeigt sich die Verwundbarkeit von vernetzen Gesellschaften durch stetig zunehmende Angriffe in der digitalen Welt. Cybersicherheit darf dabei nicht in erster Linie militärisch oder technisch verstanden werden, sondern ist die Grundlage für demokratische politische Prozesse und wirtschaftlichen Austausch in freien Gesellschaften. Die Gefahren durch Attacken bestehen vor allem in drei sich oftmals überschneidenden Bereichen:

1. Schädigung und Zerstörung von IT-Infrastruktur, wie zum Beispiel des Deutschen Bundestags im Jahr 2015,
2. Abgreifen von Informationen, wie beim Angriff auf die Europäische Arzneimittelbehörde EMA und den Bundestag und
3. Gezielte Verbreitung von Fehlinformationen durch Desinformationskampagnen im digitalen Raum, wie im Zusammenhang mit den US-Präsidentschaftswahlen 2016.

Dabei können die Verursacherinnen und Verursacher von Cyberattacken sowohl staatliche Stellen (z.B. Geheimdienste) als auch nichtstaatliche Akteure (z.B. Kriminelle) sein. Das Gleiche gilt für die Ziele der Angriffe. Insbesondere bei Täterinnen und Tätern ist aber eine trennscharfe Unterscheidung staatlicher und nichtstaatlicher Akteure schwierig, wenn beispielsweise Geheimdienste mit kriminellen Einzelpersonen oder Organisationen zusammenarbeiten. Außerdem richten sich globale Cyberangriffe oftmals sowohl gegen private Unternehmen als auch gegen öffentliche Einrichtungen. So griff die Schadsoftware „WannaCry" im Mai 2017 die IT-Infrastruktur von Krankenhäusern in England und Schottland, aber auch die der Deutschen Bahn und der Automobilhersteller Nissan und Renault an.

In der Regel kommen die Hackerangriffe aus dem Ausland; ein zentrales Problem ist dabei jedoch die Zuordnung („Attribution") der Attacken. Die Identifizierung der Täterinnen und Täter und die Abwehr der Angriffe im digitalen Raum bedarf technischer Fähigkeiten und klarer Abläufe. In Deutschland gibt es bislang keinen einheitlichen Prozess zur Beantwortung feindlicher Cyberoperationen aus dem Ausland von nationaler Tragweite (Herpig 2021). Die Europäische Union nutzt zunehmend das Instrument der Sanktionen, um Cyberangriffe zu bestrafen und mögliche Täterinnen und Täter abzuschrecken. Seit drei Jahren verfügt die EU über einen sogenannten Cyberdiplomatie-Werkzeugkasten, der den Rahmen für einen

europäischen Umgang mit Cyberbedrohungen definiert. Bei dessen Verabschiedung im Jahr 2017 ging es jedoch zunächst vor allem um ein gemeinsames Verständnis bestehender Bedrohungen und möglicher Reaktionen. Neben der gemeinsamen Reaktion auf böswillige Cyberaktivitäten sollen zukünftige Angriffe durch technische Prävention und Abschreckung verhindert werden. Eine besondere Rolle bei der Reaktion und Abschreckung spielt das Instrument der Cybersanktionen. Der Rechtsrahmen für restriktive Maßnahmen – wie Sanktionen im EU-Kontext bezeichnet werden – in Reaktion auf Cyberangriffe wurde im Jahr 2019 verabschiedet und im darauffolgenden Jahr erstmals angewandt. Die Auslöser waren ein versuchter Angriff auf die Organisation für das Verbot chemischer Waffen (OVCW) sowie weitere böswillige Cyberaktivitäten gegen global tätige Unternehmen und Ministerien sowie Behörden verschiedener Länder.

## Eine neue Art der Sanktionen?

Cybersanktionen sind ein zentrales Beispiel für die dynamische Entwicklung von Sanktionen als Mittel der Außenpolitik. Zunehmend zielen diese „individuellen Sanktionen“ (von Soest 2019) auf verantwortliche Personen und nicht auf ganze Staaten und Volkswirtschaften. Mit ihrem Ratsbeschluss 2019/797 zu Cybersanktionen hat die EU im Mai 2019 einen neuen rechtlichen Rahmen für restriktive Maßnahmen in diesem Politikfeld geschaffen (Europäischer Rat 2019). Diese sind Teil eines Trends zu themenspezifischen Sanktionsmechanismen. Bereits im Jahr 2018 beschlossen die EU-Mitgliedsstaaten eine Regelung zu restriktiven Maßnahmen in Reaktion auf den Einsatz von Chemiewaffen. Im vergangenen Jahr wurde außerdem ein „horizontales“ Sanktionsregime bei Menschenrechtsverletzungen verabschiedet (Portela 2019).

Dies bedeutet nicht, dass zuvor keine EU-Sanktionen in diesem Themenfeldern beschlossen werden konnten. Die neuen Regelungen sollen vielmehr dazu führen, dass restriktive Maßnahmen einfacher und schneller verhängt werden können. Sie dienen daher auch der Abschreckung, wie die EU in ihren entsprechenden Beschlüssen betont. Der entscheidende Vorteil aus Sicht der „Sanktionierer“ wie der EU besteht darin, dass diese „horizontalen“ Sanktionen auf die verantwortlichen Personen und nicht wie die klassischen, umfassenden Sanktionsregime auf Staaten abzielen.

Die EU muss somit keinen Umweg über die Heimatstaaten der Hackerinnen und Hacker nehmen, sondern setzt nur bei ihnen selbst an. Sie nimmt damit potenziell auch geringere politische Verwerfungen mit Zielstaaten wie Russland, Nordkorea oder der Volksrepublik China in Kauf. Während die technische Zurechnung der Täterinnen und Täter eine Voraussetzung für Cybersanktionen ist, betont die EU, dass ihre Sanktionen keine politische Zuschreibung staatlicher Verantwortung bedeuten (Beschluss 2019/797, Europäischer Rat 2019). Letzteres bleibe eine souveräne Entscheidung jedes einzelnen Mitgliedsstaates.

Die Sanktionsforschung unterscheidet grundsätzlich drei mögliche Wirkungen von Sanktionen: Eine Verhaltensänderung des Sanktionsziels („coercing“), die Einschränkung der Handlungsmöglichkeiten des Ziels („constraining“) und das Senden eines Signals, dass eine rote Linie überschritten wurde und bestimmte internationale Normen verletzt wurden („signalling“) (Giumelli 2011). Cybersanktionen

zielen direkt auf die für Hackerangriffe verantwortlichen Personen und sollen als Strafe, aber auch als weithin sichtbares Symbol nach außen wirken. Sie bekräftigen damit Cybersicherheit als Norm, zeigen die Handlungsfähigkeit der EU als Akteurin und sollen andere potenzielle Täterinnen und Täter abschrecken. Im Kern geht also eine Signalwirkung („signalling") von Cybersanktionen aus. Die Forschung betont dabei die Bedeutung einer möglichst großen und einheitlichen Unterstützung für die Sanktionierer, um ein kohärentes und schwer zu delegitimierendes Signal zu senden (Grauvogel und von Soest 2014). Außerdem wird der Bewegungs- und Handlungsspielraum von sanktionierten Hackerinnen und Hackern eingeschränkt („constraining"). Dagegen ist zweifelhaft, ob Einreiseverbote und Kontensperrungen tatsächlich eine Verhaltensänderung der Täterinnen und Tätern erzwingen können („coercing"). Dies wird als zentrales Ziel für umfassende Sanktionen wie Handelsembargos formuliert, spielt bei Cybersanktionen hingegen eine untergeordnete Rolle.

## Cybersanktionen im internationalen Vergleich

Sanktionen werden in der Außenpolitik oft als Mittelweg zwischen Dialog und militärischer Intervention verstanden. Eine solche Rolle spielen sie auch bei der Reaktion auf Cyberbedrohungen. Die aktivsten Anwender von Sanktionen weltweit – die USA, die Europäische Union und die Vereinten Nationen – finden jedoch nur langsam eine Antwort auf die neuen Bedrohungen im digitalen Raum und haben bisher keinen einheitlichen Zugang zu Cybersanktionen entwickelt.

### Die Europäische Union

Die europäischen Cybersanktionen sind zentraler Bestandteil des Cyberdiplomatie-Werkzeugkastens der EU. Die EU betont in ihrem Beschluss aus dem Jahr 2017, in der Cyberdiplomatie vom „gesamten Spektrum aller Instrumente" der Gemeinsamen Außen- und Sicherheitspolitik (GASP) Gebrauch zu machen (EU Kommission 2017). Dennoch lag der Schwerpunkt zunächst auf internationaler Zusammenarbeit. Entsprechend dieser Prämisse, internationalem Dialog Vorrang einzuräumen, wurde das Vorgehen bei Cyberangriffen erst im Jahr 2019 explizit um Sanktionen ergänzt.

Voraussetzung für die Verhängung von EU-weiten Sanktionen ist eine „erhebliche Wirkung" des Cyberangriffs. Da auch versuchte, aber abgewehrte feindliche Cyberoperationen sanktioniert werden können, ist in diesem Fall die potenziell erhebliche Wirkung ausschlaggebend. Artikel 2 der Durchführungsverordnung enthält eine Liste, die zur Beurteilung der Auswirkung herangezogen werden soll: Entscheidend ist demnach „Umfang, Ausmaß, Wirkung oder Schwere der verursachten Störung" in Hinblick auf den wirtschaftlichen oder gesellschaftlichen Schaden und die öffentliche Ordnung (Europäischer Rat 2019). Auch die Anzahl der betroffenen Personen, Firmen und EU-Mitgliedsstaaten, die Höhe des ökonomischen Schadens bzw. Nutzens für die Hackerinnen und Hacker sowie die Menge und Art der gestohlenen Daten sind weitere Indikatoren. Bei den Kriterien handelt es sich jedoch um eine nicht abschließende Liste. Die Quantifizierung von Schäden ist schwierig und

im Fall von versuchten Angriffe fast unmöglich, sodass es sich letztlich um eine politische Einzelfallentscheidung handelt, ob der Schaden als erheblich eingestuft wird (Pawlak and Biersteker 2019: 36).

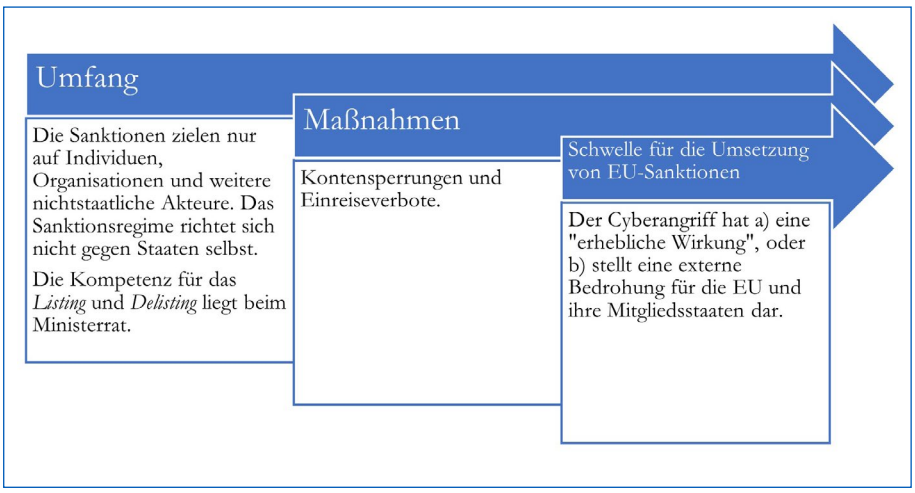


**Abb. 1**
**EU-Cybersanktionsregime**
*Quelle: Eigene Zusammenstellung.*

Sanktionen beschränken sich nicht nur auf Fälle, in denen EU-Mitgliedsstaaten direkt betroffen sind. Auch Cyberangriffe auf Drittstaaten oder internationale Organisationen können sanktioniert werden, wenn dies im Sinn der Gemeinsamen Außen- und Sicherheitspolitik ist. Die vorgesehenen Maßnahmen umfassen das Einfrieren wirtschaftlicher Güter und Reisebeschränkungen. Wie bei anderen zielgerichteten Maßnahmen der EU richten sich die Cybersanktionen nur gegen natürliche und juristische Personen, also z.B. Organisationen und Gruppen, die nicht in der EU ansässig sind. Bei den ersten Cybersanktionen waren dies eine nordkoreanische Organisation, die in Zusammenhang mit der Schadsoftware „WannaCry“ gebracht wird, eine chinesische Gruppe, die den Hackerangriff „Cloud Hopper“ unterstützte, und eine Einheit des russischen Geheimdienstes GRU, die für „NotPetya“ verantwortlich gemacht wurde. Für EU-Staatsangehörige und Firmen hingegen ist das Mittel der Strafverfolgung durch Staatsanwaltschaft und Polizei der Mitgliedsstaaten vorgesehen. Neben den direkten Verantwortlichen können auch Personen oder Organisationen belangt werden, die feindliche Cyberoperationen nicht selbst organisieren, sondern unterstützen.

## Die USA

Bereits seit sechs Jahren – und damit deutlich länger als die EU – setzen die USA auf Cybersanktionen (siehe Tabelle 1). Die von Präsident Joe Biden am 15. April 2021 verhängten umfangreichen und harten Cybersanktionen gegen russische Entscheidungsträgerinnen und Entscheidungsträger, Unternehmen und Organisationen stellen dabei einen vorläufigen Höhepunkt der Nutzung des Instruments dar. Bereits im Januar 2015 erweiterten die Vereinigten Staaten ihre Sanktionen gegenüber Nordkorea unter Verweis auf die dem Land zugeschriebenen Cyberangriffe auf den japanischen Elektronikkonzern Sony. Die US-Regierung verhängte Einreiseverbote und sperrte die Konten von zehn Personen. Seit dem 1. April 2015 definiert die Executive Order 13694 ein einheitliches Vorgehen für die Verhängung von Sanktionen gegen Hackerinnen und Hacker sowie Einrichtungen, die für böswil-

lige Cyberaktivitäten verantwortlich oder zumindest mitschuldig sind. Die Regierung kann auf dieser Grundlage Cybersanktionen schneller aussprechen. Die US-Verordnung sieht Kontensperrungen und Einreisebeschränkungen vor und richtet sich gegen Personen und Firmen, die (überwiegend) außerhalb der USA ansässig sind. Sanktionen können verhängt werden, wenn die Cyberangriffe eine Gefahr für die Sicherheit oder Wirtschaft der Vereinigten Staaten darstellen. Anders als beim Menschenrechtsregime gibt es aber bisher keinen rechtlichen Rahmen durch ein Gesetz des Kongresses.

| | EU | USA |
|---|---|---|
| Erster Anwendungsfall | 2020 | 2015 |
| Rechtlicher Rahmen | 2017/19 | 2015 |
| Anwendungsbereich | Cyberangriffe mit (potenziell) erheblicher Wirkung | Cyberangriffe, die eine Gefahr für die Sicherheit oder Wirtschaft der Vereinigten Staaten darstellen |
| Sanktionsziele | Natürliche und juristische Personen außerhalb der EU | Natürliche und juristische Personen überwiegend außerhalb der USA |
| Maßnahmen | Kontensperrungen und Einreisebeschränkungen | Kontensperrungen und Einreisebeschränkungen |

**Tab. 1**
**Cybersanktionen von EU und USA**
*Quelle: Eigene Zusammenstellung.*

### Die Vereinten Nationen

Seitens der Vereinten Nationen, einem der wichtigsten Sanktionssender weltweit, gibt es bisher keine spezifischen Regelungen zu Cybersanktionen. Im Jahr 2002 wurde eine Gruppe von Regierungsexperten der Vereinten Nationen für „Entwicklungen auf dem Gebiet der Information und Telekommunikation im Kontext der internationalen Sicherheit“ (United Nations Group of Governmental Experts, UN GGE) ins Leben gerufen. Die dritte UN GGE stellte in ihrem Bericht aus dem Jahr 2013 einstimmig fest, dass die UN-Charta auch im Cyberraum gilt.

Im Lauf der Zeit zeigten sich jedoch Divergenzen bei den Expertinnen und Experten, die aus den fünf ständigen Mitgliedern des Sicherheitsrats stammen und darüber hinaus nach regionalem Proporz ausgewählt wurden. So herrscht beispielsweise Uneinigkeit, inwiefern die in der UN-Charta beschriebenen Gegenmaßnahmen – also potenziell auch Sanktionen nach Artikel 41 – in Reaktion auf feindliche Cyberoperationen ergriffen werden können. Aber auch andere sonst aktive Sanktionierer wie die Afrikanische Union oder die Westafrikanische Wirtschaftsgemeinschaft ECOWAS haben bislang keine Cybersanktionen verhängt. Während bereits in der EU aus politischen, rechtlichen und technischen Gründen die Anwendung von „restriktiven Maßnahmen“ gegen Cyberangriffe eine Herausforderung darstellt, hinken andere Regionen noch weiter hinterher.

## Zögerliche Anwendung von Cybersanktionen durch die EU

Die EU hat von dem neuen Instrument bisher nur sehr eingeschränkt Gebrauch gemacht. Im Juli 2020 beschloss der Ministerrat erstmals Sanktionen gegen In-

dividuen und Organisationen. Dabei handelt es sich um zwei chinesische und vier russische Staatsangehörige sowie um drei Organisationen. Neben einer nordkoreanischen und einer chinesischen Gruppe, die Cyberangriffe technisch, finanziell und materiell unterstützt haben sollen, betreffen die Maßnahmen auch das Hauptzentrum für Spezialtechnologien des russischen Militärgeheimdienstes GRU. Alle sanktionierten Personen und Organisationen sollen an dem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) bzw. den als „Wanna Cry", „NotPetya" und „Operation Cloud Hopper" bekannt gewordenen Cyberoperationen beteiligt gewesen sein. Von diesen drei Angriffen mit globalem Ausmaß waren internationale Unternehmen, aber auch Ministerien und Behörden in verschiedenen europäischen und außereuropäischen Ländern betroffen. Die Sanktionsmaßnahmen umfassen neben einem Einreiseverbot in die EU und dem Einfrieren von Konten auch das Verbot jeglicher finanzieller Transaktionen mit den sanktionierten Personen und Firmen. Die Sanktionsliste wurde im Oktober 2020 um zwei Individuen und eine Organisation ergänzt, die mit dem Hackerangriff auf den Deutschen Bundestag im Jahr 2015 in Verbindung gebracht werden.

Begründet werden die EU-Cybersanktionen damit, dass die Cyberangriffe einen „beträchtlichen Schaden und wirtschaftlichen Verlust in und außerhalb der Union angerichtet" haben (Beschluss 2020/1127, Europäischer Rat 2020a) und eine „externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen" (Verordnung 2020/1536, Europäischer Rat 2020b). Trotz der ersten Anwendung stellen sich verschiedene juristische, politische und technische Herausforderungen.

## Individuelle Schutzrechte

Auffällig ist, dass sowohl die Beschreibung des entstandenen Schadens als auch die Zurechnung zum sanktionierten Verhalten, also der Nachweis der Täterschaft, verglichen mit anderen Sanktionsbeschlüssen äußerst detailliert ausfallen. Dies entspricht einerseits dem Trend, EU-Sanktionen zunehmend besser zu begründen und damit „gerichtsfest" zu machen. Sanktionierte Personen oder Firmen klagen mittlerweile regelmäßig gegen die EU-Beschlüsse beim Gericht der Europäischen Union in Luxemburg und waren damit in der Vergangenheit mitunter erfolgreich. Um dies zu verhindern, wurde die Messlatte für Belege des sanktionierten Fehlverhaltens zunehmend höher gelegt. Aus Sicht der sanktionierenden Regierungen ergibt sich das Problem, dass diese nur öffentlich zugängliche Informationen für die Begründung der Auswahl einzelner Sanktionsziele („Listings") nutzen können, um ihre Geheimdienstquellen nicht offen legen zu müssen und diese damit zu gefährden.

## Attribution

Andererseits verweist die ausführliche Begründung aber auch auf die besondere Bedeutung der sogenannten Attribution im Fall von Cyberangriffen. Attribution bezeichnet schlicht den Versuch, feindliche Cyberoperationen mit ihren Urhebern in Verbindung zu bringen. Dabei wird zwischen der technischen Zuordnung – die sowohl die Identifikation der Computer und Netzwerke als auch die der dahinter-

stehenden Individuen umfasst – und der politischen Zuschreibung unterschieden (Egloff 2020; Herpig 2021). Während die technische Zurechnung eine Voraussetzung für Cybersanktionen ist, betont die EU, dass Sanktionen keine politische Zuschreibung staatlicher Verantwortung, der hinter den Täterinnen und Tätern stehenden (staatlichen) Auftraggeberinnen und Auftraggeber, darstellen (Beschluss 2019/797, Europäischer Rat 2019). Letzteres bleibe eine souveräne Entscheidung jedes einzelnen Mitgliedsstaates. Da sich die EU-Cybersanktionen nicht gegen Staaten, sondern gegen juristische oder natürliche Personen richten, erfordern sie keine politische Zuschreibung.

### Unterschiedliche Positionen und Kapazitäten in der EU

Innerhalb der EU gibt es unterschiedliche Vorstellungen darüber, wie „offensiv" das neue Instrument der Cybersanktionen angewendet werden soll. Während Italien eher skeptisch ist und Finnland, Belgien sowie Schweden einen graduellen Ansatz, also eine schrittweise Verschärfung der Maßnahmen befürworten, ist Frankreich ein großer Befürworter eines schnellen und umfassenden Einsatzes von Cybersanktionen. Die Bundesregierung macht sich vor allem im Zusammenhang mit dem Cyberangriff auf den Bundestag ebenfalls für eine Nutzung des Instruments stark. Auch die technische Expertise und Kapazitäten bei der Identifizierung und Abwehr von Cyberangriffen divergiert zwischen den EU-Mitgliedsstaaten, was ein einheitliches Vorgehen zusätzlich erschwert.

### Alignment

Genau wie bei anderen EU-Sanktionen können (potenzielle) Beitrittsländer, Länder des europäischen Wirtschaftsraumes sowie Länder der „Östlichen Partnerschaft" die Sanktionen durch eine formale Erklärung, ein sogenanntes „Alignment", mittragen. Dies ist bei EU-Sanktionen gängige Praxis. Im Fall der ersten EU-Cybersanktionen verzichteten die Republik Moldau, Aserbaidschan und die Türkei, die zu den traditionellen Alignment-Ländern gehören (Hellquist 2016), auf diesen Schritt. Dies zeigt, dass bestimmte Länder dem neuen Instrument skeptisch gegenüberstehen und so ein einheitliches Vorgehen über die Grenzen der EU hinaus erschweren. Demgegenüber schlossen sich die Republik Nordmazedonien, Montenegro, Albanien, Bosnien und Herzegowina, Island, Norwegen, die Ukraine und Georgien den EU-Cybersanktionen an.

## Schritte zu wirksamen Cybersanktionen

Cyberangriffe bedrohen den demokratischen Prozess, die Sicherheit und die wirtschaftliche Entwicklung in den betroffenen Staaten. Das relativ neue Instrument der Cybersanktionen ist für mehr Sicherheit im digitalen Raum deshalb wichtiger denn je – es zielt auf die Verantwortlichen und kann potenzielle Täterinnen und Täter abschrecken. Exemplarisch stehen Cybersanktionen damit für die

Weiterentwicklung internationaler Sanktionen: Die Sanktionspraxis reagiert auf – aus der Perspektive traditioneller Außenpolitik – neue Sicherheitsbedrohungen.

Gleichzeitig haben Cybersanktionen in ihrer aktuellen Form verschiedene Schwächen. Der UN-Sicherheitsrat wird absehbar höchstens in jenen Fällen intervenieren, die die gesamte Staatengemeinschaft (oder zumindest die Interessen der fünf ständigen Sicherheitsratsmitglieder) bedrohen. Ein abgestimmtes Handeln der EU mit den USA und anderen *like-minded*-Staaten und -Organisationen ist daher von entscheidender Bedeutung, um das Instrument der Cybersanktionen wirksam einzusetzen.

Selbst innerhalb der EU ist dies bislang jedoch selten der Fall. Unter den EU-Mitgliedsstaaten bestehen unterschiedliche Ansichten, wie umfassend Cybersanktionen verhängt werden sollen. Umstritten ist vor allem die Frage, wann ein gemeinsames Handeln der EU erforderlich ist. Sanktionen sollen bei Angriffen mit „erheblicher Wirkung" ausgesprochen werden. Diese ist aber nicht definiert und muss im Einzelfall festgestellt werden. Zu den Aufgaben gehört auch, die technischen Kapazitäten für die Attribution von Cyberattacken in den Mitgliedsstaaten auszubauen. Zunehmend sollte die EU-Außenpolitik und Entwicklungspolitik auch die Stärkung der technischen Kapazitäten zur Abwehr von Cyberangriffen in Drittstaaten, zum Beispiel in Ländern des globalen Südens, in den Blick nehmen. Eine Cyber-Entwicklungszusammenarbeit könnte helfen, gemeinsam gegen schädliche Attacken im digitalen Raum vorzugehen. Dies ist umso wichtiger, da Cyberangriffe auf Parlamente, Behörden und private Firmen in Zukunft eine noch größere Bedrohung darstellen werden.

## Literatur


Egloff, Florian J. (2020), Public Attribution of Cyber Intrusions, in: *Journal of Cybersecurity*, 6, 1, tyaa012.

EU Kommission (2017), *Empfehlung (EU) 2017/1584 der Kommission - vom 13. September 2017 - für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen*, Brüssel: Europäische Kommission, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017H1584&from=CS (12. April 2021).

Europäischer Rat (2020a), *Beschluss (GASP) 2020/1127 des Rates vom 30. Juli 2020 zur Änderung des Beschlusses (GASP) 2019/797 über Restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen*, Brüssel: Europäischer Rat, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32020D1127&from=EN (12. April 2021).

Europäischer Rat (2020b), *Durchführungsverordnung (EU) 2020/1536 des Rates vom 22. Oktober 2020 zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen*, Brüssel: Europäischer Rat, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32020R1536&from=EN (12. April 2021).

Europäischer Rat (2019), *Beschluss (GASP) 2019/797 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen*, Brüssel: Europäischer Rat, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019D0797&rid=11 (12. April 2021).

European Council (2019), *Council Decision Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States*, Brussels: Council of the European Union, https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf (1. April 2021).

Giumelli, Francesco (2011), *Coercing, Constraining and Signalling: Explaining and Understanding International Sanctions After the End of the Cold War*, Colchester: European Consortium for Political Research (ECPR).

Grauvogel, Julia, und Christian von Soest (2014), Claims to Legitimacy Count: Why Sanctions Fail to Instigate Democratisation in Authoritarian Regimes, in: *European Journal of Political Research*, 53, 4, 635-653.

Hellquist, Elin (2016), Either with Us or against Us? Third-Country Alignment with EU Sanctions against Russia/Ukraine, in: *Cambridge Review of International Affairs*, 29, 3, 997-1021.

Herpig, Sven (2021), *Die Beantwortung von Staatlich-Verantworteten Cyberoperationen* [Arbeitstitel], Studie, Berlin: Stiftung Neue Verantwortung.

Pawlak, Patryk, und Thomas Biersteker (2019), *Guardian of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace*, Paris: European Union Institute for Security Studies (EUISS), www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf (24. Februar 2021).

Portela, Clara (2019), *The Spread of Horizontal Sanctions*, Centre for European Policy Studies, www.ceps.eu/publications/spread-horizontal-sanctions (9. März 2019).

*Spiegel* (2021), Offenbar russischer Hack: Erneute Attacke auf Bundestagspolitiker – sieben Abgeordnete betroffen, www.spiegel.de/politik/deutschland/russischer-hack-erneute-attacke-hack-auf-bundestag-sieben-abgeordnete-betroffen-a-75e1adbe-4462-4e30-bd94-96796aed6b8a (26. März 2021).

von Soest, Christian (2019), Individual Sanctions: Toward a New Research Agenda, in: *CESifo Forum*, 20, 4, 28-31.

## Die Autorin und der Autor

Dr. Julia Grauvogel ist Senior Research Fellow am GIGA Institut für Afrika-Studien, Sprecherin des Forschungsteams „Interventionen und Sicherheit“ sowie Herausgeberin der Fachzeitschrift *Africa Spectrum*. Zu ihren Forschungsschwerpunkten gehören internationale Sanktionen und autoritäre Regime. Im Projekt „Beendigung internationaler Sanktionen: Ursachen, Prozesse und innerstaatliche Folgen“ (www.giga-hamburg.de/de/project/the-termination-of-international-sanctions-causes-processes-and-domestic-consequences), gefördert von der DFG, analysieren GIGA-Forscherinnen und -Forscher, wie und warum Sanktionen aufgehoben werden und welche Nachwirkungen die Beendigung von Sanktionen hat.
Julia.Grauvogel@giga-hamburg.de, www.giga-hamburg.de/de/team/11565528-grauvogel-julia/

Dr. Christian von Soest ist Lead Research Fellow am GIGA Institut für Afrika-Studien und Leiter des GIGA-Forschungsschwerpunkts 2 „Frieden und Sicherheit“. Seine Arbeitsschwerpunkte sind Sanktionen und internationale Interventionen, gewaltsame Konflikte sowie die Innen- und Außenpolitik autoritärer Regime. Ge-

meinsam mit Prof. Dr. Amrita Narlikar und Prof. Dr. Jann Lay leitet er das neue, vom Auswärtigen Amt geförderte Digital Transformation Lab (DigiTraL) des GIGA. Christian.vonSoest@giga-hamburg.de, www.giga-hamburg.de/de/team/11564977-von-soest-christian/

Die Autorin und der Autor danken Emilian Berutti für seine wertvolle Recherche.

## GIGA-Forschung zum Thema

Das vom Auswärtigen Amt geförderte Digital Transformation Lab (DigiTraL) des GIGA analysiert die politischen Treiber und Konsequenzen der globalen digitalen Transformation mit einem Fokus auf Diplomatie und internationale Politik (www.giga-hamburg.de/en/projects/digital-diplomacy-statecraft-digitral-diplo-i-giga-digital-transformation-digitral-a-global-approach/). Die Forschung wird die damit verbundenen globalen Entwicklungen und die Perspektiven aus Asien, Afrika, Lateinamerika und dem Nahen Osten untersuchen.

Das Forschungsteam 3 „Interventionen und Sicherheit“ das GIGA-Forschungsschwerpunkts 2 „Frieden und Sicherheit“ untersucht, wie externe Akteure sowie internationale und regionale Vereinbarungen Friedens- und Konfliktdynamiken beeinflussen und welche sicherheitspolitischen Auswirkungen ihre Interventionen auf lokaler, nationaler, regionaler und internationaler Ebene haben. Ein Hauptaugenmerk liegt dabei auf der Analyse internationaler Sanktionen.

## GIGA-Publikationen zum Thema

Attia, Hana und Julia Grauvogel (2019), *Easier In Than Out: The Protracted Process of Ending Sanctions*, GIGA Focus Global, 5, Oktober, www.giga-hamburg.de/de/publikationen/11854089-easier-in-than-out-protracted-process-ending-sanctions/.

Attia, Hana, Julia Grauvogel, und Christian von Soest (2020), The Termination of International Sanctions: Explaining Target Compliance and Sender Capitulation, in: *European Economic Review*, 129, 103565, https://doi.org/10.1016/j.euroecorev.2020.103565.

Basedau, Matthias und Jann Lay (2021), *Ten Things to Watch in Africa in 2021*, GIGA Focus Afrika, 1, Januar, www.giga-hamburg.de/en/publications/23327611-things-watch-africa-2021/.

Grauvogel, Julia, und Hana Attia (2019), Wie enden internationale Sanktionen? Zur Bedeutung von Prozessen, Beziehungen und Signalen, in: *Zeitschrift für Internationale Beziehungen*, 26, 2, 5-33.

Grauvogel, Julia, und Christian von Soest (2015), *Die verfehlte Sanktionspolitik des Westens gegen Simbabwe*, GIGA Focus Afrika, 2, März, www.giga-hamburg.de/de/publikationen/11569821-verfehlte-sanktionspolitik-westens-gegen-simbabwe/.

Grauvogel, Julia, Amanda A. Licht, und Christian von Soest (2017), Sanctions and Signals: How International Sanction Threats Trigger Domestic Protest in Targeted Regimes, in: *International Studies Quarterly*, 61, 1, 86-97, https://doi.

org/10.1093/isq/sqw044.
Köllner, Patrick (2019), *Die Denuklearisierung Nordkoreas: Von Maximalforderungen zu Rüstungskontrolle*, GIGA Focus Asien, 2, Februar, www.giga-hamburg.de/de/publikationen/11569475-denuclearisation-north-korea-from-maximum-demands-arms-control/.
Narlikar, Amrita (2020), *Deutschland im Sicherheitsrat der Vereinten Nationen: Multilateralismus reformieren*, GIGA Focus Global, 2, März, www.giga-hamburg.de/de/publikationen/17780803-germany-united-nations-security-council-reforming-multilateralism/.
Wirth, Christian, und Valentin Schatz (2020), *„Lawfare" im Südchinesischen Meer: Der Kampf um die Freiheit der Schifffahrt*, GIGA Focus Asien, 5, August, www.giga-hamburg.de/de/publikationen/20691035-south-china-lawfare-fighting-over-freedom-navigation/.

## Impressum



Das German Institute for Global and Area Studies (GIGA) gibt Focus-Reihen zu Afrika, Asien, Lateinamerika, Nahost und zu globalen Fragen heraus. Der GIGA Focus wird vom GIGA redaktionell gestaltet. Die vertretenen Auffassungen stellen die der Autorinnen und Autoren und nicht unbedingt die des Instituts dar. Die Verfassenden sind für den Inhalt ihrer Beiträge verantwortlich. Irrtümer und Auslassungen bleiben vorbehalten. Das GIGA und die Autorinnen und Autoren haften nicht für Richtigkeit und Vollständigkeit oder für Konsequenzen, die sich aus der Nutzung der bereitgestellten Informationen ergeben.

Das GIGA dankt dem Auswärtigen Amt und der Freien und Hansestadt Hamburg (Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke) für die institutionelle Förderung.

Gesamtredaktion GIGA Focus: Prof. Dr. Sabine Kurtenbach
Redaktion GIGA Focus Global: Prof. Dr. Sabine Kurtenbach
Lektorat: Christine Berg, Dr. James Powell

GIGA | Neuer Jungfernstieg 21
20354 Hamburg
www.giga-hamburg.de/de/publikationen/giga-focus/
giga-focus@giga-hamburg.de

GIGA
German Institute for Global and Area Studies
Leibniz-Institut für Globale und Regionale Studien