3

2020 / Zwischen Cyberfrieden und Cyberkrieg / RÜSTUNGSDYNAMIKEN

↓ EMPFEHLUNGEN

1 **Russische Bereitschaft für sicherheitspolitische Kooperation testen** Die Bundesregierung sollte eruieren, ob Russland aufgrund des Rückgangs seiner Militärausgaben bereit ist, über die Eingrenzung konventioneller militärischer Fähigkeiten zu verhandeln.

2 **G20 als Adressat für Rüstungskontrolle** Die G20 sind für 82 % der weltweiten Militärausgaben verantwortlich. Die Bundesregierung sollte eine Begrenzung dieser Ausgaben als rüstungskontrollpolitische Maßnahme auf die Tagesordnung der G20 setzen.

3 **Stärkung der Kontrollen in der EU** Bevor die EU ihre Ausgaben für militärische Forschung und Entwicklung massiv ausweitet, sollten Instrumente der Kontrolle durch das EU-Parlament und den europäischen Rechnungshof gestärkt werden.

4 **Entscheidung über Tornado-Nachfolgesystem aussetzen** Die politischen, finanziellen und technischen Auswirkungen der Beschaffung eines nuklearfähigen amerikanischen bzw. europäischen Trägersystems sind in einem transparenten Prozess zu klären.

5 **Rüstungskooperation und Exportkontrolle zusammen denken** Die EU-Staaten sollten sich bei gemeinsamen Rüstungsprojekten vorab auf mögliche Empfängerländer einigen. Diese müssen, entsprechend den Kriterien des Gemeinsamen Standpunkts der EU zu Rüstungsexporten, unbedenklich sein.

6 **Keine Rüstungsexporte an Ägypten und die Vereinigten Arabischen Emirate** Angesichts der Menschenrechtslage in Ägypten und der Beteiligung beider Staaten in regionalen Gewaltkonflikten soll die Bundesregierung keine weiteren Rüstungsexporte an diese beiden Staaten genehmigen.

7 **Digitale Gegenangriffe auf begründete Ausnahmefälle beschränken** „Hackbacks" müssen auf die Abwehr gravierender und akuter Gefahren – gerade für die Zivilbevölkerung – beschränkt und an die Zustimmung des Bundestags gebunden sein.

8 **Investitionen in Resilienz statt in Offensive** Geplante Investitionen in die Entwicklung offensiver Kapazitäten im Cyber-Bereich sollten umgewidmet und für die Stärkung der Resilienz staatlicher Strukturen genutzt werden.

9 **Angriffe auf kritische Infrastruktur ächten** Die Bundesregierung sollte sich in den VN für die Tabuisierung von Angriffen auf den „Public Core" des Internets und für eine Norm des Verzichts auf Cyberattacken gegen kritische zivile Infrastrukturen einsetzen.

10 **Schaffung unparteiischer Analyseinstanzen und Austauschforen** Die Bundesregierung sollte für die Einrichtung eines transnationalen Attributionskomitees in den VN werben und informelle Austauschforen über Cyberrisiken stärken.

RÜSTUNGSDYNAMIKEN / Zwischen Cyberfrieden und Cyberkrieg /

Global ist eine kontinuierliche Steigerung der Militärausgaben zu konstatieren, während Rüstungskontrollmechanismen zunehmend wegbrechen. Zudem löst sich sukzessive die zivil-militärische Abgrenzung auf. Das beste Beispiel hierfür ist der Cyberraum, der gegenwärtig eine rasante Militarisierung erlebt und in diesem Jahr im Fokus des Kapitels steht. Die Bundesregierung bewegt sich bei den meisten Rüstungsdynamiken im Mainstream und vermag nur punktuell friedenspolitische Akzente zu setzen.

3.1 ↙ Rüstungsdynamiken

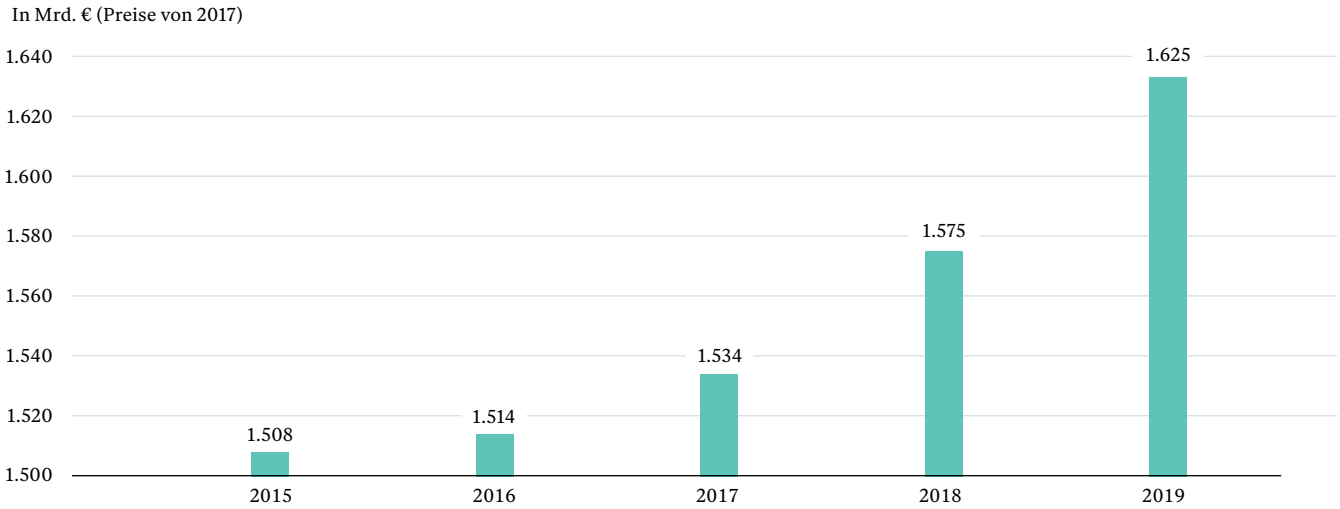
MILITÄRAUSGABEN

Die weltweiten Ausgaben für Militär und Rüstung erreichten 2019 einen Rekordstand und lagen bei über 1.600 Mrd. € → **27** /96; real fast 20 % über dem höchsten Niveau zu Zeiten des Kalten Krieges. Während Steigerungsraten nach der Finanzkrise von 2008 niedrig waren, nahmen sie seit 2015 vor allem aufgrund deutlich gestiegener Ausgaben der USA und Chinas zu. Die G20 hatten 2019 einen Anteil von mehr als 82 % an den globalen Militärausgaben. Die russischen Militärausgaben hingegen sanken im gleichen Zeitraum deutlich; sie lagen 2019 um mehr als 20 % unter denen von 2016. Die Militärausgaben der NATO-Mitgliedsstaaten übersteigen die Russlands um fast das 16-fache → **28** /96. Der Anteil der Militärausgaben am globalen Einkommen lag 2019 bei ca. 2,2 %. Regional sind die Belastungen mit ca. 4,5 % des Einkommens im Mittleren Osten besonders hoch und in Lateinamerika mit 1,4 % vergleichsweise niedrig (→ SIPRI 2020).

Die Militärausgaben Deutschlands nach NATO-Kriterien stiegen 2019 um 12 % auf 47,9 Mrd. €. Der Anteil am Bruttoinlandsprodukt (BIP) stieg auf 1,38 %. Im Globalen Militarisierungsindex (GMI) liegt Deutschland 2019 mit Rang 97 von 154 Staaten unverändert im Mittelfeld (→ Mutschler/Bales 2020);[1] → **29** /97. Das Bundeshaushaltsgesetz

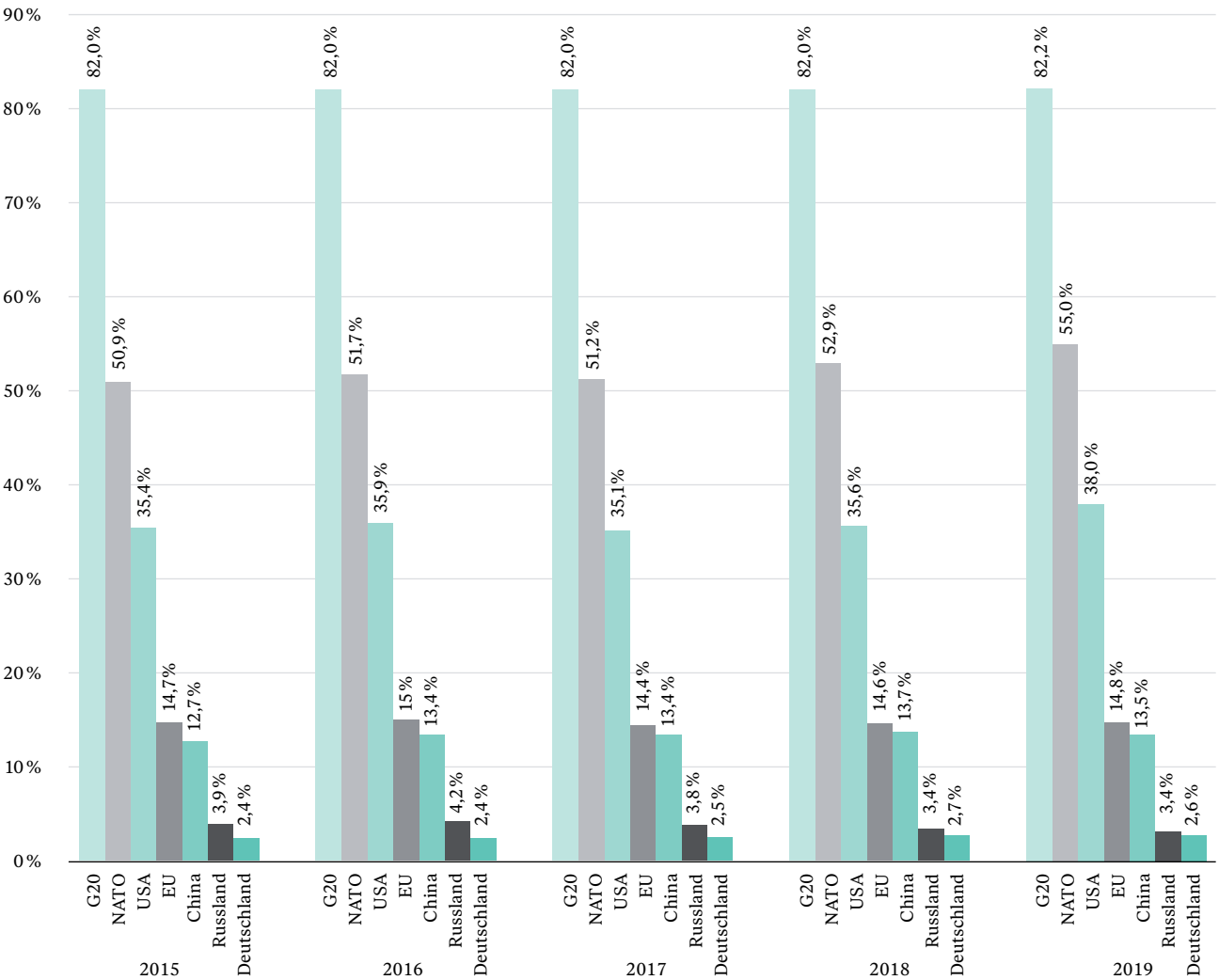
27 Globale Militärausgaben

Quelle → **3** /115



28 Globale Militärausgaben: ausgewählte Anteile

Quelle → **3** /115



29 Rang Deutschlands für verschiedene Indikatoren von Militarisierung und Friedlichkeit 2019

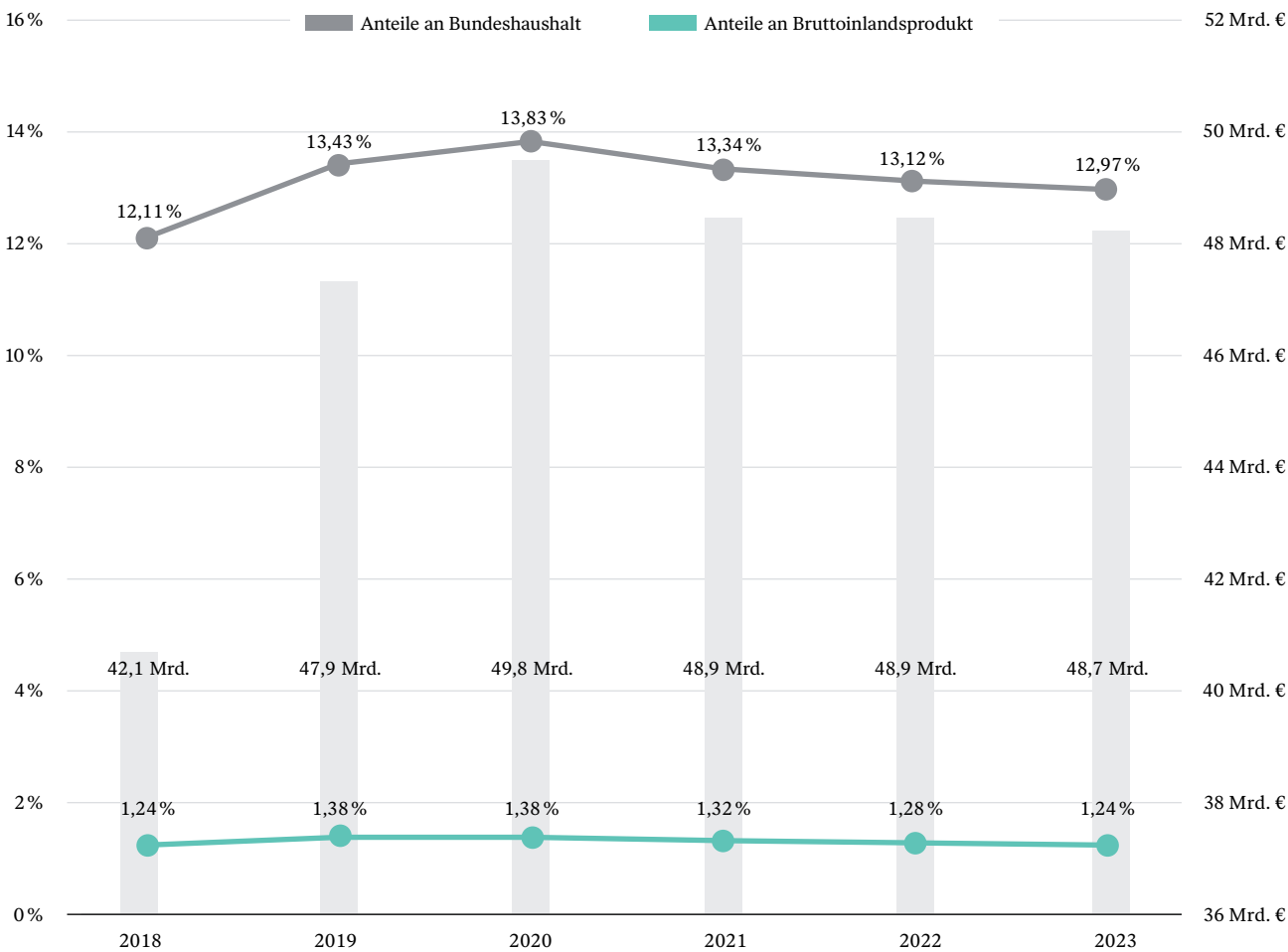
Quelle → 3 /115

Indikator	Rang Deutschlands unter erfassten Ländern
Militärausgaben	7 von 155 Staaten
Exporte von Großwaffen	5 von 189 Staaten
Militärausgaben als Anteil am Bruttoinlandsprodukt	88 von 149 Staaten
Militärausgaben als Anteil an Staatsausgaben	117 von 150 Staaten
Global Militarisation Index (GMI)	97 von 154 Staaten
Global Peace Index (GPI), invertiert	142 von 163 Staaten

Rang unter allen in den jeweiligen Quellen erfassten Staaten.

30 Tatsächliche (2019) und gemäß Bundeshaushaltsplan ermittelte deutsche Militärausgaben nach NATO-Kriterien

Quelle → 3 /115



Anmerkung: Angaben für 2019 vorläufig; für 2020ff.: Fortschreibung der NATO-Angabe für 2019 mit Zuwachsraten für Verteidigungsausgaben, Bundeshaushalt und Bruttoinlandsprodukt aus Finanzplan des Bundes 2019–2023.

für 2020 sieht einen Anstieg der Ausgaben des Bundesverteidigungsministeriums, die den Löwenanteil der deutschen Militärausgaben ausmachen, um weitere 4 % vor. Die Bundesregierung signalisierte 2019 der NATO, 2024 einen Anteil der Militärausgaben am BIP von 1,5 % erreichen zu wollen (→ Bundesregierung 2018). Das entspräche Militärausgaben von ca. 61 Mrd. € im Jahr 2024. Allerdings sollen laut der vor der Corona-Krise erstellten Finanzplanung des Bundes die Verteidigungsausgaben zwischen 2020 und 2023 nicht weiter steigen und der Anteil am Bruttoinlandsprodukt damit leicht sinken → **30** /97. Durch Beschlüsse für neue ambitionierte Rüstungsprojekte wie das gemeinsam mit Frankreich geplante Luftkampfsystem (Future Combat Air Systems, FCAS) oder einen neuen Kampfpanzer werden aber laufend Finanzbedarfe fällig, die nur mit deutlich steigenden Ausgaben finanzierbar sein werden. Dies gilt auch für die Beschaffung von US-amerikanischen, mit Nuklearwaffen bestückbaren Kampfflugzeugen. Hier besteht die Gefahr, dass die Bundesregierung voreilig die „nukleare Teilhabe" aufrechterhält, ohne dass die langfristigen politischen, finanziellen und technische Auswirkungen in einem transparenten Prozess geklärt werden und damit der Bundestag über eine belastbare Entscheidungsgrundlage verfügt.

Ambitionierte Rüstungsprojekte werden teuer

Ein Teil der Mittel für gemeinsame europäische Rüstungsprojekte soll in Zukunft aus dem Haushalt der EU kommen. Der aktuelle Haushaltsentwurf der EU für 2021–2027 sieht Mittel für gemeinsame Rüstungsforschung und -entwicklung von Mitgliedsstaaten in Höhe von 13 Mrd. € vor,[2] eine Steigerung um das 22-fache gegenüber dem vorigen Haushalt für die Jahre 2014–2020, der erstmals Mittel der EU für Rüstungszwecke budgetierte (→ European Court of Auditors 2019). Insbesondere stehen der Rüstungsforschung erhebliche, neue Finanzmittel in Höhe von 4,1 Mrd. € für einen Siebenjahreszeitraum zur Verfügung. Alle Mitgliedsstaaten (ohne Großbritannien) gaben 2018 zusammen etwa 1,6 Mrd. € für diesen Zweck aus.[3] Sollten diese Pläne trotz der Corona-Krise Bestand haben, würde die EU damit zu einem finanziell relevanten Faktor der Aufrüstung in Europa werden. Rüstungsproduktion und -beschaffung würden komplexer, was nach Ansicht des europäischen Rechnungshofs zu Defiziten in der Kontrolle führen könnte (→ European Court of Auditors 2019: 61).

Massive Erhöhung der EU-Mittel für Rüstungsforschung – bessere Kontrolle nötig

RÜSTUNGSHANDEL

Der internationale Handel mit Großwaffen stieg 2015–2019 im Vergleich zum Zeitraum 2010–2014 um 5,5 % an. Die deutschen Waffenexporte stiegen zwischen diesen beiden Vergleichszeiträumen sogar um 17 % (→ Wezeman et al. 2019). Die fünf größten Exporteure sind die USA (36 %), Russland (21 %), Frankreich (7,9 %), Deutschland (5,8 %) und China (5,5 %) → **31** /99.

Die Bundesregierung genehmigte 2019 Rüstungsexporte im Wert von mehr als 8 Mrd. € (→ BMWi 2020). Dies ist ein neuer Rekordwert. 2018 hatte die Bundesregierung Rüstungsexporte im Wert von 4,8 Mrd. € (Einzelausfuhrgenehmigungen) an 129 Staaten bewilligt, mehr als die Hälfte (52,9 %) davon an Drittstaaten (außerhalb der EU, der

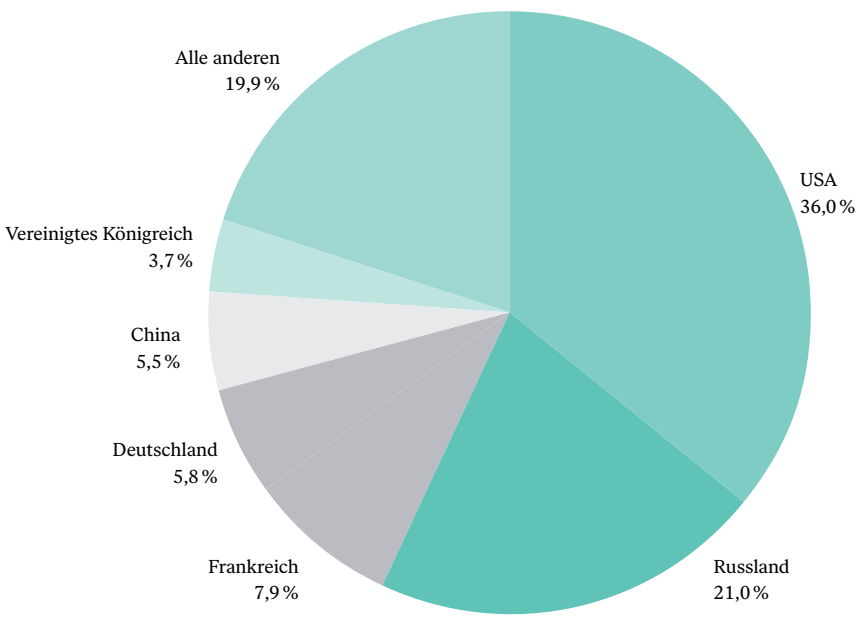
NATO und gleichgestellter Länder) (→ BMWi 2019a). Zwar wurden 2019 nur 44,1 % der Genehmigungen für Rüstungsexporte an Drittstaaten erteilt, jedoch liegt dieser Rückgang vor allem an den hohen Genehmigungswerten für EU- und NATO-Staaten → **32** /100. Spitzenreiter unter den Empfängerstaaten war Ungarn, das unter der rechtsnationalen Regierung Victor Orbans stark aufrüstet. Unter den Hauptempfängern der Drittstaaten für 2019 befinden sich unter anderem Ägypten, für das allein im ersten Halbjahr 2019 Rüstungsexporte im Wert von über 800 Mio. € genehmigt wurden, sowie die Vereinigten Arabischen Emirate (VAE) (267 Mio. €), Algerien (170 Mio. €) und Katar (165 Mio. €) (→ BMWi 2019b). Bei den Ausfuhren von Kriegswaffen 2019 für insgesamt 1,1 Mrd. € zählt die Türkei zu den Hauptempfängern. Die genaue Höhe des Lieferwerts für die Türkei erklärte die Bundesregierung zur Verschlusssache (→ BMWi 2020b).

Rüstungsexporte an Ägypten und die Vereinigten Arabischen Emirate sind hoch problematisch

Rüstungsexporte an ein Militärregime wie in Ägypten, das für die Folter und das Verschwindenlassen von Oppositionellen verantwortlich ist, sind nicht vereinbar mit der Erklärung der Bundesregierung, Menschenrechte seien Fundament deutscher Außenpolitik und dienten deutschen Interessen. Ägypten und die VAE gehören zur Jemen-Kriegskoalition, der nach wie vor massive Verstöße gegen das humanitäre Völkerrecht vorgeworfen werden. Beide Länder unterstützen auch General Haftar im libyschen Bürgerkrieg gegen die rechtmäßig anerkannte Regierung. Es gibt Hinweise, dass die VAE Haftar Luftabwehrsysteme zur Verfügung gestellt haben, die auf Militärtrucks der deutschen Marke MAN montiert sind (→ Tillack 2019).

31 Anteile an globalen Exporten von Großwaffen 2015–2019

Quelle → **3** /115



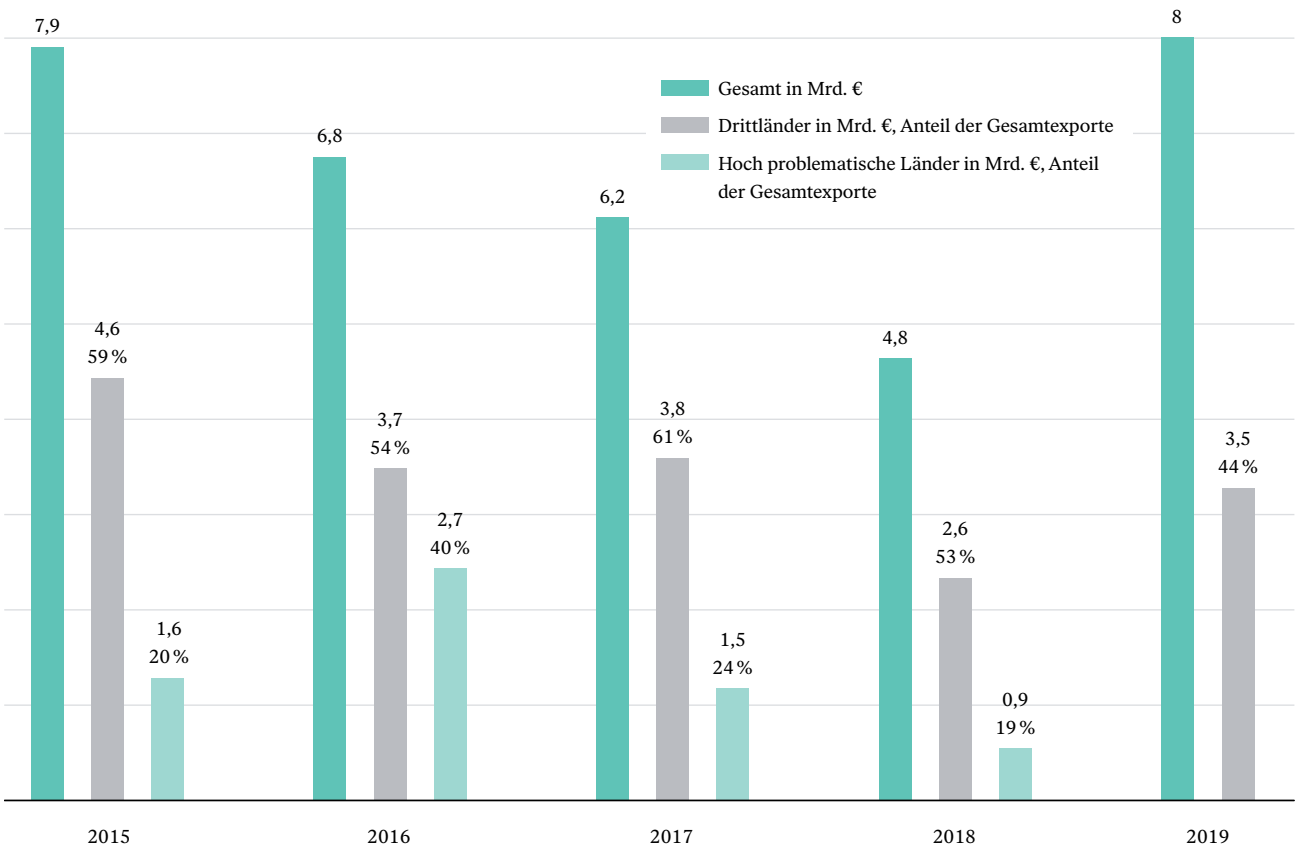
Das sind keine Ausnahmefälle. Die Bundesregierung genehmigt immer wieder Rüstungsexporte an autoritäre Regime und in Konfliktregionen. Nach Berechnungen des BICC genehmigte sie 2018 Rüstungsexporte an 52 Staaten, deren Menschenrechtssituation als sehr schlecht eingestuft wird. In 24 Empfängerländern gab es interne Gewaltkonflikte und bei 16 Empfängerländern sind Frieden und Sicherheit in der jeweiligen Region gefährdet (→ BICC 2019). 2018 genehmigte die Bundesregierung Rüstungsexporte im Gesamtwert von 941,8 Mio. € an 18 Länder, die mindestens hinsichtlich vier der acht Kriterien des Gemeinsamen Standpunktes der EU zu Rüstungsexporten problematisch sind → **32** /100.

Positiv zu vermerken ist der deutliche Rückgang der Exportgenehmigungen für Kleinwaffen an Drittstaaten. Ihr Wert belief sich 2017 auf 15 Mio. €; 2018 waren es 0,4 Mio. €, im ersten Halbjahr 2019 0,3 Mio. € (→ BMWi 2019a/b).

Dass die Rüstungskooperation innerhalb der EU an Fahrt aufnimmt, begründen die Befürworter wie etwa die Bundesregierung mit der effizienteren Nutzung vorhandener Ressourcen. Gleichzeitig bleibt die EU-Rüstungsexportkontrolle schwach. So brachte

32 Deutsche Rüstungsexporte

Quelle → **3** /115



Noch keine Berechnung für hochproblematische Länder im Jahr 2019 möglich

die jüngste Überarbeitung des Gemeinsamen Standpunkts der EU zu Rüstungsexporten 2019 kaum nennenswerte Verbesserungen. Daher besteht bei der Europäisierung von Rüstungsvorhaben die Gefahr, dass deutsche Exportregelungen umgangen werden, indem Deutschland Rüstungskomponenten liefert, die fertigen Waffensysteme aber andere Staaten exportieren. Bislang behielt sich die Bundesregierung vor, Einwände gegen bestimmte Exporte zu erheben. In ihren überarbeiteten Politischen Grundsätzen zum Rüstungsexport vom Juni 2019 deutet sie jedoch an, solche Einwände nur noch geltend zu machen, wenn der deutsche Anteil einen bestimmten Prozentsatz überschreitet. Mit Frankreich wurden Sätze von 20 % vereinbart (→ GKKE 2020). Die Aushebelung der deutschen Rüstungsexportkontrolle ist zu befürchten. Um Rüstungsexporten nicht Tür und Tor zu öffnen, sollten sich die EU-Staaten bei gemeinsamen Rüstungsprojekten vorab auf eine Liste möglicher Empfängerländer einigen, die entsprechend den Kriterien des Gemeinsamen Standpunkts der EU unbedenklich sind. Bei relevanten Veränderungen in einem der Länder muss die Liste angepasst werden.

RÜSTUNGSKONTROLLREGIME

Abhängig von Waffenart und -system sind der Stand, die Ausrichtung sowie die Ausdifferenziertheit der Kontrollregime recht unterschiedlich. An dieser Stelle gibt das FGA einen Überblick über die jüngsten Entwicklungen.

Nuklearwaffen: Russland und die USA setzen die nukleare Rüstungskontrolle erheblich unter Druck. Der INF-Vertrag über die Abrüstung landgestützter Mittelstreckenwaffen lief am 2. August 2019 aus, nachdem Washington sechs Monate zuvor den Austritt erklärt hatte. Vorwürfe der NATO, dass Russland neue nuklearfähige Marschflugkörper stationiert, sind ungeklärt. Russland und die USA entwickeln neuartige Nuklearwaffen. Alle neun Atomwaffenbesitzer modernisieren ihre Nuklearsenale. Der New START-Vertrag über die Begrenzung strategischer Waffen ist der letzte verbliebene nukleare Rüstungskontrollvertrag. Er läuft am 5. Februar 2021 aus, sofern Russland und die USA nicht die im Abkommen vorgesehene Option einer Verlängerung der Vertragsdauer von bis zu fünf Jahren nutzen. Russland ist zu einem solchen Schritt bereit, die USA zögern.

Nukleare Rüstungskontrolle unter Druck

Am 7. Februar erneuerte der französische Präsident Emmanuel Macron in einer Grundsatzrede zur Nuklearpolitik das Angebot, die französische force de frappe in den Dienst Europas zu stellen. Er lud die europäischen Partner zu einem strategischen Dialog über die Rolle der französischen Atomwaffen in der europäischen Sicherheit und zur Teilnahme an Atomübungen ein. Allerdings lehnte er jede Form der europäischen Mitsprache an der französischen Nuklearwaffenpolitik ab. Deutsche Entscheidungsträger wollen die Einladung zu einem strategischen Dialog annehmen.

Nachdem die USA sich seit Mai 2018 nicht mehr an den Gemeinsamen Umfassenden Aktionsplan mit Iran halten, verletzt auch Teheran seit Mai 2019 das Atomabkommen. Bisherige Bemühungen der Europäer, den Handel mit Iran trotz des umfänglichen US-Sanktionsregimes aufrechtzuerhalten, sind über symbolische Transaktionen etwa unter dem neuen Instrument INSTEX (Instrument in Support of Trade Exchanges) nicht hinausgekommen. Effektive Instrumente, die die wirtschaftliche Autonomie Europas auch gegen die ökonomischen Druckmittel Washingtons gewährleisten könnten, sind nicht vorhanden.

Biowaffen: Im Rahmen der Biowaffenkonvention (BWÜ) stieß Deutschland 2019 gemeinsam mit Schweden und den Niederlanden die Einrichtung eines wissenschaftlichen Beratungsgremiums (Scientific and Technological Experts Advisory Forum, STEAF) an. Wohl auch angesichts der schnellen Entwicklung auf den Gebieten der Genomeditierung und der umweltverändernden Biotechnologien gibt es hierfür derzeit ein stärkeres Momentum als in früheren Jahren. Ein Beschluss müsste auf der Überprüfungskonferenz 2021 aber konsensual gefasst werden. Immerhin verstärkten viele Staaten ihre Anstrengungen, den Generalsekretärsmechanismus[4] zu implementieren, etwa durch Übungen und den Aufbau eines Netzwerks von Referenzlaboren. Damit steht dem VN-Generalsekretär ein unabhängiges Instrument für die Untersuchung möglicher Einsätze biologischer und chemischer Waffen zur Verfügung, das er bereits 2013 nutzte, um zu untersuchen, ob das syrische Ghouta mit C-Waffen angegriffen wurde.

Chemiewaffen: In der Chemiewaffenkonvention (CWÜ) beschloss die 21. Vertragsstaatenkonferenz überraschend einhellig die Aufnahme der 2018 in Salisbury verwendeten „Novichok"-Substanzen in die Liste 1 der Stoffliste des CWÜ, was zum Stichtag 7. Juni 2020 mit Verpflichtungen zur Deklaration von Produktion und Produktionsanlagen verbunden ist. 2019 nahm zudem das Investigation and Identification Team (IIT) seine Arbeit auf; ein erster substanzieller Bericht ist am 8. April 2020 erschienen; drei Luftangriffe mit chemischen Waffen wurden darin klar der syrischen Armee zugeordnet. Nachdem das IIT in einer Mehrheitsentscheidung der CWÜ-Mitglieder, aber gegen die Stimme Russlands, eingesetzt wurde, bleibt abzuwarten, welche politischen Folgen der Bericht haben wird. Deutschland hatte 2019 eine Mio. € in den OPCW (Organisation für das Verbot chemischer Waffen) Trust Fund für Missionen in Syrien eingezahlt, die auch der Arbeit des IIT zugute kommen.

Konventionelle Munition: 2020 befasste sich eine internationale Gruppe von Regierungsexperten (GGE) mit der Verbesserung der Kontrolle überschüssiger konventioneller Munitionsbestände. Schon 2008 hatte sich eine GGE zusammengefunden, um Standards für den Umgang mit konventioneller Munition auf den Weg zu bringen. Die

VN-Abrüstungsabteilung entwickelte daraus die technischen Richtlinien für sachgemäßen Umgang mit Munition (IATG). Auf die Kontrolle von Munition konnten sich die Staaten innerhalb des Kleinwaffenaktionsprogramms von 2001 bislang nicht einigen.

Unbemannte Waffensysteme: Der Trend zur Beschaffung und Automatisierung unbemannter Waffensysteme hält an. Deutschland entschloss sich 2018 zum Leasing bewaffnungsfähiger Heron-TP-Drohnen und beteiligt sich auch an der Entwicklung einer europäischen Kampfdrohne. Über die Bewaffnung dieser Drohnen findet in Deutschland weder eine breite Diskussion statt, noch wurde eine politische Grundsatzentscheidung getroffen. In der Frage, ob autonome Waffensysteme die Prinzipien des Völkerrechts verletzen und daher reguliert werden müssen, konnte das internationale VN-Expertentreffen 2019 in Genf erneut keinen Durchbruch erzielen. Die Diskussion ist festgefahren. Man einigte sich auf die Fortsetzung der Gespräche 2020 und 2021 und auf die Erarbeitung eines gemeinsamen, normativen und operationellen Rahmens als Grundlage weiterer Verhandlungen.

Weltraum: Die Militarisierung des Weltraums schreitet voran, und seine Bewaffnung ist zu befürchten. Russland, China und die USA schufen sogenannte Weltraumstreitkräfte, und einige Staaten, zu denen neben den drei genannten auch Indien zählt, verfügen über Raketen- bzw. Raketenabwehrsysteme, mit denen potenziell Satelliten zerstört werden können. Weltraumschrott, der insbesondere durch die Trümmer zerstörter oder kollidierter Weltraumobjekte entsteht, stellt eine enorme Gefahr für die Raumfahrt dar. Verlässlich lassen sich Unfälle und Angriffe im Weltraum nur schwer voneinander unterscheiden, was die Gefahr von Missverständnissen in Krisensituationen und einer ungewollten militärischen Eskalation birgt. Expertengruppen, u.a. im Rahmen der VN, konnten bislang keine substanziellen Fortschritte in Hinblick auf Rüstungskontrolle und die Verhinderung bewaffneter Angriffe im Weltraum erzielen. Deutschland sprach sich richtigerweise 2019 im VN-Weltraumausschuss für ein Verbot der absichtlichen Zerstörung von Weltraumobjekten aus.

3.2 ↙ Aufrüstung und Rüstungskontrolloptionen im Cyberraum

Der Begriff Cyberkrieg wurde vor fast 30 Jahren geprägt. Bisher herrscht keine Einigkeit darüber, was dieser Begriff umfasst. Ob der Begriff des Krieges sich auf den Cyberraum übertragen lässt, ist umstritten. Wenngleich die Häufigkeit und Intensität von Cyberangriffen zunimmt, so ist doch deren Mehrzahl krimineller Natur oder kann als Subversion und Sabotage eingestuft werden – nicht jedoch als Krieg. Im Friedensgutachten ziehen wir daher Begriffe wie Cyberangriffe oder Cyberattacken vor, um Kriegsanalogien zu vermeiden. Mit Blick auf Frieden und Sicherheit ist

Cyberraum als Ort neuer Rüstungsdynamiken

jedoch relevant, inwiefern der Cyberraum zum Ort neuer Rüstungsdynamiken avanciert und wie diese eingehegt werden können. Rüstung im Cyberraum richtet sich auf den Schutz sowie die Manipulation oder Zerstörung digitaler Systeme – mit zum Teil erheblichen Risiken für den zivilen Datenverkehr.[5]

FACETTEN DER CYBER-BEDROHUNGEN

Obwohl die meisten Cyberangriffe in erster Linie störend und nicht zerstörerisch sind, stellen sie eine Bedrohung für Gesellschaften dar, die stark von modernen Technologien abhängig sind. Cyberangriffe können dazu dienen, Daten auszuspionieren oder zu manipulieren, Informationen zu stehlen oder Infrastruktur zu zerstören. Das Spektrum der Angriffe ist breit gefächert und reicht von kriminellen Machenschaften, Desinformationskampagnen und Datenlecks bis hin zu zerstörerischen Angriffen auf kritische Infrastrukturen, Regierungseinrichtungen oder militärische Systeme. Während früher Einzelpersonen das Hauptziel waren, sind in jüngster Zeit vermehrt Industrie- und Regierungssysteme Ziel von Cyberattacken. Beispielsweise unterbrachen 2015 Cyberattacken gegen mehrere Energieversorger die Stromversorgung in der Westukraine.

33 Akteure im Cyberraum

Staaten können nicht nur Forschung und Entwicklung betreiben oder fördern, sondern agieren häufig auch intransparent. Den Vulnerabilities Equities Process (VEP) wenden etwa die USA an, wenn sie eine Computersicherheitslücke identifiziert haben. In diesem Verfahren behalten sie sich vor zu entscheiden, ob betroffene Unternehmen und die Öffentlichkeit über Computersicherheitslücken informiert werden oder diese bewusst geheim gehalten werden, um sie offensiv zu nutzen. Weitere Staaten mit VEPs sind Australien, China, Kanada und Großbritannien.

Wirtschaftsunternehmen fungieren als Zulieferer für staatliche Programme oder agieren in Bereichen, die außerhalb staatlicher Zuständigkeit liegen. Hinzu kommen Unternehmen, die defensive Maßnahmen für den Cyberraum entwickeln.

Advanced Persistent Threat (APT)-Gruppen sind oft mit staatlichen Akteuren verbunden oder werden als deren Stellvertreter angesehen. APT-Gruppen werden häufig von einem staatlichen Akteur geleitet und unterstützt. Die bei Angriffen verwendeten Instrumente können verschiedene Operationen oder sogar Gruppen gemeinsam nutzen, was die Zuordnung zusätzlich erschwert.

Cyber-Söldner werden oft als staatliche Stellvertreter betrachtet. Sie untergraben Verschlüsselungen, spionieren oder überwachen. Cyber-Söldner tragen erheblich dazu bei, die Unterscheidung zwischen privater und staatlicher Sphäre zu verwischen.

Kriminelle nutzen vor allem bereits verfügbare Schadsoftware. Im militärischen Cyberraum spielen sie eine untergeordnete Rolle.

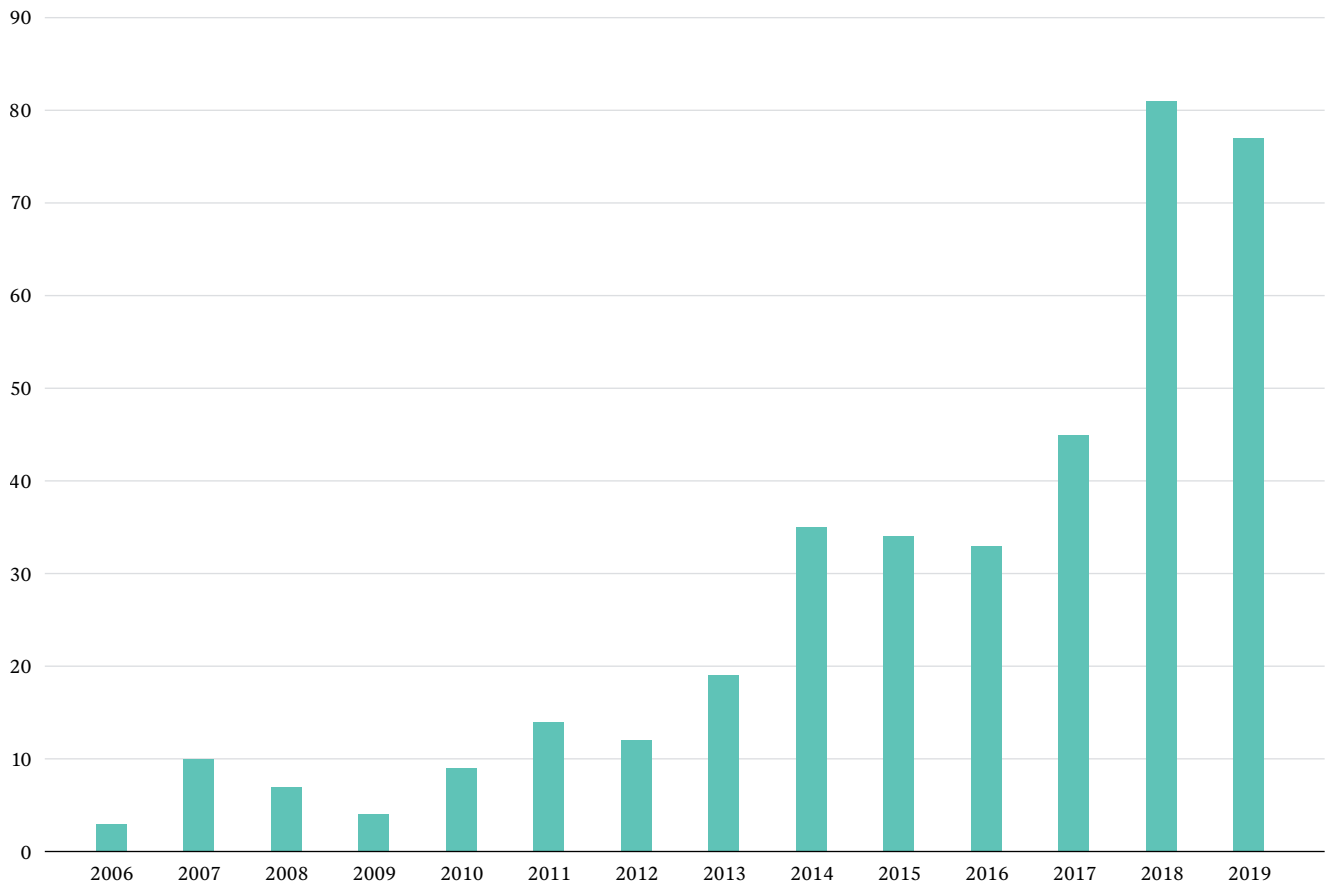
Hacktivisten beteiligen sich aus weltanschaulichen oder politischen Gründen an Cyber-Angriffen, oft mit einer sehr großen Bandbreite an Aktivitäten und Zwecken. Patriotische Hacker sind Hacktivisten, die Angriffe auf vermeintliche Feinde eines Staates verüben oder Angriffe von ihnen blockieren, weshalb sie auch in militärisch sensiblen Feldern auftreten.

Cyberoperationen entwickeln sich zudem zu einem integralen Bestandteil der Kriegsführung. Bereits 2007 soll die israelische Armee Cyberangriffe gegen die syrische Luftverteidigung durchgeführt haben, um einen Forschungsreaktor bombardieren zu können (→ Busch 2020: 5). Gegnerische Informations- und Kommandostrukturen sollten lahmgelegt werden. Cyberattacken können jedoch auch selbstständig physische Zerstörung herbeiführen. Bekanntestes Beispiel ist die Sabotage der iranischen Nuklearanreicherung durch den Computerwurm Stuxnet im Jahr 2010, für die mutmaßlich die USA und Israel verantwortlich zeichneten. Staaten sind im militärischen Cyberraum die dominanten Akteure, da sie über die Ressourcen und Kapazitäten verfügen, um etwa Folgen von Cyberangriffen zu simulieren. Dennoch sind die Akteure vielfältig und die Übergänge fließend → **33** /104.

Es ist methodisch äußerst schwierig, verlässliche Daten zu Cyberattacken zu erheben. Viele Cyberattacken werden nicht entdeckt oder die angegriffenen Akteure veröffentlichen sie nicht. Wirtschaftsunternehmen fürchten Reputationsschäden, während Staaten abwägen müssen, welche Attacken öffentlich gemacht und welche Akteure beschuldigt werden. Darum können allenfalls grobe Trends identifiziert werden.

34 Anzahl staatlich lancierter Cyberattacken

Quelle → **3** /115



Ein besonderes Problem – technisch wie politisch – ist die Attribution von Cyberangriffen, also ihre Zuordnung zum Verursacher. Oft besteht Unsicherheit darüber, ob die Täter für sich selbst oder als Agenten anderer handeln. Dass sich der Ausgangsort in einem bestimmten Land befindet, bedeutet nicht, dass die dortige Regierung den Auftrag gegeben hat. Selbst wenn sich der Angriff auf eine staatliche Einrichtung zurückverfolgen lässt, könnte es sich immer noch um eine unautorisierte Operation oder Manipulation handeln. Hinzu kommt die Problematik der öffentlichen Beweisführung. Wenn die Methoden der Attribution als geheim klassifiziert oder urheberrechtlich geschützt sind, bleibt die Zuordnung anfechtbar. Dies war etwa der Fall beim Angriff auf Sony im Jahr 2014, für den die USA Nordkorea verantwortlich machten, aber ihre Beweisführung zunächst nicht offenlegten. Erschwerend kommt hinzu, dass viele der Zuweisungsmethoden für Cyberangriffe technisch manipuliert werden können: Digitale Aufzeichnungen können kopiert, verändert, erstellt oder gelöscht werden, Identitäten können gefälscht und Angriffe als Unfälle oder Inkompetenz getarnt werden. Obwohl es selten möglich ist, einen Angriff vollständig zu tarnen, ist es ebenso schwierig, die für die Attribution notwendigen digitalen Informationen zeitnah und zuverlässig zu erhalten.

Zuordnung von Cyberangriffen zum Verursacher ist oft schwierig

Auch die Intention von Cyberangriffen ist nicht immer eindeutig: Dieselbe Verwundbarkeit, Software (oder Malware) und dieselben Vorgehensweisen lassen sich für ganz unterschiedliche Arten von Angriffen nutzen. Zum Beispiel kann ein Angriff, der nach Spionage aussieht, die erste Stufe eines zukünftigen Datenlecks oder Sabotageaktes sein. Desgleichen können Computersysteme Verwundbarkeiten vortäuschen, z.B. in der Form von sogenannten Scheinzielen („honey pots“), um vom eigentlichen Ziel abzulenken und den Angreifer in eine Falle zu locken. Die Grenzen zwischen Abwehr und Angriff im Cyberraum sind fließend.

Es gibt unterschiedliche Möglichkeiten, auf Cyberangriffe zu reagieren. Die Optionen reichen vom passiven Erdulden über Verteidigungsmaßnahmen bis zu Vergeltungsangriffen innerhalb oder außerhalb des Cyberraums.

AUFRÜSTUNG IM CYBER-BEREICH

In jüngster Zeit entschließen sich Staaten vermehrt zu Strategien der Abschreckung und Vorwärtsverteidigung im Cyberraum. Auch Privatunternehmen reagieren zunehmend mit Hackbacks auf Cyberattacken (→ Faesen et al. 2019b). Hackbacks bezeichnen Aktionen, die ein Angegriffener über seine eigenen Netzwerke hinaus unternimmt, um den Angriff zu stoppen und die Angreifer zu identifizieren, oder sogar, um gestohlene Daten zu zerstören. Sie bergen das Risiko falscher Zuschreibungen, unbeabsichtigter Kollateralschäden und der Eskalation. Zugleich geben Militärs vermehrt

offensive Absichten zu erkennen. Nationale Sicherheitsstrategien identifizieren staatlich gelenkte Cyberattacken als ernstzunehmende Bedrohung. Die Militarisierung des Cyberraums ist an verschiedenen Indikatoren ablesbar: dem Ausbau militärischer Strukturen, der Entwicklung von Doktrinen und Budgets sowie der Einbettung von Cyberattacken in laufende militärische Operationen.

Nahezu alle Groß- und Regionalmächte haben die traditionellen militärischen Operationsbereiche – See, Luft, Land und Weltraum – um den Cyberraum als fünfte Dimension erweitert sowie zivile und militärische Cyberbehörden mit sowohl defensiver als auch offensiver Ausrichtung geschaffen. Einige Staaten sehen deren Hauptaufgabe im Schutz der digitalen Infrastruktur, während andere dies als den Beginn einer neuen Ära des Wettrüstens bezeichnen. So deklarierten bereits 21 Staaten offensive militärische Ziele im Cyberraum (→ Faesen et al. 2019a). Mindestens 31 Staaten verfügen nachweisbar über eine dezidiert militärische Cyberstrategie (→ Center for Strategic & International Studies o.J.). Die tatsächliche Zahl dürfte deutlich darüber liegen, da Cyberstrategien und -doktrinen in vielen Ländern unter Geheimhaltung fallen. Derselbe Vorbehalt betrifft militärische Cyberausgaben, die in der Regel klassifiziert oder aufgrund überlappender Zuständigkeiten nicht vergleichbar erfasst werden können. Marktanalysen erwarten allerdings eine Steigerung der weltweiten militärischen Cyberbudgets von derzeit 13,8 Mrd. US-$ 2019 auf 16 Mrd. US-$ im Jahr 2023 (→ Orr 2019). Weltweit führend sind die USA, die 2019 8,5 Mrd. US-$ für militärische Cyberkapazitäten ausgaben; das sind 4 % mehr als im Vorjahr (→ Morgan 2019). Verlässliche Zahlen für das chinesische oder russische Budget liegen nicht vor.

Staaten verfügen zunehmend über militärische Cyberstrategien

Prinzipiell können militärische Cyberausgaben sowohl in defensive als auch in offensive Kapazitäten fließen. Aus friedenspolitischer Sicht ist beunruhigend, dass offensive Cyberoperationen nicht mehr „nur“ in die Planung militärischer Einsätze integriert werden. Vielmehr werden sie zu tragenden Säulen der Cyberabwehr und -abschreckung in Friedenszeiten. Das hat Folgen für Bereiche wie die Integrität demokratischer Wahlen, die traditionell nicht durch das Militär geschützt werden. Das Vision Statement des US-Cyberkommandos sowie die 2018 revidierte militärische Cyberdoktrin der USA sind tonangebend. Sie lassen die eher reaktive Doktrin der Obama-Ära hinter sich, nennen China und Russland explizit als Bedrohung und orientieren sich an den Leitprinzipien persistenter Aktionen und der Vorwärtsverteidigung. Demnach sollen potenzielle Attacken bereits an ihrem Ursprung unterbunden werden. Das setzt den kontinuierlichen Zugriff auf Netzwerke potenzieller Gegner und eventuell auch Präemptivschläge voraus. Die Entwicklung zukünftiger Angriffsoptionen, etwa durch Platzierung „logischer Bomben“, wird als Mittel der Abschreckung gerechtfertigt. Was das in der Praxis bedeutet, verdeutlichte die US-amerikanische Reaktion auf die russische Desinformation während der US-Kongresswahlen 2018. Nicht nur störte

US-amerikanische Cyberstrategie ist offensiv ausgerichtet

das US-Cyberkommando die Internetverbindung einer russischen Trollfabrik. Es schleuste als Vergeltungsmaßnahme auch Schadprogramme in russische Energieversorgungsnetze ein (→ Sanger/Perlroth 2019). Solche Aktionen sind im Kontext der organisatorischen Aufwertung des Cyberkommandos zu betrachten, das seit Mai 2018 als eigenständiges Unified Combatant Command fungiert. Ebenfalls seit 2018 ist das US-Militär nicht mehr gezwungen, offensive Cyberoperationen vom Weißen Haus autorisieren zu lassen und mit anderen Ressorts, etwa dem State Department, abzustimmen.

Kritiker bemängeln, dass das Konzept der Abschreckung im Cyberraum untauglich und riskant ist. Der Glaube an die Überlegenheit der Offensive, die dem Präemptivgedanken zugrunde liegt, ist nicht durch empirische Fakten belegt (→ Valeriano/Jensen 2019). Dessen ungeachtet zeichnet sich ab, dass einige Cybermächte und Bündnisse dem Beispiel der USA folgen und zunehmend offensive Gegenmaßnahmen androhen: So sprach der britische Außenminister im März 2019 über diverse Vergeltungsmaßnahmen für Cyberattacken, wozu auch Cybergegenschläge gehören könnten. Bereits 2014 kamen die NATO-Mitglieder überein, dass schwerwiegende Cyberattacken prinzipiell den Bündnisfall auslösen können. Ende 2017 traf die NATO eine Grundsatzentscheidung, die die Androhung offensiver Cybergegenschläge als Teil ihrer Abschreckungsstrategie beinhaltet. Allerdings hat das 2018 gegründete NATO Cyber Operations Center nur koordinierende Funktion. Die Entwicklung und der Einsatz offensiver Kapazitäten verbleiben unter der Kontrolle der Mitgliedsstaaten.

Während russische Militärs und Sicherheitsexperten dem Konzept der Abschreckung im Cyberspace skeptisch gegenüberstehen, wandelt sich die politische Praxis: Russische Vertreter drohen zunehmend explizit mit Vergeltungsmaßnahmen für Cyberattacken (→ Meakins 2018). Auch in China kündigt sich ein Kurswechsel an. Es gewinnen jene Stimmen an Einfluss, die sich für eine chinesische Cyberabschreckung stark machen, um auf die doktrinäre Verschärfung in den USA zu reagieren (→ Jiang 2019: 13-15). Gerade die Entwicklung in China und Russland deutet darauf hin, dass die Logik des Sicherheitsdilemmas immer stärker die Politik bestimmt. Die Folge ist ein absehbarer Rüstungswettlauf im Cyberraum. Noch fataler: Es ist davon auszugehen, dass Aktionen der Vorwärtsverteidigung im Krisenfall als Angriffsvorbereitungen fehlgedeutet und mit präemptiven Attacken beantwortet werden. Das Resultat könnte sein, dass Konfliktparteien die Kontrolle über die Eskalation verlieren.

Gefahr eines Rüstungswettlaufs im Cyberraum

Deutschland war bislang keine treibende Kraft dieser Entwicklung. Seit der schweren Cyberattacke auf den Bundestag 2015 zeichnet sich jedoch ein Richtungswechsel hin zu einer aktiven Verteidigung ab, und es wird über staatliche Hackback-Operationen diskutiert. Diese könnte das im April 2017 eingesetzte Bundeswehrkommando Cyber- und Informationsraum (KdoCIR) ausführen. Der gesamte Organisationsraum, dem

das KdoCIR zugeordnet ist, soll bis 2021 etwa 14.500 Dienstposten umfassen. Das seit 2018 bestehende Zentrum Cyberoperationen (ZCO) könnte schon bald über die technischen Voraussetzungen für eine „aktive Verteidigung“ verfügen. Rechtlich umstritten ist, auf welcher Grundlage die Bundeswehr im Rahmen der Gefahrenabwehr gegen ausländische Computersysteme vorgehen darf (→ Busch 2020: 3-4). Kritiker werfen zudem ein, dass darunter die Glaubwürdigkeit deutscher Cyberaußenpolitik leiden könnte, die sich auf internationaler Ebene für eine Beschränkung militärischer Handlungen im Cyberraum einsetze.

RÜSTUNGSKONTROLLE IM CYBER-BEREICH

Noch kann präventive Rüstungskontrolle eine ungebremste militärische Konfrontation im Cyberraum verhindern, auch weil die tatsächlich möglichen Effekte von Cyberattacken noch gar nicht klar sind. Klassischerweise zielt präventive Rüstungskontrolle auf das gänzliche Verbot oder die Einschränkung der Fähigkeiten bestimmter Waffentypen. Im Cyberraum ist ein solches Vorgehen zum Scheitern verurteilt. Denn Cyberattacken beruhen nicht auf kinetischer Energie, sondern sie nutzen technische und organisatorische Schwachstellen des Zielobjekts aus.

Dieses Wissen ist hochgradig volatil, und die globale Detektion und Kontrolle von Schadsoftware, die auf diesem Wissen beruht, würde jedes Rüstungskontrollregime überfordern. Das Wassenaar-Abkommen sowie die EU schränken den grenzüberschreitenden Verkauf von Software ein, die das Ausspähen oder die Manipulation fremder IT-Systeme ermöglicht. Den lukrativen Schwarz- und grauen Markt für solche Produkte, auf dem Cyberkriminelle, private Hacker aber auch Staaten aktiv sind, kann die multilaterale Exportkontrolle kaum eindämmen.

In einem breiteren Verständnis kann präventive Rüstungskontrolle aber auch als Beschränkung im Umgang mit den entsprechenden Waffen verstanden werden. Diverse Initiativen wollen den militärischen Wettbewerb im Cyberraum einschränken. Sie richten sich auf die Regulierung von Verhalten, nicht auf ein Verbot von „Cyberwaffen“. Das geschieht auf drei Feldern: (1) der Konkretisierung internationaler Verpflichtungen, die sich aus bestehenden völkerrechtlichen Verträgen ergeben, (2) der Vereinbarung rechtlich unverbindlicher, aber politisch wirksamer Verhaltensnormen und (3) der Entwicklung vertrauensbildender Maßnahmen vor allem auf bilateraler und regionaler Ebene.

Präventive Rüstungskontrolle im Cyberraum

Konkretisierung internationaler Verpflichtungen: Das für Abrüstungsfragen zuständige Erste Komitee der VN-Generalversammlung beauftragt seit 2004 mehrfach GGE, gemeinsame Prinzipien und Regeln im Cyberraum zu entwickeln. Ein Meilenstein dieser Verhandlungen war das Bekenntnis zur prinzipiellen Gültigkeit und

Anwendbarkeit der VN-Charta und bestehender völkerrechtlicher Verpflichtungen im Cyberraum. Über die konkrete Anwendung dieser Bestimmungen konnte indes keine Einigung erzielt werden. Kontrovers wurde das Recht auf Selbstverteidigung debattiert sowie die Frage, was unter einem „bewaffneten Angriff" zu verstehen sei. Auch die Anwendbarkeit des humanitären Völkerrechts, beispielsweise des Prinzips der Verhältnismäßigkeit militärischer Handlungen, war umstritten. Zwar ist im NATO-Kontext mit den Tallinn Manuals 1 und 2 inzwischen eine fundierte juristische Handreichung zu diesen Fragen entstanden; nicht-westliche Staaten äußern aber den Vorwurf, dass dies auf die Legitimierung militärischer Operationen im Cyberraum hinauslaufe.

Aufgrund dieser Konfliktlinien ging die fünfte GGE 2017 ohne einen Konsensbericht auseinander. Daraufhin initiierten Russland, China und weitere Staaten einen alternativen Verhandlungsprozess, der 2019 in der Einsetzung der Open Ended Working Group (OEWG) mündete, die sich parallel zur sechsten GGE konstituierte. Derzeit sind die Folgen dieser Fragmentierung nicht absehbar. Es wird darauf ankommen, dass die teilnehmenden Staaten auf dem erreichten Verhandlungsstand auf- und diesen ausbauen. Dies schließt einen ganzen Katalog politischer Normen ein, der, ausgehend vom Prinzip der Staatenverantwortung, im Kontext der GGE erarbeitet wurde: Staaten dürfen demnach keine Cyberangriffe dulden, die von ihrem Territorium ausgehen. Sie dürfen nichtstaatliche Akteure nicht als Proxies zur Verschleierung eigener Absichten nutzen. Sie sind angehalten, sich am zwischenstaatlichen Informationsaustausch über Cybervorfälle zu beteiligen sowie angegriffenen Staaten zu helfen. Außerdem dürfen sie die Arbeit von Computer Emergency Response Teams (CERT) weder behindern noch missbrauchen. Solche Spielregeln können als weiches Recht Bindewirkung entfalten und zum Ausgangpunkt für ein späteres Gewohnheits- oder Vertragsrecht werden.

Entwicklung von Normen zur Einhegung von Cyberangriffen

Vereinbarung rechtlich unverbindlicher Normen: Nichtstaatliche Akteure (v.a. Unternehmen) treiben rechtlich unverbindliche Normbildungsprozesse voran. Beispielsweise schlossen sich multinationale Konzerne (u.a. Siemens) 2018 in der Charter of Trust zusammen. Sie betonen die Notwendigkeit erhöhter Sicherheitsstandards für Lieferketten und Produkte. Zugleich richten sie Forderungen an die Staatenwelt, etwa Cybersicherheit zum Kriterium für Freihandelsabkommen zu machen. Ein anderes Beispiel für privatwirtschaftliche Unternehmen, die sich engagieren, ist Microsoft mit seinem Konzept einer „digitalen Genfer Konvention". Der Kerngedanke ist der Schutz von Individuen und zivilgesellschaftlichen Institutionen in der digitalen Welt. Attacken gegen Krankenhäuser, Stromnetze oder den internationalen Zahlungsverkehr seien zu ächten. Offensive Cyberkapazitäten sollten in ihrer Wirkung präzise, begrenzt und gegen eine unautorisierte Weitergabe gesichert sein.

Weitere Initiativen beruhen auf heterogenen Zusammenschlüssen staatlicher und zivilgesellschaftlicher Akteure. Darunter fällt die 2017 von der niederländischen Regierung, dem Hague Center for Strategic Studies und dem East-West Institute eingerichtete Global Commission for the Stability of Cyberspace (GCSC). Unter deren zentralen Normen findet sich die Verpflichtung, keine Angriffe gegen die Kerninfrastruktur des Internets (Public Core) durchzuführen. Ebenso seien demokratische Prozesse (Wahlen, Referenden) Tabu. Nichtstaatliche offensive Operationen seien grundsätzlich illegitim. Damit geht die GCSC einen Schritt weiter als der Paris Call for Trust and Security in Cyberspace, den der französische Präsident Emmanuel Macron im November 2018 initiierte. Im Call heißt es nur, dass Maßnahmen getroffen werden müssten, um Hackbacks privater Akteure zu vermeiden. Besonders herausgestellt wird der Schutz demokratischer Wahlen und des Public Core des Internets, etwa des Domainnamensystems. Ebenso seien Staaten und Unternehmen verpflichtet, die Proliferation von Schadsoftware einzudämmen. Auf ihrer Website spricht sich die Initiative dafür aus, die Zusammenarbeit mit ethischen Hackern durch geeignete Belohnungs- und Berichtssysteme zu stärken.

Vertrauensbildende Maßnahmen: Auf bilateraler Ebene gehört zur Entwicklung vertrauensbildender Maßnahmen die Verstärkung direkter Kommunikationskanäle zwischen nationalen Cyber-Behörden, wie sie die US-Regierung unter Barack Obama mit China und Russland vereinbarte („heißer Draht“). Auch das bilaterale amerikanisch-chinesische Abkommen zur Einschränkung von Cyberspionage 2015 stellte eine erste vertrauensbildende Maßnahme dar. Seit dem Amtsantritt Donald Trumps stehen die Zeichen jedoch auf Konfrontation. Größere Fortschritte werden vor allem im regionalen Kontext erzielt. So erarbeitete die OSZE einen breiten Katalog vertrauensbildender Maßnahmen. Diese beinhalten die Benennung von Point of Contacts zur Krisenkommunikation, gegenseitige Informationspflichten bei Cyberangriffen, die Offenlegung staatlicher Doktrinen sowie die Erarbeitung einer gemeinsamen Terminologie. Vergleichbare Bemühungen existieren im Rahmen von ASEAN und der Organisation Amerikanischer Staaten (OAS).

Transnationales Attributionskomitee zur Aufklärung von Cybervorfällen einsetzen

Mittelfristig könnten gemeinsame Standards für die Attribution von Cybervorfällen ein wirksames Instrument sein, um die Stabilität im Cyberraum zu erhöhen. Denn dadurch könnte zwischen international legitimen und illegitimen Beschuldigungen und Sanktionierungen unterschieden werden. Noch einen Schritt weiter gehen Vorschläge zur Einrichtung eines transnationalen Attributionskomitees, in dem sich unabhängige Experten um die Aufklärung brisanter Cybervorfälle bemühen. Eine solche Institution könnte die Voraussetzung für ein international akzeptiertes Anprangern von Angriffen schaffen, wodurch Verstöße gegen Verhaltensnormen kostspieliger und seltener würden.

SCHLUSSFOLGERUNGEN

Dem Trend zunehmend offensiver Cyberdoktrinen sollte Deutschland auf mehreren Ebenen entgegenwirken. Die Bundesregierung sollte die Option militärischer Hackbacks auf begründete Ausnahmefälle beschränken, also auf die Abwehr gravierender und akuter Gefahren, die mit diplomatischen oder polizeilichen Maßnahmen nicht bewältigt werden können. Analog zu konventionellen Auslandseinsätzen der Bundeswehr muss die Zustimmung des Bundestags verpflichtend sein. Um angemessen schnelle Reaktionen zu ermöglichen, könnte die Autorisierung zunächst durch einen ständig erreichbaren Unterausschuss erfolgen. Der gesamte Bundestag müsste aber umgehend in Kenntnis gesetzt werden. Er könnte dann beispielsweise den Abbruch fortdauernd eskalierender Einsätze verlangen. Die Entwicklung offensiver Kapazitäten sollte auf wenige Einsatzszenarien begrenzt werden. Stattdessen sollten Ressourcen in die Stärkung der Resilienz kritischer Infrastrukturen fließen. Sicherheitsanforderungen für Hard- und Softwareanbieter sollten erhöht und der Informationsaustausch über Cyberattacken und Verwundbarkeiten verbessert werden.

Bewegung gibt es in globalen Normbildungsinitiativen. Um dem beobachtbaren „Wettrüsten“ im Cyberraum entgegenzuwirken, sollte die Bundesregierung darauf hinwirken, dass die Arbeit von GGE und OEWG im VN-Kontext mittelfristig wieder zusammengeführt wird und kurzfristig eine enge Koordination der Agenden erfolgt. Inhaltlich sollte sich Deutschland für eine möglichst universelle Bekräftigung grundlegender Normen einsetzen. Dazu gehören die Tabuisierung von Angriffen auf den Public Core des Internets sowie der Verzicht auf Cyberattacken (no first-use) gegen kritische zivile Infrastruktur. Ebenso wichtig ist es, positive Anreize für Verhaltensänderungen nichtstaatlicher Akteure zu schaffen. So ließe sich der bisherige GGE-Normenkatalog durch die Verpflichtung ergänzen, eine Kultur der Offenlegung von Sicherheitslücken durch eine stärkere Zusammenarbeit mit „ethischen Hackern“ zu fördern.

Um die Logik von Nullsummenspielen und Präventivschlägen zu durchbrechen, sollte Deutschland stärker als Sponsor divers zusammengesetzter Austauschforen wie der GCSC agieren, die Eskalationsrisiken, den Einfluss von Fehlwahrnehmungen auf das Krisenmanagement sowie Proliferationsgefahren thematisiert sollten. Um das Risiko ungewollter Eskalationen zu verringern, bedarf es schließlich dringend einer internationalen Verständigung über Standards für die Attribution von Cyberattacken sowie unparteiischer Analyseinstanzen. Die Bundesregierung sollte für die Einrichtung eines transnationalen Attributionskomitees werben und einen Vorschlag für dessen Organisation und Finanzierung machen. Um dessen Unabhängigkeit und Integrität zu garantieren, sollten international anerkannte Forschungsinstitutionen auf dem Gebiet der Computerforensik dieses Gremium besetzen und nicht die Staaten selbst. Eine hinreichend unabhängige und international legitimierte Institution könnte das Reputationsrisiko für die Verletzung internationaler Normen steigern und zugleich die Gefahr militärischer Überreaktionen auf Cybervorfälle senken.

1 Der GMI des BICC bildet das relative Gewicht und die Bedeutung des Militärapparats eines Staates im Verhältnis zur Gesellschaft als Ganzes ab. Hierzu setzt er die Militärausgaben in Relation zum Bruttoinlandsprodukt (BIP) eines Staates und zu den staatlichen Gesundheitsausgaben und berücksichtigt weitere Indikatoren wie die Relation der Soldaten zur Gesamtbevölkerung.

2 European Commission o.J: European Defence Fund, in: https://ec.europa.eu/growth/sectors/defence/european-defence-fund_en; 19.03.2020. Ansätze 2014–2020: 590 Mio. €. Endgültige Beschlussfassung steht noch aus. Zahlen könnten sich noch ändern.

3 Geschätzt auf der Grundlage der Angaben in European Defence Agency 2020: Defence Data 2016-17, in: https://eda.europa.eu/info-hub/defence-data-portal; 29.04.2020.

4 Der Generalsekretärsmechanismus der VN dient der Untersuchung eines vermuteten Einsatzes chemischer, biologischer und toxikologischer Waffen. Er bietet den Rahmen für objektive Untersuchungen angeblicher Verstöße gegen internationale Vereinbarungen.

5 Auf künstliche Intelligenz und Robotik geht dieses Kapitel nicht ein, da diese nicht zu einer direkten Gefährdung der digitalen Infrastrukturen (v.a. Internet) beitragen. Fake News und Deep Fakes behandelte das Friedensgutachten 2019 ausführlich (→ Friedensgutachten 2019, Kap. 5).

Autorinnen und Autoren

Dr. Christian Alwardt
IFSH – Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Prof. Dr. Michael Brzoska
IFSH – Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Dr. Mischa Hansel
BICC – Bonn International Center for Conversion / SEF – Stiftung Entwicklung und Frieden

Dr. Gunnar Jeremias
Carl Friedrich von Weizsäcker-Zentrum für Naturwissenschaft und Friedensforschung, Universität Hamburg

Dr. Margret Johannsen
IFSH – Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Dr. Oliver Meier
IFSH – Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Dr. Max Mutschler
BICC – Bonn International Center for Conversion

Prof. Dr. Conrad Schetter (Koordination)
BICC – Bonn International Center for Conversion

Jantje Silomon, PhD
IFSH – Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Dr. Simone Wisotzki
HSFK – Leibniz-Institut Hessische Stiftung Friedens- und Konfliktforschung

Prof. Dr. Herbert Wulf
BICC – Bonn International Center for Conversion

Quellenverzeichnis

Bonn International Center for Conversion (BICC) 2019: Datenbank zu Rüstungsexporten, in: http://ruestungsexport.info; 29.01.2020.

Bundesministerium für Wirtschaft und Energie (BMWi) 2019a: Bericht der Bundesregierung über ihre Exportpolitik für konventionelle Rüstungsgüter im Jahr 2018, in: https://www.bmwi.de/Redaktion/DE/Publikationen/Aussenwirtschaft/ruestungsexportbericht-2018.pdf?__blob=publicationFile&v=2; 12.03.2020.

Bundesministerium für Wirtschaft und Energie (BMWi) 2019b: Bericht der Bundesregierung über ihre Exportpolitik für konventionelle Rüstungsgüter im ersten Halbjahr 2019, in: https://www.bmwi.de/Redaktion/DE/Publikationen/Aussenwirtschaft/ruestungsexport-zwischenbericht-2019.pdf?__blob=publicationFile&v=10; 12.03.2020.

Bundesministerium für Wirtschaft und Energie (BMWi) 2020a: Antwort von Staatssekretär Dr. Ulrich Nußbaum an Katja Keul (MdB) vom 06.01.2020 (Schriftliche Frage an die Bundesregierung im Monat Dezember 2019, Frage Nr. 478); in: https://www.bmwi.de/Redaktion/DE/Parlamentarische-Anfragen/2019/12-478.pdf?__blob=publicationFile&v=2; 12.03.2020.

Bundesministerium für Wirtschaft und Energie (BMWi) 2020b: Antwort von Staatssekretär Dr. Ulrich Nußbaum an Sevim Dagdelen (MdB) vom 23.04.2020 (Schriftliche Frage an die Bundesregierung im Monat April 2020, Frage Nr. 242); in: https://www.linksfraktion.de/fileadmin/user_upload/PDF_Dokumente/2020/Antwort_-_Schriftliche_Frage_4-242_-_Waffenexporte.pdf; 05.05.2020

Bundesregierung 2018: Pressekonferenz von Bundeskanzlerin Merkel und dem NATO-Generalsekretär Stoltenberg, 15. Juni 2018, Berlin, in: https://www.bundesregierung.de/breg-de/aktuelles/pressekonferenzen/pressekonferenz-von-bundeskanzlerin-merkel-und-dem-nato-generalsekretaer-stoltenberg-1142060; 11.03.2020.

Busch, Carolin 2020: Von Firewall bis Hackback: Das Spektrum militärischer Cyberoperationen, Arbeitspapier 1/20, Bundesakademie für Sicherheitspolitik, in: https://www.baks.bund.de/sites/baks010/files/arbeitspapier_sicherheitspolitik_2020_1.pdf; 11.03.2020.

Center for Strategic & International Studies o.J.: Global Cyber Strategies Index, in: https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/global-cyber-strategies-index; 02.02.2020.

European Court of Auditors 2019: European Defence, Review 09/2019, in: https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=51055; 11.03.2020.

Faesen, Louk et al. 2019a: Conflict in Cyberspace. Parsing the Threats and the State of International Order in Cyberspace, in: https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/conflict-in-cyberspace/; 02.02.2020.

Faesen, Louk et al. 2019b: Conflict in Cyberspace. Global Security Pulse 2019, Strategic Monitor 2019–2020, in: https://hcss.nl/sites/default/files/files/reports/190625%20Cyber%20Pulse%20Final.pdf; 02.02.2020.

Gemeinsame Konferenz Kirche und Entwicklung (GKKE) 2020: Rüstungsexportbericht 2019 der GKKE, in: https://www.gkke.org/wp-content/uploads/2019/12/R%C3%BCstungsexportbericht-2019.pdf; 12.03.2020.

Jiang, Tianjiao 2019: From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar, in: Chinese Journal of International Review 1: 2, 1–23.

Meakins, Joss 2018: Living in (Digital) Denial: Russia's Approach to Cyber Deterrence. Euro-Atlantic Security Report, in: https://www.europeanleadershipnetwork.org/wp-content/uploads/2018/07/Living-in-Digital-Denial-Russia%E2%80%99s-Approach-to-Cyber-Deterrence.pdf; 02.02.2020.

Morgan, Steve 2019: Global Cybersecurity Spending Predicted to Exceed $1 Trillion from 2017–2021, https://cybersecurityventures.com/cybersecurity-market-report/; 02.02.2020.

Mutschler, Max/Bales, Marius 2020: Globaler Militarisierungsindex 2019, in: https://www.bicc.de/uploads/tx_bicctools/BICC_GMI_2019_D.pdf; 05.03.2020.

Orr, Jeff 2019: Global Military Transformation Includes $16 Billion in Cyber Security by 2023, in: https://www.cshub.com/data/articles/global-military-transformation-includes-16-billion-in-cyber-security-by-2023; 02.02.2020.

Sanger, David E./Perlroth, Nicole 2019: U.S. Escalates Online Attacks on Russia's Power Grid, in: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html; 02.02.2020.

Stockholm International Peace Research Institute (SIPRI) 2020: SIPRI Military Expenditure Database, in: https://www.sipri.org/databases/milex; 27.04.2020.

Tillack, Hans-Martin 2019: Luftabwehrsysteme auf Militärtrucks deutscher Hersteller offenbar im Einsatz in Libyen, in: https://www.stern.de/politik/ausland/militaertrucks-deutscher-hersteller-im-buerger-krieg-in-libyen-im-einsatz-8788606.html; 29.01.2020.

Valeriano, Brandon/Jensen, Benjamin 2019: The Myth of the Cyber Offense, Cato Institute Policy Analysis Nr. 862, in: https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint; 02.02.2020.

Wezeman, Pieter D. et al. 2020: Trends in International Arms Transfers, 2019, SIPRI Fact Sheet, in: https://sipri.org/sites/default/files/2020-03/fs_2003_at_2019.pdf; 12.02.2020.

Abbildungen / Grafiken / Tabellen

27 /96
Globale Militärausgaben
Quelle: SIPRI Military Expenditure Data Base.
Layout: Vincent Glasow. BICC, März 2020.

28 /96
Globale Militärausgaben: ausgewählte Anteile
Quelle: SIPRI Military Expenditure Data Base.
Layout: Vincent Glasow. BICC, März 2020.

29 /97
Rang Deutschlands für verschiedene Indikatoren von Militarisierung und Friedlichkeit
Quellen: Militärausgaben und Exporte von Großwaffen: SIPRI Datenbanken; GPI: Institute for Economics and Peace: Global Peace Index 2019, http://visionofhumanity.org/app/uploads/2019/06/GPI-2019-web003.pdf; BICC GMI.

30 /97
Tatsächliche (2019) und gemäß Bundeshaushaltsplan ermittelte deutsche Militärausgaben nach NATO-Kriterien
Quellen: Defence Expenditure of NATO Countries (2013–2019), in: https://www.nato.int/cps/en/natohq/news_171356.htm; Deutscher Bundestag: Finanzplan des Bundes 2019–2023, Drucksache 19/11801; Bundesministerium der Finanzen: Bundeshaushalt 2019, in: https://www.bundeshaushalt.de/fileadmin/de.bundeshaushalt/content_de/dokumente/2019/soll/Haushaltsgesetz_2019_Bundeshaushaltsplan_Gesamt.pdf.
Angaben für 2019 vorläufig; für 2020ff.: Fortschreibung der NATO-Angabe für 2019 mit Zuwachsraten für Verteidigungsausgaben, Bundeshaushalt und Bruttoinlandsprodukt aus Finanzplan des Bundes 2019–2023.
Layout: Vincent Glasow. BICC, März 2020.

31 /99
Anteil an globalen Exporten von Großwaffen 2015–2019
Quelle: SIPRI Arms Transfer Database
Layout: Vincent Glasow. BICC, März 2020.

32 /100
Deutsche Rüstungsexporte
Quellen: GKKE Rüstungsexportberichte. Die Angaben für hochproblematische Länder erfolgen auf Grundlage der Einstufung der Rüstungsexportdatenbank des BICC (ruestungsexport.info). Als "hoch problematisch" werden Länder eingestuft, die mindestens im Hinblick auf vier der insgesamt acht Kriterien als "kritisch" bewertet werden. Die acht Kriterien der Datenbank orientieren sich dabei an den acht Kriterien des Gemeinsamen Standpunktes der EU zu Rüstungsexporten. Hierzu zählen etwa die Menschenrechtssituation im Land, innere Gewaltkonflikte oder die regionale Stabilität. Aufgrund der seit 2017 geänderten methodischen Grundlagen der Rüstungsexportdatenbank sind diese Angaben nur bedingt von Jahr zu Jahr vergleichbar.
Layout: Vincent Glasow. BICC, März 2020.

34 /105
Anzahl staatlich lancierter Cyberattacken
Quelle: Cyber Operations Tracker, Council of Foreign Relations, in: https://www.cfr.org/interactive/cyber-operations; 11.03.2020. Grundlage der Grafik bildet die Datensammlung des Cyber Operations Tracker (COT) des Council of Foreign Relations. COT weist ausdrücklich darauf hin, dass die Attribution von Cyberangriffen ein aufwendiger, methodisch schwieriger und oftmals nicht abgeschlossener Prozess ist. COT bezieht sich auf frei zugängliche Verzeichnisse unparteiischer Organisationen sowie Veröffentlichungen von Cyber-Sicherheitsunternehmen als auch Pressemitteilungen von Regierungsinstitutionen, erhebt jedoch keinen Anspruch auf Vollständigkeit. Die Cyber-Vorfälle werden nach dem Datum ihrer Aufdeckung erfasst, dabei können die Malware oder der Akteur bereits über einen längeren Zeitraum aktiv gewesen sein. Der Zugang zu Quellen wird durch sprachliche Barrieren eingeschränkt, weshalb Cyberangriffe auf Ziele im „Westen“ überrepräsentiert sind.