66. Jahrgang, 43–45/2016, 24. Oktober 2016

bpb:

AUS POLITIK UND ZEITGESCHICHTE

Internationale Sicherheit

APuZ

ZEITSCHRIFT DER BUNDESZENTRALE FÜR POLITISCHE BILDUNG

Beilage zur Wochenzeitung Das **Parlament**

Internationale Sicherheit
APuZ 43–45/2016

EDITORIAL

Internationale Sicherheitspolitik hat sich seit dem Ende des Kalten Krieges deutlich verkompliziert: Statt zweier Machtblöcke, die sich gegenseitig weitgehend in Schach halten und der internationalen Ordnung ein Gerüst geben, gibt es heute viel mehr relevante Akteure, von deren Kooperation oder Konfrontation globale Sicherheit abhängt. Wie schwierig und langwierig es ist, multilateral Konfliktlösungen auszuhandeln, die anschließend auch eingehalten werden, zeigen die Kriege in Syrien und der Ukraine.

Auch die Bedrohungen haben an Komplexität gewonnen: Staaten sind nicht mehr nur „klassischen" Sicherheitsgefahren ausgesetzt, sondern diversen „hybriden" Bedrohungen, die von Desinformationskampagnen über Cyberattacken bis hin zu verdeckten militärischen Operationen reichen können. Sie zeichnen sich unter anderen dadurch aus, dass ihre Urheberschaft gezielt verschleiert wird, was die Abwehr erheblich erschwert. Nicht weniger schwer in den Griff zu bekommen ist die Gefahr, die vom internationalen Terrorismus ausgeht. Ihn einzudämmen, ist eine der wenigen gemeinsamen Prioritäten, auf die sich die Staatengemeinschaft offiziell einigen kann. Wirksame Terrorismusbekämpfung erfordert größte Anstrengungen und eine bessere Vernetzung auf allen Ebenen. Die Anschläge in Paris und Brüssel 2015/16 haben sowohl Stärken als auch Schwächen der internationalen Sicherheitszusammenarbeit deutlich vor Augen geführt.

Staaten wie Deutschland, aber auch die Europäische Union insgesamt, sehen sich stärker denn je gezwungen, sicherheitspolitische Verantwortung zu übernehmen, Lasten und Aufgaben zu teilen und sich – etwa durch Geheimdienstkooperation – immer intensiver auszutauschen. In demokratischen Gesellschaften sollte dies einhergehen mit einer öffentlichen Debatte über die Balance zwischen Freiheit und Sicherheit sowie über die ethische und rechtliche Angemessenheit der angewendeten Mittel.

Johannes Piepenbrink

ESSAY

WOHIN TREIBT DIE WELT?

Ulrich Menzel

1994 skizzierte der Friedensforscher Dieter Senghaas in dem Band „Wohin driftet die Welt?“ ein zivilisatorisches Hexagon aus staatlichem Gewaltmonopol, Rechtsstaatlichkeit, demokratischer Partizipation, sozialer Gerechtigkeit, konstruktiver Konfliktkultur und Affektkontrolle.[01] Noch unter dem Eindruck des säkularen Umbruchs der Jahre 1989/90 lautete die idealistische Botschaft, dass die Probleme dieser Welt lösbar sind, dass im Rahmen der von US-Präsident George Bush sen. verkündeten „Neuen Weltordnung“ die friedliche Koexistenz der Nationen, eine Kultur des Friedens, möglich ist, sofern die zivilisatorischen Eckpunkte des Hexagons sich erfüllen. Senghaas versäumte nicht den Hinweis, dass die Kultur des Friedens brüchig ist, sobald es zu neuen Konfliktlagen kommt.

Heute, gut 20 Jahre später, erweist sich die Warnung leider als gerechtfertigt. Die ernüchternde Botschaft lautet: In einer wachsenden Zahl von Ländern ist kein zivilisatorischer Fortschritt, sondern ein schleichender, in manchen sogar ein dramatischer Rückschritt in jeder der Hexagon-Dimensionen zu verzeichnen. Die Kluft zwischen Arm und Reich wächst nicht nur innerhalb, sondern auch zwischen den Gesellschaften.[02] Von einer neuen, auf Kooperation beruhenden Weltordnung unter dem Dach der Vereinten Nationen kann keine Rede sein.

Im Gegenteil – die Welt treibt Richtung Unregierbarkeit. Die unsortierten Stichworte dieses seit Jahren zu konstatierenden Trends lauten: Krieg in der Ukraine, Griechenland-Krise, Krieg und Staatszerfall im Komplex Irak-Syrien mit destabilisierenden Konsequenzen für die Nachbarländer, Scheitern der militärischen Interventionen weltweit, Ausbreitung terroristischer Organisationen, grassierender Staatszerfall in Subsahara-Afrika, neue und massenhafte Migrationsbewegungen, die nicht nur durch das Elend des Krieges, sondern auch durch die Perspektivlosigkeit in vielen Ländern ausgelöst werden, Restauration des 1990 geschrumpften ehemaligen sowjetischen Einflussbereichs, Rückkehr des Rüstungswettlaufs, Krise der Linksregierungen in Lateinamerika, Krise der EU, Brexit, Trump.

Ein Problem verdrängt das andere in der öffentlichen Wahrnehmung, ohne dass nur eines gelöst wäre. Sicher ist nur, dass sie und weitere, die noch im Verborgenen schlummern, auf absehbare Zeit auf der Agenda stehen werden – mit der Konsequenz, dass die internationalen Institutionen überfordert und die USA nicht mehr bereit sind, allein oder ganz überwiegend die Lasten zur Ordnung der Welt zu tragen, während die anderen als *free-* oder *cheaprider* daran partizipieren. Obwohl Europa eigentlich mehr Verantwortung übernehmen müsste, wächst der Trend zur Selbsthilfe statt des Vertrauens in die EU, wodurch Deutschland in die ungeliebte Rolle des „Eurohegemons“ gedrängt wird. Verantwortlich für das düstere Szenario wachsender Unregierbarkeit sind langfristige Entwicklungen, die keinen linearen, sondern einen exponentiellen Verlauf nehmen, bis sogenannte Kipppunkte erreicht sind.

Eine wesentliche Ursache der geschilderten Problemlage ist paradoxerweise, dass in großen Teilen der Welt Entwicklung nachgeholt wird und in den alten Industrieländern unvermindert fortschreitet. Dies bedeutet Wirtschaftswachstum, bessere Ernährung und medizinische Versorgung mit der Konsequenz von Bevölkerungswachstum bei steigender Lebenserwartung und höherem Pro-Kopf-Einkommen – und zugleich wachsende Ungleichheit bei Einkommen und Vermögen innerhalb und zwischen den Ländern. In einer Generation hat sich die Weltbevölkerung auf mehr als 7,5 Milliarden verdoppelt – ein welthistorisch einmaliger Vorgang, der zeigt, dass ein langfristiges lineares in ein kurzfristiges exponentielles Wachstum umgeschlagen ist.[03] Alles zusammen führt mit dem gleichen Exponenten zu steigendem Verbrauch und steigender Belastung von Böden, Mineralien, Energie, Wasser, Biodiversität und Luft mit Konsequenzen für Umweltverschmutzung und Klimawandel. Da-

raus resultieren innergesellschaftliche Verteilungskonflikte um Berufschancen, Lebensperspektiven, knapper werdende Ressourcen, Renteneinkommen und neue Formen des Kolonialismus, die sich etwa im *landgrabbing* äußern.

VIER ORDNUNGSMODELLE

Während der Bedarf nach Weltordnung wächst, schwindet zugleich die Fähigkeit, diesen zu bedienen. Angesichts dessen, dass es einen mit einem globalen Gewaltmonopol ausgestatteten Weltstaat nicht gibt, sind grundsätzlich vier Modelle denkbar, wie mit der wachsenden Anarchie der Staatenwelt umgegangen werden kann.[04] Dem realistischen Denken entspricht das **Selbsthilfeprinzip**. Jeder Staat versucht so gut er kann, seine Interessen gegenüber einer abträglichen Welt aus eigener Kraft wahrzunehmen. Dazu benötigt er Macht und wirtschaftliche Ressourcen. Für große Staaten ist dies eher möglich als für kleine, zumal Erstere immer die Option des Isolationismus besitzen. China und die USA sind die prominentesten Beispiele.

Dem idealistischen Denken entspricht die **Kooperation der Staaten** durch Verträge, internationale Organisationen, das Völkerrecht und normengeleitetes Handeln, das auf gemeinsamen Werten beruht. Das Recht ersetzt die Macht, Arbeitsteilung ersetzt die Autarkie. Die EU war und ist das prominenteste und weltweit erfolgreichste Beispiel.

Wenn man nicht die Anarchie, sondern die Hierarchie der Staatenwelt als ihr wesentliches Merkmal ansieht, kann man zudem zwischen dem **hegemonialen Modell** und dem **imperialen Modell** unterscheiden. Anstelle des nicht vorhandenen Weltstaats sorgen die großen Mächte für Ordnung. Der (benevolente) Hegemon stützt sich auf seine überragende Leistungsfähigkeit und die Akzeptanz der Gefolgschaft, weil er Ordnung durch die Bereitstellung internationaler öffentlicher Güter garantiert und zivilisatorische Ausstrahlungskraft (*soft power*) besitzt. Die USA haben die Rolle des Hegemons nach 1945 über die westliche und nach 1990 über die gesamte Welt eingenommen. Das Imperium hingegen nimmt seine Ordnungsfunktion über Herrschaft wahr, braucht keine Gefolgschaft, sondern kennt nur Knechtschaft. Es liefert aber sogenannte Clubgüter für die zuvor Unterworfenen und stützt sich auf deren Ressourcen. Die Sowjetunion gehörte zu diesem Typ.

(UN)ORDNUNG IN DER BI- UND UNIPOLAREN WELT

Damit konzentriert sich die Frage internationaler Ordnung durch Weltregieren darauf, wer, wie und in wessen Interesse internationale öffentliche Güter wie (militärische) Sicherheit und (wirtschaftliche) Stabilität bereitstellt. Öffentliche Güter sind durch die Kriterien Nichtausschließbarkeit und Nichtrivalität definiert. Die Bereitstellung erfolgt durch den Staat, der auch die Regeln ihrer Nutzung bestimmt. Um private Güter handelt es sich, wenn die gegenteiligen Kriterien erfüllt sind. Der Markt liefert die Regeln zu deren Nutzung. Fehlt die Nichtrivalität, spricht man von Allmendegütern, die als freie Gaben der Natur bereitstehen, zur nachhaltigen Nutzung aber sehr wohl der Verregelung bedürfen. Fehlt die Nichtausschließbarkeit, spricht man von Clubgütern, für deren Regeln die Satzung eines Vereins zuständig ist.

Bei internationalen öffentlichen Gütern kommt als drittes Kriterium deren Unentgeltlichkeit hinzu. Nur der Hegemon beziehungsweise dessen Steuerzahler kommen für die Bereitstellung auf, alle anderen sind *freerider*. Internationale Clubgüter haben eine regionale Reichweite, da sie nur von denen in Anspruch genommen werden, die zum „Club" des Imperiums gehören. Da sie zu den Finanzierungskosten herangezogen werden, sind sie auch keine *freerider*. Am schwierigsten gestaltet sich die Verregelung der internationalen Allmendegüter (Hohe See, Luft, grenzüberschreitende Flusssysteme, Polargebiete), bei denen immer die Übernutzung und somit die „Tragik der Allmende" (*tragedy of the commons*) droht.[05] Dies erklärt, warum internationale Umweltabkommen so wenig Erfolg zeigen.

01 Vgl. Dieter Senghaas, Wohin driftet die Welt? Über die Zukunft friedlicher Koexistenz, Frankfurt/M. 1994.

02 Vgl. Thomas Piketty, Das Kapital im 21. Jahrhundert, München 2014.

03 Die ursprünglich für die Erderwärmung gebrauchte, aber auch hier passende Metapher lautet „Hockeyschläger-Effekt". Vgl. Michael Mann, The Hockeystick and the Climate War: Dispatches from the Frontline, New York 2012.

04 Vgl. Ulrich Menzel, Die Ordnung der Welt. Imperium und Hegemonie in der Hierarchie der Staatenwelt, Berlin 2015.

05 Dass diese aber nicht zwingend ist, zeigt Elinor Ostrom, Die Verfassung der Allmende. Jenseits von Staat und Markt, Tübingen 1999. Siehe hierzu auch die APuZ 28–30/2011 (Gemeingüter), www.bpb.de/33201 (*Anm. d. Red.*).

Insofern wirkte die bipolare Konstellation bis 1990 trotz Ost-West-Konflikt stabilisierend. Die USA stellten internationale öffentliche Güter und die Sowjetunion regionale Clubgüter für die Staaten des Warschauer Paktes und weitere Länder des sozialistischen Lagers wie Kuba oder Vietnam bereit. Auch Neutrale standen als *freerider* unter dem Nuklearschirm der USA. Die unipolare Konstellation nach 1990 hat dazu geführt, dass die Hegemonie der USA quasi über Nacht global geworden ist. Aus dem „unipolaren Moment“[06] wurde ein Zustand. Zu den Ordnungsleistungen der USA gehörten neben der durch ein weltweites System von Stützpunkten gewährleisteten militärischen Sicherheit die Garantie eines Welthandels- und Weltfinanzsystems mit dem US-Dollar als Leitwährung und den Vereinigten Staaten als letzten Kreditgeber und *safe haven*, die Sicherung der Tankerrouten zum Persischen Golf, der Aufbau eines globalen Kommunikations-, Informations- und Orientierungssystems durch Internet und GPS und vieles weitere mehr. Seit den Anschlägen vom 11. September 2001 gab es zudem eine deutliche Ausweitung der Rolle des „Weltpolizisten“, der sich im Rahmen des „Kriegs gegen den Terror“ auch für die innere Sicherheit in verbündeten Staaten zuständig sieht.

Mit Antritt der Obama-Administration 2009 haben sich jedoch die Anzeichen gemehrt (Doppeldefizit von Haushalt und Handel), dass die USA nicht mehr bereit und in der Lage sind, die Rolle des Hegemons wahrzunehmen. Daraus resultiert die Forderung der USA nach Lastenteilung, die sich an die *freerider* in Westeuropa, Asien und am Persischen Golf richtet. Zudem besteht für ein Land von der Größe der USA immer die Alternative des Isolationismus. Aus dem „Battleship USA“ würde dann eine „Fortress USA“, statt „America as Number One“ hieße es „America First“. Der Wahlkampfslogan des Präsidentschaftskandidaten Donald Trump „Make America Great Again!“ ist der bewusste oder unbewusste Ausdruck dieser Alternative und reflektiert auf populistische Art den zweiten „Niedergang Amerikas“ (*American decline*).[07]

06 Vgl. Charles Krauthammer, The Unipolar Moment, in: Foreign Affairs 1/1991, S. 22–33.

07 Als erster „American Decline“ wurde in den 1980er Jahren die vermeintliche Gefährdung der wirtschaftlichen Vormachtstellung der USA durch Japan diskutiert. Vgl. Paul Kennedy, The Rise and Fall of the Great Powers, New York 1987.

Ein Zwischenfazit lautet demzufolge, dass sich derzeit keine der vier skizzierten Optionen (Selbsthilfe, Kooperation, hegemoniales Modell, imperiales Modell) aufdrängt, auch wenn die Attraktivität des Selbsthilfeprinzips angesichts des wachsenden Zulaufs populistischer Strömungen derzeit im Aufwind ist.

MULTIPOLARE (UN)ORDNUNG

Wenn die USA isolationistische Neigungen zeigen, wie es bis zum Ersten Weltkrieg und erneut in der Zwischenkriegszeit der Fall war, wer könnte die Rolle der USA allein oder im Verbund übernehmen oder zumindest substanziell stützen?

China, dessen Sozialprodukt etwa bis 2030/35 das US-amerikanische übertreffen wird, ist der erste Kandidat für eine Lastenteilung. Aber anders als Japan, das in den 1980er Jahren als der wirtschaftliche Herausforderer galt, will China kein Juniorpartner der USA sein. In ungebrochenem traditionellem Selbstverständnis sieht es sich als „Land der Mitte“. Es verweigert daher auf allen Feldern, die nicht im chinesischen Interesse liegen, eine Lastenteilung, zumal die USA (noch) nicht bereit sind, die Rolle des Hegemons zu teilen.

Chinas Aktivitäten konzentrieren sich auf Zentralasien („Neue Seidenstraße“), den asymmetrischen Handel mit Russland (Fertigwaren gegen Rohstoffe), Ostafrika (*landgrabbing* zur Versorgung mit Nahrungsmitteln), das Rote Meer und den Persischen Golf, um die Ölversorgung zu sichern. Dazu investiert es in die Rohstoffsektoren vieler Länder, durchdringt häufig auch deren Binnenwirtschaft und unterhält gute Beziehungen zu sogenannten Schurkenstaaten, die unter dem Druck des Westens stehen. Zudem wird es in neuen internationalen Organisationen aktiv, die ohne Beteiligung der USA auskommen (etwa in den BRICS, der Shanghaier Organisation für Zusammenarbeit oder asiatischen Entwicklungsbanken). Mit der pazifischen Flotte forciert China darüber hinaus eine Rüstung, die nicht der Landesverteidigung dient, sondern die Seerouten in das Becken des Indischen Ozeans sichern soll. Die Redeweise vom „friedlichen Aufstieg“ hat demgegenüber nur legitimatorischen Charakter.

Das chinesische Modell eines Entwicklungsstaates, das Wachstum mit einem autoritären politischen System verbindet, verströmt eine Art *soft power* der speziellen Art und ist für afrikanische und asiatische Despoten eine attraktive Al-

ternative zum westlichen Modell im Sinne des oben geschilderten Hexagons. Theoretisch ausgedrückt ist China zwar bereit, Clubgüter für solche Staaten zu liefern, die zu seinem Interessenbereich gehören, aber unter Verweis, dass man immer noch Entwicklungsland sei, versteht sich das Land in globaler Hinsicht als *freerider* der USA. Für den Europa umgebenden Krisengürtel von der Ukraine über den Kaukasus bis hin zum Nahen Osten bedeutet das: Das Engagement der USA lässt nach, und China bleibt passiv.

Ganz anders verhält es sich mit **Russland**. Nach Überwindung der Transformationskrise der Jelzin-Ära, spätestens seit Beginn der zweiten Präsidentschaft Putins, verfolgt es eine revisionistische Politik der Rückgewinnung des ehemaligen sowjetischen Einflusses. Das ist der Kern des „Putinismus". Dazu werden politische (Konfrontation in der UNO), wirtschaftliche (Konditionierung bei Gasexport, Trassenverlauf von Pipelines) und militärische Mittel (Ukraine, Syrien) strategisch eingesetzt. Russlands internationales Engagement ist gerade in Syrien nicht im Sinne einer Lastenteilung mit den USA zu verstehen, sondern als Versuch, die Reichweite der US-Hegemonie zu reduzieren. Insofern hat der Revisionismus eine prinzipiell antiamerikanische Tendenz. In Syrien wird prioritär nicht der selbsternannte „Islamische Staat" (IS) bekämpft, sondern das Assad-Regime gestützt, um einen alevitischen Reststaat an der Küste unter russischer Garantie zu behaupten, der einen Marinestützpunkt im Mittelmeer (wie auf der Krim) garantiert. Die Kaspische Flotte und nicht die Schwarzmeerflotte wird eingesetzt, weil so der Luftweg über Iran und Irak möglich ist und das NATO-Mitglied Türkei nicht überflogen werden muss. Die USA sehen sich mit der paradoxen Situation konfrontiert, einerseits die syrischen Kurden gegen den IS zu unterstützen und andererseits mit der Türkei zu kooperieren, obwohl Türken und Kurden sich an vielen Fronten bekämpfen.

ÜBERGREIFENDE ENTWICKLUNGEN

Damit verschärft Russland eine komplexe Gemengelage von Konflikten, die ursprünglich separate Wurzeln hatten und in denen vor allem drei übergreifende Entwicklungen in fataler Weise zutage treten und zusammenlaufen. Als *erstes* ist die religiöse Aufladung kriegerischer Auseinandersetzungen zu nennen.[08] Diese speist sich zum einen aus dem alten Schisma des Islam zwischen Sunniten und Schiiten, das sich heute im Hegemonialkonflikt zwischen Saudi-Arabien im Verbund mit den Golfstaaten und Iran offenbart: In allen arabischen Ländern, die religiös gespalten sind, unterstützt Iran die Schiiten. Die arabischen Ölstaaten intervenieren auf der sunnitischen Seite finanziell, durch Waffenlieferungen und, wie im Falle des Jemen, auch militärisch. Zum anderen werden zahlreiche Konflikte zu einem Kampf zwischen Christentum und Islam stilisiert. Für IS-Kämpfer etwa sind US-Amerikaner und Europäer schlicht „Kreuzfahrer", wodurch eine Religionsfeindschaft mit jahrhundertealter Tradition konstruiert wird. Sowohl innerstaatliche Konflikte (etwa in Nigeria) als auch der globale islamistische Terrorismus erfahren eine solche religiöse Aufladung.

Die *zweite* Entwicklung, die im aktuellen Krisenbündel eine Rolle spielt, ist die wachsende Unregierbarkeit im Weltmaßstab, resultierend aus dem Zerfall vieler postkolonialer Staaten, die vielfach nur auf dem Papier beziehungsweise in der Hauptstadt bestanden und nur die staatliche Symbolik zu inszenieren wussten, ohne öffentliche Güter für ihre Bürger bereitzustellen. Hier wirkte der Ost-West-Konflikt stabilisierend, weil beide Seiten ihre Klientel mit Waffen, Ausbildern, Entwicklungs- und Finanzhilfe und damit die vorrangige Rentenorientierung unterstützten, die einer Entwicklung nach westlichem Muster entgegenstand. Nach 1990 fiel die sowjetische Hilfe für die Länder des Ostblocks weg, und die westliche Hilfe für die eigenen Verbündeten wurde reduziert beziehungsweise mit politischen Auflagen versehen. In dieses Vakuum ist nun China vorgestoßen, und Russland könnte diesem Beispiel folgen, weil Menschenrechtsverletzungen ignoriert und die Rentenorientierung nicht infrage gestellt werden.

Drittens kommt die Transformation des Terrorismus zum quasistaatlichen Akteur hinzu. Al-Qaida war der Prototyp eines weltweit operierenden Netzwerkes, das lediglich Rückzugsräume und Ausbildungslager benötigte. Die neue Generation – vornehmlich der IS – baut staatliche Strukturen auf, in denen die Akteure im wahrsten Sinne des Wortes das Gewaltmonopol behaupten. Nicht nur der Westen, die gesamte Welt soll

08 Ein Phänomen, das bezeichnenderweise nur die monotheistischen Religionen betrifft, die einen absoluten Wahrheitsanspruch haben.

mit einem radikal alternativen Gesellschaftsmodell konfrontiert werden. Der Terrorismus wird zu einer Macht und für die Unterprivilegierten und Perspektivlosen weltweit attraktiv. Da sich Verhandlungen mit Organisationen wie dem IS grundsätzlich ausschließen und die USA nach den Erfahrungen in Afghanistan und Irak den Einsatz von Bodentruppen scheuen, bleibt nur der Drohnenkrieg und am Ende die Stützung der autoritären Regime in den vom Terrorismus bedrohten Ländern.

WIE WEITER?

Die vielfältigen Krisen haben dazu geführt, dass wir derzeit ein Szenario erleben, das der Soziologe und Ökonom Albert O. Hirschman mit seinem Buch „Exit, Voice and Loyality“[09] schon in den 1970er Jahren auf den Begriff gebracht hat: Nach langer passiver Erduldung von autoritären Systemen und Staatsversagen und dem Versuch einiger Gesellschaften, den Weg des Widerspruchs zu gehen (etwa im „Arabischen Frühling“), sehen sich viele Menschen angesichts von Perspektivlosigkeit und Krieg nun dazu gezwungen, die Exit-Option zu „wählen“ und abzuwandern. Das exponentielle Bevölkerungswachstum der zurückliegenden 30 bis 40 Jahre mit den oben skizzierten Konsequenzen hat mancherorts einen Kipppunkt erreicht, an dem die sozialen und politischen Systeme implodieren. Die Exit-Option ist zur gemeinsamen Konsequenz der vielen Krisenherde dieser Welt geworden, gleichviel welche Ursachen sie von Fall zu Fall haben.

Eine Befriedung des Europa umgebenden Krisengürtels ist in absehbarer Zukunft kaum zu erwarten. Eher droht die Destabilisierung der noch stabilen Inseln, wird sich die Krisenregion über die Sahara hinweg ausweiten. Weil die USA zögern, China passiv bleibt und Russland eine revisionistische Politik betreibt, wird Europa gezwungen sein, in stärkerem Maße als bisher im eigenen Interesse für die öffentlichen Güter Sicherheit und Stabilität an seiner Peripherie zu sorgen und selbst wie eine große Macht zu handeln.

Eine wirksame gesamteuropäische Strategie, den Herausforderungen, insbesondere den wachsenden Fluchtbewegungen, zu begegnen, ist aufgrund der heterogenen Betroffenheit wenig wahrscheinlich, zumal das „Projekt EU“ insgesamt in eine vor wenigen Jahren noch unvorstellbare Krise geraten ist. Das politische Ziel, die Fluchtursachen zu bekämpfen, kann zudem nur langfristig Wirkung zeigen. Kurzfristig sind daher zwei Szenarien denkbar: Entweder kehrt Europa zum Selbsthilfeprinzip zurück, und jedes Mitgliedsland greift nach ungarischem Muster zu den Maßnahmen, die seiner individuellen Interessenlage und seinen Kapazitäten entsprechen. Dies würde die Krise Europas verschärfen. Oder es kommt zu einer hegemonialen Lösung, bei der Deutschland notgedrungen voranschreitet.

In der benevolenten Variante hieße das, dass Deutschland den größten Teil der Kosten und des Personals für die europäische Grenzschutzagentur Frontex, den Marineeinsatz im Mittelmeer, den Bau von Erstaufnahmelagern in Griechenland, Spanien und Italien sowie der Zahlungen an die Türkei, Ägypten oder Jordanien zu leisten hätte, damit die Geflüchteten dort in den Lagern bleiben. Es wäre aber auch dasjenige Land, das mit Abstand die meisten Menschen aufnähme.

In der malevolenten Variante würde Deutschland sich auf die Kontrolle der eigenen Grenzen konzentrieren, die eigene Attraktivität durch Kürzung der Sozialleistungen reduzieren, Asylverfahren beschleunigen und Rückführungen intensivieren. Dazu gehört auch, dass es nicht etwa ein europäisches, sondern nur ein deutsches Einwanderungsgesetz gäbe.

Welches der Szenarien verfolgt wird, hängt nicht zuletzt von Wahlen ab. Zuwanderung ist überall das große innenpolitische Thema. So wie sich die US-amerikanische Innenpolitik als entscheidende Variable bezüglich der Richtung in der Weltpolitik herausgestellt hat, so dürfte sich das künftig im Falle Deutschlands bezüglich der Europapolitik erweisen. Wohin treibt die Welt? Dass sie nicht weiter Richtung Unregierbarkeit treibt, hängt davon ab, inwiefern die großen Mächte ihre Verantwortung erkennen und wahrnehmen.

ULRICH MENZEL
ist Professor für Politikwissenschaft. Er war bis 2015 Inhaber des Lehrstuhls für Internationale Beziehungen und Vergleichende Regierungslehre an der TU Braunschweig. Zuletzt erschien von ihm „Die Ordnung der Welt“ (2015).
p.u.menzel@t-online.de

09 Vgl. Albert O. Hirschman, Abwanderung und Widerspruch. Reaktionen auf Leistungsabfall bei Unternehmungen, Organisationen und Staaten, Tübingen 1974.

HYBRIDE BEDROHUNGEN

Sicherheitspolitik in der Grauzone

Florian Schaurer · Hans-Joachim Ruff-Stahl

Das sicherheitspolitische Umfeld der vergangenen Jahre ist sowohl von einer begrifflichen Popularisierung „hybrider Bedrohungen" und unzähligen Versuchen der Theoriebildung einerseits sowie von einer tatsächlichen Zunahme entsprechender Konfliktpotenziale andererseits gekennzeichnet. Während sich in Ermangelung übergreifender Legaldefinitionen weiterhin insbesondere akademische Kontroversen um das Verständnis dieses wenigstens in der Gesamtschau zum Teil neuartigen Konflikttyps entfachen, schreiten die politische Strategieentwicklung und Operationalisierung von Abwehrmaßnahmen national und international voran. Im Folgenden soll dies genauer beleuchtet werden.

Hybride Bedrohungen können verstanden werden als ein planvoller, mithin nichtlinearer Einsatz unterschiedlicher Fähigkeiten über das gesamte DIMEFIL-Spektrum[01] hinweg mit dem Ziel, politische Wirkung unterhalb der Schwelle eines bewaffneten Angriffs zu erzielen und die Handlungs- und Reaktionsfähigkeit des Gegners zu beeinträchtigen.[02] Hybride Bedrohungen manifestieren sich in den Peripherien und Einflusssphären vornehmlich staatlicher Akteure, deren Verhalten und Vorgehen vom Versuch der Verschleierung und Dementierbarkeit eigener Urheberschaft gekennzeichnet sind. Intensität und Attribution sind somit die zwei wesentlichen Hebel und Schwellen des hybriden Kontinuums, das stets sowohl innen- wie außenpolitische Bezüge aufweist und von Einflussnahme bis hin zur Kriegführung reichen kann.

Die Perspektive der Verteidigung richtet sich zuerst auf mögliche schädigende Effekte hybriden Vorgehens. Dabei können die politischen Intentionen hybrider Akteure durchaus variieren, die zur Anwendung kommenden Instrumente ähneln einander jedoch und sind Ausgangspunkte für die zivile und militärische Verteidigungsplanung. Das Vorliegen einer hybriden Bedrohung lässt sich allein in ihrem Gesamtzusammenhang feststellen. Im Zusammenspiel verschiedener, auf den ersten Blick womöglich nicht zusammenhängender Komponenten ergibt sich der hybride Kontext.

„SHADES OF GREY"

Die hybride „Grauzone", die weniger einen organischen Wandel als vielmehr eine beabsichtigte Diffusion der Form internationaler Konfliktaustragung darstellt, ist sowohl Ort als auch Methode. Hybridität ist in ihren Einzelbestandteilen eine essenziell taktisch-operative, in der Gesamtschau aber eine strategisch-politische Herausforderung. Die konstruierte und inszenierte Ambiguität und Adaptivität des Geschehens und seiner Urheber macht dabei die „Originalität" des hybriden Ansatzes aus – und zugleich die beträchtlichen Schwierigkeiten einer zutreffenden analytischen Bewertung und angemessenen politischen Würdigung. Hinzu kommt, dass die Methode oft experimentell und innovativ angelegt ist. So lassen sich hybride Angriffe etwa im Cyber- und Informationsraum bisweilen als Improvisationen mit zunächst ungewissem Ausgang bewerten, was ihre Gefährlichkeit tendenziell erhöht und ihr Erkennen im Voraus verunmöglicht.

Wo aber Versuch ist, da ist auch Irrtum, und so sind bei Weitem nicht alle potenziell Erfolg versprechenden hybriden Angriffe wirklich erfolgreich. Natürlich ist nicht jeder Versuch der Einflussnahme ein gegen die nationale Sicherheit eines Staates gerichteter subversiver Sabotageakt, nicht jedes Scharmützel Auftakt einer größeren Kampagne. Der Verteidiger darf es dabei jedoch nicht bewenden lassen und muss bestrebt sein, eigene Verwundbarkeiten zu beseitigen und unvermeidliche Restrisiken klar zu erkennen. Dabei sollte er die destruktive Kreativität und den von Regeln selten gehegten Pragmatismus möglicher Gegner antizipieren und das eigene Arsenal an Mitteln und Optionen – selbstverständlich unter Achtung der Regeln – entsprechend ausrichten.

Insoweit die hybride Einflussnahme als politische Methode zunehmend einen Regelfall der Austragung von Antagonismen in den internationalen Beziehungen darstellt – auch und gerade im Zuge der „Renaissance klassischer Machtpolitik“[03] – ist sie ganz ungeachtet etwaiger konzeptioneller Vagheit in ihren Auswirkungen real erfahr- und damit beschreibbar. Bereits aus abstrakten Gefährdungslagen, das heißt der bloßen Denkbarkeit und damit Möglichkeit der Materialisierung einer Bedrohung, ergeben sich Anforderungen an eine effiziente zivil-militärische Gesamtverteidigung.

Historisch gesehen ist die hybride Methode nichts gänzlich Neues. Bereits der preußische Militärphilosoph Carl von Clausewitz erfasste, dass die Anwendung strategischer Instrumente ausschließlich der Willensmodifikation des politisch Anderen dient, denn Frieden, Konflikte und Krieg sind allesamt soziale Phänomene. Die Wahl des politischen Instruments zur Beeinflussung ist dabei zweitrangig. Allerdings muss sich der Anwender dieser Mittel mit Unberechenbarkeiten abfinden, die aus der „wunderlichen Dreifaltigkeit“ von, modern ausgedrückt, strategischem Handeln, der öffentlichen Meinung und nichtlinearen Ursache-Wirkungsbeziehungen entstehen.

CYBERRAUM ALS OPERATIONSRAUM

Das im Juli 2016 vorgestellte „Weißbuch der Bundesregierung zur Sicherheitspolitik und zur Zukunft der Bundeswehr“ greift die hybride Bedrohungslage als eine zentrale sicherheitspolitische Herausforderung prominent auf. In ihrer Querschnittlichkeit über Landes- und Ressortgrenzen hinweg sind hybride Bedrohungen ähnlich gelagert wie solche aus dem Cyberraum, weshalb es nicht überrascht, dass der Cyberraum selbst ein bevorzugter Operationsraum hybrider Akteure ist. So fanden im Frühjahr 2015 etwa Cyberangriffe auf die Websites verschiedener Bundesministerien statt, im Dezember 2015 wurden Teile des ukrainischen Stromnetzes durch einen Cyberangriff ausgeschaltet.[04]

Während Cyberkriminalität vor allem an einem unmittelbar materiellen Gewinn orientiert und damit zunächst Gegenstand der Strafverfolgung ist, nutzen hybride Akteure, deren Verhalten häufig einen nichtstaatlichen Eindruck erweckt, diese Domäne aus strategischen Gründen, um politische Ziele durchzusetzen. Cyberangriffe können, vorausgesetzt ihre Erheblichkeit ist in Ausmaß und Auswirkung mit der eines konventionellen bewaffneten Angriffs vergleichbar, als eine Form der Kriegführung gewertet werden. Daher bedarf es einer möglichst nahtlosen Organisation der Cybersicherheit, sowohl als Cyberabwehr im Kontext des Friedens (unter Federführung des Innenministeriums), wie auch als Cyberverteidigung im Spannungs- und Verteidigungsfall (unter Federführung des Verteidigungsministeriums). Dies bedeutet auch, dass Rollenverteilung und Zuständigkeiten der Ressorts weiter ausdefiniert werden müssen, nicht zuletzt im Rahmen der Cyber-Sicherheitsstrategie 2016 der Bundesregierung. Die Bundeswehr wiederum vollzieht derzeit die Einrichtung eines Kommandos Cyber- und Informationsraum.

Ein Denken in starren Zuständigkeiten ist dabei zu vermeiden. „Innere und äußere Sicherheit sind nicht mehr trennscharf voneinander abzugrenzen. Störungen und Gefährdungen bewegen sich vielfach an deren Schnittstelle. Sie nehmen gezielt Verwundbarkeiten unserer offenen und global vernetzten Gesellschaft ins Visier.“[05]

Die im August 2016 vom Bundesministerium des Innern vorgestellte „Konzeption Zivile Verteidigung“, die gemeinsam mit der aus dem Weißbuch abgeleiteten „Konzeption der Bundeswehr“ in eine Novelle der „Rahmenrichtlinien für die Gesamtverteidigung“ einfließen soll, knüpft hieran an. Für den bundesdeutschen Föderalismus und die vorrangige Zuständigkeit der Länder für die innere Sicherheit wird – unterhalb der Schwelle eines bewaffneten Angriffs – eine potenziell schwerwiegende Schwachstelle identifiziert: „Zu den besonderen Herausforderungen hybrider Bedrohungen für die nationale Zivile Verteidigung gehört die späte Erkennbarkeit und Zurechenbarkeit entsprechender

01 DIMEFIL steht für Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal.

02 Entsprechende Einsätze können derweil sehr wohl einen Bruch des als Völkergewohnheitsrecht anerkannten Gewaltverbots (Artikel 2(4) UN-Charta) oder des Prinzips der Nichteinmischung in die inneren Angelegenheiten eines Staates sowie anderer Gepflogenheiten und Normen der internationalen Beziehungen bedeuten.

03 Bundesregierung, Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr, Berlin 2016, S. 38.

04 Vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE (Sogenannte hybride Bedrohungen und deren tatsächliche Gefährlichkeit), 11.8.2016, Bundestagsdrucksache (BT-Drs.) 18/9388, S. 2

05 Weißbuch (Anm. 3), S. 48.

Handlungen zu staatlichen Akteuren. Solange der Spannungs-, Verteidigungs- oder Bündnisfall nicht formal festgestellt wird, verbleibt die Zuständigkeit für die Gefahrenabwehr und Lagebewältigung bei den Ländern. In diesem Vorfeld bleibt der Bund auf die Unterstützung der Länder beschränkt und verschiedene rechtliche Instrumente bleiben unanwendbar. So können sich Lagen ergeben, bei deren Bewältigung das verfügbare rechtliche Instrumentarium an seine Grenzen stößt."[06]

ROLLE DER EU

Die Bundesregierung antwortete unlängst auf eine Kleine Anfrage zu hybriden Bedrohungen: „In der jüngsten Vergangenheit lieferte vornehmlich das russische Vorgehen auf der Krim und in der Ost-Ukraine Beispiele hybrider Eskalationsdynamik. Diese Fälle haben das Bewusstsein der Bundesregierung dafür geschärft, dass zur Abwehr ‚hybrider Bedrohungen' neben der Stärkung nationalstaatlicher Resilienz eine Kooperation zwischen der NATO und der EU sowie ggf. die Einbindung weiterer Organisationen zielführend sind."[07]

In einer gemeinsamen Mitteilung an das Europäische Parlament und den Rat haben die Europäische Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik Federica Mogherini im April 2016 einen „Gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen" vorgelegt. Dessen Schwerpunkte sind Sensibilisierung, Prävention, Reaktion und Resilienz, die wiederum durch 22 vorgeschlagene Einzelmaßnahmen erreicht werden sollen. Die Stärkung präventiver und reaktiver Resilienz, die im Mittelpunkt der Abwehrmaßnahmen steht, dient vornehmlich dem Schutz und der Aufrechterhaltung beziehungsweise Wiederherstellung kritischer Infrastrukturen, die ausdifferenziert werden in Energienetze, Verkehr und Lieferketten, Raumfahrt, Verteidigungsfähigkeit, Gesundheit und Ernährungssicherheit, Cybersicherheit und das Finanzwesen. Die Priorisierung des Schutzes kritischer Infrastrukturen ist nicht notwendigerweise spezifisch hybriden Bedrohungen geschuldet, sondern ist in allen Bedrohungslagen als originäre Aufgabe des Staates und der Betreiber zu gewährleisten. Allerdings erfordern hybride Angriffstechniken, diesen Schutz ganzheitlicher zu denken und verstärkt unkonventionelle Szenarien zu berücksichtigen. Vorangestellt wird die Priorisierung strategischer Kommunikation, die ganz überwiegend auf genuin hybride Bedrohungen im Informationsraum rekurriert und in der Tätigkeit der bereits bestehenden „East StratCom Task Force"[08] und „Arab StratCom Task Force"[09] in ersten Zügen operationalisiert wird.

Auch dieses in seiner Breite und Tiefe im EU-Kontext bisher einmalige, auf bestehende Instrumente und Strategien der Union verweisende Dokument zum Thema hybride Bedrohungen verzichtet auf eine verbindliche und damit allzu enge Definition. Es skizziert stattdessen deren konstitutive Elemente explizit unterhalb der „Schwelle eines offiziell erklärten Kriegs" – zum Beispiel „die Ausnutzung von Verwundbarkeiten der Zielgemeinschaft und (…) Verschleierungsstrategien zur Behinderung von Entscheidungsprozessen. Großangelegte Desinformationskampagnen und die Nutzung der sozialen Medien zur Beherrschung des politischen Diskurses oder zur Radikalisierung, Rekrutierung und Steuerung von Stellvertreterakteuren (‚proxy actors') können als Vehikel für hybride Bedrohungen dienen. Soweit die Abwehr hybrider Bedrohungen die nationale Sicherheit und Verteidigung und die Aufrechterhaltung von Recht und Ordnung betrifft, liegt die Hauptverantwortung bei den Mitgliedstaaten, da die meisten nationalen Verwundbarkeiten länderspezifischer Natur sind. Allerdings sehen sich viele EU-Mitgliedstaaten gemeinsamen Bedrohungen ausgesetzt, die sich auch gegen länderübergreifende Netze oder Infrastrukturen richten können."[10]

06 Bundesministerium des Innern, Konzeption Zivile Verteidigung (KZV), Berlin 2016, S. 15.

07 Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE (Einsatzmöglichkeiten von Militär und Geheimdiensten gegen sogenannte hybride Bedrohungen), 1.6.2016, BT-Drs. 18/8631, S. 3.

08 Die East StratCom Task Force gehört zur Abteilung für Strategische Kommunikation im Europäischen Auswärtigen Dienst (EEAS) und wurde von der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik nach EU-Ratsbeschluss vom März 2015 eingesetzt, um insbesondere russischen Desinformationskampagnen zu begegnen.

09 Im Unterschied zur East StratCom Task Force verfügt die Arab StratCom Task Force über keinen permanenten Stab dezidierter Regionalexperten, sondern setzt auf die interinstitutionelle Kooperation zwischen dem EEAS, der EU-Kommission und dem Koordinator für die Terrorismusbekämpfung im Rat der EU. Ihre Aufgabe ist es, im arabischen Raum positive Nachrichten über das Engagement der EU in der Region zu lancieren.

10 Europäische Kommission/Hohe Vertreterin der Union für Außen- und Sicherheitspolitik, Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen. Eine Antwort der Europäischen Union, Brüssel 2016, S. 2.

Bemerkenswert ist hier die Anerkennung der „länderspezifischen Natur" hybrider Angriffe bei einer gleichzeitig insgesamt generischen, länderübergreifenden Bedrohungslage. Trotz ähnlichen methodischen Vorgehens können sich die Ziele hybrider Einflussnahme stark voneinander unterscheiden und verweisen auf eine hohe Komplexität und Adaptivität der Komposition und Orchestrierung entsprechender Operationen. Die daraus abgeleitete Notwendigkeit umfassenderer analytischer Fähigkeiten[11] findet ihre erste konkrete Entsprechung in der mittlerweile erfolgten Einrichtung einer im Rahmendokument geforderten „EU Hybrid Fusion Cell" innerhalb des zivilen EU Intelligence Analysis Center (INTCEN),[12] das im Europäischen Auswärtigen Dienst angesiedelt ist. Deutschland engagiert sich hier nachdrücklich und stellt den Behördenleiter sowie sekundierte Fachexperten. Ebenso wie INTCEN betreibt die Fusion Cell keine eigenständige Beschaffung, sondern wertet die freiwillig bereitgestellten Erkenntnisse und Meldungen der beteiligten nationalen Nachrichtendienste aus und liefert den einschlägigen Bedarfs- und Entscheidungsträgern in der EU Lagebeurteilungen. Während sich die Zelle noch im personellen Aufwuchs befindet, ist eine analytische Anfangsbefähigung hergestellt, die sich prioritär mit hybriden Bedrohungen in der östlichen und südlichen Peripherie der EU sowie im Cyberraum auseinandersetzt.

Darüber hinaus wird die Einrichtung eines multinationalen, interdisziplinären „Kompetenzzentrums zur Abwehr hybrider Bedrohungen" angeregt, das sich – ähnlich der auch in der NATO bewährten Zentren – der Erforschung des Themas und der Entwicklung von Konzepten und Handlungsempfehlungen widmen soll. Für die Analyse hybrider Bedrohungen sind hier vor allem das NATO Strategic Communications Centre of Excellence in Riga, das NATO Cooperative Cyber Defence Centre of Excellence in Tallinn oder das NATO Energy Security Centre of Excellence in Vilnius zu nennen. Deutschland nimmt in diesen und weiteren Zentren die Möglichkeit zur aktiven Mitgestaltung sicherheitspolitisch und strategisch wichtiger Handlungsfelder durch die Gestellung von Personal und Zuwendungen wahr.

ROLLE DER NATO

Angesichts der gemeinsamen euroatlantischen Bedrohungswahrnehmung entlang der östlichen und südlichen Bündnisgrenzen erweisen sich hybride Bedrohungen mit der ihnen eigenen Dynamik und Vielgestalt gleichsam als geeigneter Katalysator einer stärkeren und komplementären Zusammenarbeit von EU und NATO.[13] Sowohl für die Bündnisse selbst als auch für ihre jeweiligen Mitgliedsstaaten, in denen die Hauptverantwortung zur Abwehr hybrider Bedrohungen verbleibt, ergibt sich daraus ein hoher Bedarf an Koordinierung und Kooperation. In ihrer gemeinsamen Erklärung anlässlich des Warschauer NATO-Gipfels am 8. Juli 2016 bezeichneten der Präsident des Europäischen Rates Donald Tusk, EU-Kommissionspräsident Jean-Claude Juncker sowie NATO-Generalsekretär Jens Stoltenberg die hybride Herausforderung denn auch als einen Schwerpunkt der gemeinsamen Anstrengungen. Es bestehe eine „dringende Notwendigkeit", hybriden Bedrohungen wirkungsvoll entgegenzutreten, namentlich durch die Stärkung von Resilienz, Aufklärung und Informationsaustausch, strategischer Kommunikation und gemeinsamen Übungen. Diese Empfehlungen decken sich freilich mit wesentlichen im Gemeinsamen Rahmen der EU vorgeschlagenen Maßnahmen und finden sich auch im Weißbuch wieder.

Die Handlungsstränge, die in der „Strategy on NATO's Role in Countering Hybrid Warfare" vom Dezember 2015 und im dazugehörigen Implementierungsplan, der im Februar 2016 vom Nordatlantikrat beschlossen wurde, angelegt wurden, konkretisieren Resilienz im Sinne der Sicherstellung und Aufrechterhaltung grundlegender Staats-, Regierungs-, Versorgungs- und Kommunikationsfunktionen im Ernstfall, das heißt sobald sich hybride (und selbstverständlich auch anders gelagerte) Bedrohungen materialisieren. Wie im Weißbuch und in der „Konzeption Zivile Verteidigung" angeklungen, erweist sich dabei die Feststellung des Bündnisfalls nach Artikel 5 des NATO-Vertrages als besonders diffizil,[14] insoweit die Schwelle eines bewaffneten Angriffes womöglich nicht durch einen einzelnen hybriden Angriff überschritten wird, sehr wohl aber in der Gesamtschau aller zusammengehöriger Operationen.

11 Vgl. Weißbuch (Anm. 3), S. 38.

12 Die Funktionen des militärischen Nachrichtenwesens sind wiederum im Intelligence Directorate des EU-Militärstabs abgebildet.

13 Vgl. Gemeinsamer Rahmen (Anm. 10), S. 3.

14 Vgl. Weißbuch (Anm. 3), S. 65.

Im Falle eines Überschreitens der Schwelle bleibt wiederum jedwedes Verteidigungshandeln an die üblichen Kategorien wie Legalität, Notwendigkeit und Verhältnismäßigkeit gebunden. Es ist herrschende Meinung, dass das in Artikel 51 der UN-Charta verbriefte und als Völkergewohnheitsrecht anerkannte Recht auf Selbstverteidigung nicht auf eine *reaction in kind* beschränkt ist. Das heißt, dass etwa Cyberangriffe, sobald sie in ihren Auswirkungen einem konventionellen Angriff gleichkommen, beispielsweise durch die Zerstörung eines Kraftwerks, und damit die Schwelle eines bewaffneten Angriffes überschreiten, sehr wohl auch mit anderen, gegebenenfalls kinetischen Mitteln beantwortet werden können.

Diese Auffassung folgt nicht zuletzt einer Logik der Abschreckung, die die „Kosten" eines Angriffes erhöhen und den „Nutzen" für den Angreifer vermindern soll. Auch der Abschreckung gegen hybride Bedrohungen wohnt eine gewollte Ambiguität inne, insofern sie keine Automatismen vorzeichnet, sondern lageabhängig und gestaffelt auf verschiedene Instrumente zurückgreifen kann. Die Unklarheit über die zu erwartende Reaktion erschwert die Kalkulation eines Angreifers, wobei das Ausbleiben einer angemessenen Reaktion Anreize für weitere Aggression stiften kann. Umgekehrt kann eine unangemessene Reaktion zur Eskalation beitragen (*from bits to bullets*) und damit den Konflikt verschärfen anstatt ihn einzuhegen.

Davon unbenommen bleibt die für hybride Bedrohungen typische Attributionsproblematik, also die gezielte Verschleierung der Urheberschaft eines Angriffs, die die Mechanismen der Verteidigung nicht grundsätzlich unmöglich macht, aber doch stark verzögern und dadurch schwächen kann. Die erschwerte Freund-Feind-Erkennung kommt insbesondere auch im Cyberraum zum Tragen, wo die gezielte Irreführung hinsichtlich der eigenen Identität (*false flag*) begünstigt wird.

INFORMATIONSRAUM ALS MASSGEBLICHE DIMENSION

Durch die anhaltende Weiterentwicklung und steigende Verfügbarkeit von Informations- und Kommunikationstechnologien bietet der Cyberraum nicht nur einen möglichen Hebel für konventionell unterlegene Akteure, sondern bietet zugleich ein ideales Vehikel für die effiziente Verbreitung von Botschaften an ein großes Publikum.

Nun gehören Meinungspluralismus und Pressefreiheit zum unveräußerlichen Wertekanon, ja zu den Garanten freiheitlich demokratischer Ordnungen schlechthin. Zugleich ist eine offene Gesellschaft grundsätzlich in hohem Maße verwundbar, insofern sämtliche „Bereiche gesellschaftlichen Lebens (…) zum Ziel hybrider Angriffe" werden können.[15] Im Bereich der Einflussoperationen wird die daraus erwachsende Herausforderung offenkundig, nämlich in Form der „Nutzung der digitalen Kommunikation zur Beeinflussung der öffentlichen Meinung – angefangen mit der unerkannten, gezielten Steuerung von Diskussionen in sozialen Netzwerken bis hin zur Manipulation von Informationen auf Nachrichtenportalen. Bereits jetzt kommt diesem Vorgehen als Element hybrider Kriegführung zentrale Bedeutung zu."[16]

Im Informationsraum erreicht die hybride Methode ihr in letzter Konsequenz politisches Ziel nicht unmittelbar durch Handlungen, sondern durch die Provokation von Reaktionen auf Handlungen, was als „reflexive Kontrolle"[17] und „Perzeptionsmanagement" gefasst wird. Im Informationsraum überholt die Bedeutung der Wahrnehmung vielfach jene der Wahrheit, der Wettstreit um Deutungshoheit mittels „Narrativen" ist permanent. Die informationelle Bedrohung, die in ihren möglichen psychologischen Auswirkungen auf eine Zielbevölkerung nicht hoch genug eingeschätzt werden kann, tritt also neben die materielle Dimension. Dabei ist die menschliche Dimension ungleich schwieriger zu schützen.

Wenn es zutrifft – und manches spricht dafür –, dass die „größte Verwundbarkeit westlicher Gesellschaften (…) eher im psychischen als im physischen Bereich" liegt,[18] so erfordert Resilienz präventiv und reaktiv nicht zuletzt eine der Gesellschaft innewohnende psychologische Wehrhaftigkeit und Selbstbehauptung. Im Gegensatz zu kinetischen Operationen, die vor allem auf physische Wirkung ausgerichtet sind, aber sehr wohl auch *force multiplier* der informationellen Einflussnahme sein können, zielen Einflussoperationen auf die Einstellungen, Überzeugungen und das Verhalten von Menschen. Dabei erweist

15 Ebd., S. 39.
16 Ebd., S. 37.
17 Timothy Thomas, Russia's Reflexive Control Theory and the Military, in: Journal of Slavic Military Studies 17/2004, S. 237–256.
18 Herfried Münkler, Kriegssplitter. Die Evolution der Gewalt im 20. und 21. Jahrhundert, Berlin 2015, S. 247.

sich vor allem eine Einwirkung – auch kurzfristig – auf das Verhalten von Individuen und sozialen Gruppen als „attraktive“ Option für einen Angreifer, beispielsweise in Form der Mobilisierung von Auslandsbürgern oder ethnischen oder sprachlichen Diasporagemeinschaften.

Auch Einwirkungsversuche auf die öffentliche Meinung insgesamt oder das Verhalten herausgestellter Individuen sind kein Novum. War bereits im Kalten Krieg die „Feder“ ein ebenso gewichtiges – wenn nicht wichtigeres – Mittel der Konfliktaustragung wie das „Schwert“, setzten sich Versuche des *social engineering* über den Irak-Krieg (*hearts and minds*), die israelisch-palästinensischen Auseinandersetzungen, über Afghanistan bis hin zu den Gräueln des sogenannten Islamischen Staates fort. Aber die Geschichte „aktiver Maßnahmen“ ist nicht selten auch eine des Scheiterns. So war zwar die Betroffenheit der Bundesregierung im „Fall Lisa“ im Januar 2016 klar gegeben, aber schließlich entglitt selbst dem russischen Außenminister Sergej Lawrow der Anspruch auf Deutungshoheit, und Russland nahm politischen Schaden.[19] Nichtsdestotrotz ist der Bundesregierung bewusst, „dass Propaganda- und Desinformationsmaßnahmen durch (massen)psychologische Beeinflussung destabilisierend wirken können“.[20]

Im Gegensatz zu Verhaltensmodifikationen sind die Möglichkeiten zur Manipulation von Einstellungen bestenfalls langfristig fruchtbar, weshalb die überwiegende Zahl hybrider Einflussoperationen nicht auf Überzeugung abzielt, sondern auf Überredung. Sie säen Zweifel, Zwietracht, Unsicherheit und Relativierung, indem sie sich von jedweder Beweisführung ihrer Behauptungen lossagen und den Verteidiger mit immer neuen, mitunter außerordentlich kreativen Angriffen, etwa durch die Professionalisierung des Einsatzes von „Trollen“ und digitalen Provokateuren,[21] in die Enge treiben.[22]

19 Lawrow hatte behauptet, deutsche Behörden würden die Entführung eines russlanddeutschen Mädchens durch Flüchtlinge vertuschen. Die Nachricht über den „Fall“, der vor allem in russischen Medien skandalisiert worden war und zu Demonstrationen von Russlanddeutschen vor dem Kanzleramt geführt hatte, stellte sich bald als falsch heraus.

20 Antwort der Bundesregierung (Anm. 7), S. 5.

21 Vgl. NATO Strategic Communication Center of Excellence, Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia, Riga 2016.

22 Vgl. Christopher Paul/Miriam Matthews, The Russian „Firehose of Falsehood“ Propaganda Model: Why It Might Work and Options to Counter It, Santa Monica 2016.

SICHERHEIT VERNETZEN

Sicherheitsarchitekturen sind Ausdruck normativer Prinzipien einer Wertegemeinschaft, die sich nicht nur über ihre zu schützenden Güter und Interessen verständigt, sondern auch darüber, zu welchen Instrumenten und Methoden sie zu deren Schutz greift – und zu welchen nicht. Im Wettstreit der Wertevorstellungen und Weltanschauungen liegt eine gewichtige Ursache für die Rivalitäten in den internationalen Beziehungen. Durch Projektionen von Feindschaft stiftet ein Aggressor Identität und Zusammenhalt in den eigenen Reihen, seine hybriden Aktivitäten haben demnach einen abgestimmten Außen- und Innenbezug. Da heutzutage „zwischenstaatliche Kriege [jedoch] mehr kosten, als sie im günstigsten Fall einbringen können“,[23] folgt die hybride Art der Konfliktaustragung auch einem ökonomischen und nicht nur einem ideologischen Kalkül.

Die hybride Methode löst die Dichotomie von Krieg und Frieden zugunsten eines Kontinuums zwischen beiden Zuständen auf. Hybrides Vorgehen ist eine Fortsetzung der Politik mit anderen, jeweils zeitgemäßen Mitteln und damit selbst eine Form der Politik. Die Versuche hybrider Akteure, die Entscheidungs- und Handlungsfähigkeit von Staaten zu beeinträchtigen, sind in der Gesamtschau weder friedlich noch ein Akt des Krieges. Sie fallen damit, weil sie Staat und Gesellschaft als Ganzes betreffen, aus sicherheits- und verteidigungspolitischer Sicht zwischen gültige Zuständigkeiten und Ressortgrenzen. Die Analyse und Abwehr hybrider Bedrohungen kann aus diesem Grund nur ressortübergreifend, gesamtstaatlich, international vernetzt und gemeinschaftlich gelingen.

Der Beitrag spiegelt ausschließlich die persönliche Meinung der Autoren wider.

FLORIAN SCHAURER
ist promovierter Politikwissenschaftler und Referent in der Abteilung Politik des Bundesministeriums der Verteidigung.

HANS-JOACHIM RUFF-STAHL
ist promovierter Medienwissenschaftler und als Oberstleutnant Referent in der Abteilung Politik des Bundesministeriums der Verteidigung.

23 Münkler (Anm. 18), S. 213.

SICHERHEIT IM CYBERSPACE

Marcel Dickow · Nawid Bashir

Im Sommer 2016 veröffentlichte eine Hackergruppe, die sich „The Shadow Brokers" nennt, Teile des Werkzeugkastens der sogenannten Equation Group, einer offensiven Cybereinheit, die dem US-Auslandsgeheimdienst NSA nahestehen soll. Unter den offengelegten Instrumenten befanden sich unter anderem Schadcode und Programme zum Ausnutzen von Sicherheitslücken, sogenannte Exploits.[01] Der Fall war nicht nur eine Blamage für die Equation Group, sondern verdeutlichte erneut, dass das Internet mittlerweile zu einem sicherheitspolitischen Raum geworden ist, in dem die klassischen, staatlichen Verfahren allein nicht mehr ausreichen, um für Sicherheit zu sorgen. Außerdem zeigte er klar, dass Sicherheitslücken in Software selbst für diejenigen gefährlich sind, die sie üblicherweise nutzen.

Im Folgenden sollen – mit Blick auf die sicherheitspolitischen Herausforderungen – die Besonderheiten des Cyberspace analysiert und eingeordnet werden. Wir werfen dabei einen Blick auf Paradigmen und Paradoxien dieses vom Menschen geschaffenen Raums und beleuchten drei nationale Strategien (USA, Deutschland, Russland) für die Herstellung von Cybersicherheit. Weil im Datenraum einzelstaatliches Handeln allein noch keine Lösungen für sicherheitspolitische Probleme erlaubt, weiten wir im Anschluss den Fokus auf internationale Kooperation und nehmen dabei den sogenannten Cyberterrorismus in den Blick. All dies soll unter der Fragestellung geschehen, ob den konzeptionellen Besonderheiten des Raums politisch ausreichend Rechnung getragen wird.

DER CYBERRAUM WAR NIEMALS SICHER

Der Shadow-Brokers-Fall steht an der Spitze einer Entwicklung von digitaler Aufrüstung und Versicherheitlichung des Cyberraumes. Dieser wird zunehmend als Herausforderung für die nationale Sicherheit erachtet. Bislang haben 72 Staaten Cybersicherheitstrategien formuliert;[02] hinzu kommen Vereinbarungen in und zwischen supranationalen beziehungsweise intergouvernementalen Organisationen wie EU und NATO.[03] Dass der Cyberraum für Angriffe genutzt werden kann, ist keine Neuigkeit. Lange Zeit war der sicherheitspolitische Fokus allerdings auf kriminelle Akteure gerichtet. Bereits 1989 kursierte die erste Erpresser-Software „AIDS", die über 5,25-Zoll-Disketten weltweit Computer infizierte. Auf den Rechnern der Betroffenen führte sie zur Verschlüsselung zahlreicher Daten, die nur gegen eine Lösegeldzahlung wieder freigegeben wurden.[04] Über staatliche Interessenverfolgung per Cyberangriff war indes wenig bekannt. Hier wurde erst 2007 ein Präzedenzfall geschaffen: Damals legten DDoS-Attacken mutmaßlich russischer Hackergruppen etliche Regierungs-, Banken- und Nachrichtenseiten Estlands lahm, nachdem ein sowjetisches Kriegerdenkmal aus der Hauptstadt Tallinn verlegt werden sollte.[05]

Den ersten und bisher einzig bekannten militärischen Cyberangriff auf einen anderen Staat begingen die USA und Israel 2011 mit dem Trojaner „Stuxnet" auf das iranische Atomprogramm. Dabei wurden mehrere Zentrifugen zur Anreicherung von Uran zerstört.[06] Erstmalig wurde ein Cyberangriff genutzt, um Schäden physischer Infrastrukturen herbeizuführen. In nationalen Verteidigungs- und Cyberstrategien ist Stuxnet seither ein häufig zitierter Präzedenzfall. Viele Staaten versuchen deshalb, möglichst große Kontrolle über das Internet oder wenigstens über ihre nationale Internetinfrastruktur zu erlangen. So ist auch das sogenannte HACIENDA-Programm des britischen Nachrichtendienstes GCHQ zu verstehen, das 2014 durch den ehemaligen NSA-Mitarbeiter Edward Snowden aufgedeckt wurde. Es soll den Cyberraum und verwundbare Infrastrukturen kartografieren.[07] Andere Staaten verfolgen wohl ähnliche Absichten.

SPEZIELLE HERAUSFORDERUNGEN

Die konzeptionellen Besonderheiten des Cyberspace sind inzwischen vielfach dokumentiert. Kein Raum bietet bessere Möglichkeiten, die

Spuren eigener Aktivitäten zu verwischen, falsche Fährten zu legen und die Rückverfolgbarkeit von Angriffen zu verhindern. Im globalen Netz werden zwangsläufig Dritte, insbesondere ihre IT-Infrastruktur, in den Konflikt hineingezogen. Ihrer durch das Völkerrecht auferlegten Sorgfaltspflicht können Staaten nur bedingt nachkommen, wollen sie nicht die Freiheit und Offenheit des Internets durch vollständiges Überwachen gefährden. Die Attribution von Aktivitäten, insbesondere von aggressiven, bleibt schwierig, wenn nicht unmöglich. Die dafür antretende Computerforensik sammelt nachträglich meist Indizien, keine Beweise. Viele technische Merkmale, die oftmals als politische Beweiskette für oder gegen Aktivitäten bestimmter Staaten ins Feld geführt werden, halten einer konsistenten juristischen Beweisführung nicht stand. Ob Zeitstempel und sprachspezifische Kommentare in Quellcodes, spezielle Codefragmente, Routinen oder Programmiertechniken: All das ist fälschbar, und kaum etwas lässt sich so leicht verbreiten wie Software(schad)code und die dafür nötigen Sicherheitslücken.

Gleichzeitig sind die meisten Staaten abhängig von kommerzieller Hard- und Software und damit auch von deren Sicherheit. Nationale technologische Souveränität in der IT ist schon deshalb eine Illusion, weil die Produktions- und Lieferketten globalisiert sind. Wirtschaftlich würde eine nationale, souveräne IT für die meisten Staaten auch keinen Sinn ergeben, weil die heimischen Märkte zu klein für die nötigen Investitionen in Forschung, Entwicklung und Produktion sind.

Schon diese wenigen Beispiele zeigen, dass klassische Paradigmen der Sicherheitspolitik nicht ohne Weiteres auf den Cyberspace übertragbar sind. Abschreckung kann nur funktionieren, wenn der Angreifer glaubhaft mit Vergeltung rechnen muss, doch das Attributionsproblem untergräbt diese Logik. Der Staat als Garant für Sicherheit im Cyberspace ist oft selbst abhängig von kommerziellen Unternehmen und tritt zudem nicht selten janusköpfig auf, etwa wenn staatliche Stellen Sicherheitslücken aufkaufen, um sie später gezielt einzusetzen, sei es zur Strafverfolgung und polizeilichen Prävention oder nachrichtendienstlich beziehungsweise militärisch. Zudem verwischt die Trennung zwischen Zivilem und Militärischem: Akteure beider Bereiche verwenden gleiche oder ähnliche IT-Infrastruktur, beide stehen in ähnlichen Abhängigkeiten zu kommerziellen Softwareanbietern. Selbst staatliche Hacker und Cyberkriminelle unterscheiden sich kaum in den eingesetzten technischen Mitteln.

Schließlich versagt das Rechtsprinzip der Territorialität insbesondere für digitale Daten, wenn sie losgelöst von ihren realen Ursprüngen global verarbeitet und gespeichert werden. Die neueste Fassung der US-amerikanischen Cyberstrategie spricht deshalb von einem gemeinsam geteilten Raum (*shared space*).[08] Weil internationale Rechtsetzung in der Regel fehlt, kommt es zu Kollisionen unterschiedlicher nationaler Regulierungen. Dies ist nicht neu. Neu ist, dass die Daten im Datenraum delokalisiert verarbeitet und gespeichert werden. Der Cyberspace ist kein homogener, klar begrenzter Rechtsraum wie die internationale See, sondern ein durch die Anwendung von technischen Protokollen aufgespannter, virtueller Datenraum. All dies spricht dagegen, den Cyberspace als einen traditionellen, sicherheitspolitischen Raum aufzufassen; stattdessen gilt es, die Gültigkeit bestimmter Konzepte wie zum Beispiel Abschreckung, Verteidigung und Rüstungskontrolle neu zu bestimmen.

Die Gefahr von Cyberangriffen geht von unterschiedlichsten Akteuren aus. Einzeltäter tummeln sich hier genauso wie professionell organsierte Hackergruppen, kriminelle Banden ebenso wie militärische und nachrichtendienstliche Hackerkommandos. Cybersicherheitsexperten gehen davon aus, dass die Gefahr von Angriffen

01 Vgl. Patrick Beuth, NSA: Unbekannte versteigern angebliche Waffen von Elitehackern, 16.8.2016, www.zeit.de/digital/internet/2016-08/nsa-shadow-brokers-hack-equation-group.

02 Vgl. ITU, National Strategies Repository, www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

03 Vgl. NATO, Cyber Defence Pledge, 8.7.2016, www.nato.int/cps/en/natohq/official_texts_133177.htm.

04 Vgl. Hauke Gierow, Der Virus des wunderlichen Dr. Popp, 7.7.2016, www.golem.de/news/die-erste-ransomware-der-virus-des-wunderlichen-dr-popp-1607-121809.html.

05 DDoS steht kurz für „Distributed Denial of Service": Durch eine Vielzahl von gleichzeitigen Angriffen auf ein Computersystem wird dieses zeitweilig durch Überlastung zum Erliegen gebracht. Vgl. Florian Rötzer, DDoS-Angriffe auf estnische Server waren kein „Cyberwar", 12.6.2007, www.heise.de/-138918.html.

06 Vgl. David E. Sanger, Obama Ordered Wave of Cyberattacks Against Iran, 1.6.2012, www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

07 Vgl. Julian Kirsch et al., NSA/GCHQ. Das HACIENDA-Programm Zur Kolonisierung des Internet, 15.8.2014, www.heise.de/-2292574.html.

08 Vgl. The White House, U.S. Government, National Security Strategy, Washington D.C. 2015, www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

nicht ab-, sondern weiter zunimmt.[09] Als größte Gefahrenquelle gelten professionelle und staatliche Hackerteams, die (Industrie-)Spionage betreiben oder kritische Infrastrukturen angreifen.

Die US-Sicherheitssoftwarefirma Symantec entdeckte 2015 mehr als 430 Millionen neue Varianten von Schadsoftware, was einer Zunahme von 36 Prozent gegenüber dem Vorjahr entspricht. Mehr als verdoppelt habe sich die Ausnutzung von sogenannten Zero-Day-Schwachstellen.[10] Sobald diese Schwachstellen öffentlich werden, bleibt den Entwicklern kaum Zeit, diese durch ein Sicherheitsupdate zu korrigieren, bevor Kriminelle sie ausnutzen. Entdeckte und weiterverkaufte Schwachstellen werden bevorzugt von staatlichen Akteuren für Überwachungsmaßnahmen und Angriffe benutzt. Auch Stuxnet bediente sich mehrerer solcher Zero-Day-Sicherheitslücken.[11] Der Handel mit diesen Schwachstellen befeuert ein Geschäftsmodell sogenannter Sicherheitsfirmen, an dessen Austrocknung Regierungen im Sinne der staatlichen Sicherheitsvorsorge eigentlich größtes Interesse haben müssten. Dass Sicherheitsorgane diese Lücken im Namen der Sicherheit aufkaufen und dann nicht an die Hersteller melden (um sie später selbst für Angriffe zu verwenden), gehört zu den Paradoxien der Cybersicherheit.

Ein weiteres Paradoxon des Cyberspace entsteht durch die Verwischung der Unterschiede zwischen Offensive und Defensive, also das Ausnutzen von offensiven Fähigkeiten für defensive Zwecke. Insbesondere für militärische und nachrichtendienstliche Akteure gilt mittlerweile die Devise, dass das Eindringen in fremde Computersysteme und die Analyse ihrer Schwachstellen noch keinen Angriff im klassischen Sinne darstellt. Wenn aber alle die Systeme der jeweils anderen infiltriert haben, wer ist dann Angreifer und wer Verteidiger? Die politischen und technischen Hemmschwellen in diesem „Spiel" sind jedenfalls deutlich gesunken. Der Cyberangriff auf den Deutschen Bundestag im Sommer 2015 verdeutlicht den Trend und zeigt die Verwundbarkeit wichtiger staatlicher Infrastrukturen.

09 Vgl. Accenture/HfS Research, The State of Cybersecurity and Digital Trust 2016, 2016, S. 3 ff., www.accenture.com/us-en/insight-cybersecurity-digital-trust-2016.

10 Vgl. Symantec, Internet Security Threat Report 2016, Mountain View 2016, S. 5.

11 Vgl. Kim Zetter, Countdown to Zero Day. Stuxnet and the Launch of the World's First Digital Weapon, New York 2015, S. 88 ff.

NEUE RÄUME – ALTE KONZEPTE?

Mittlerweile haben viele Staaten mit Cybersicherheitsstrategien auf die Herausforderungen im Datenraum reagiert, darunter die USA, Russland und Deutschland. Die Bedrohungswahrnehmungen und Herangehensweisen unterscheiden sich zum Teil beträchtlich.

Der Direktor der US-Geheimdienste definiert die Gefahren aus dem Cyberraum inzwischen als größte Herausforderung, sogar noch vor dem Terrorismus. Als mögliche Ziele von Attacken werden in der **Cybersicherheitsstrategie des US-Verteidigungsministeriums** kritische Infrastrukturen und militärische Netzwerke ausgemacht. Potenzielle Gegner werden vor allem in Russland und China gesehen, die über fortgeschrittene Cyberfähigkeiten verfügen und diese auch einsetzen. Auch Iran und Nordkorea sind auf der Liste der vermuteten Gegner, wenngleich sie über weniger ausgeprägte Fähigkeiten verfügen. Der sogenannte Islamische Staat (IS) wird ebenfalls als Gefahr genannt, da er den Cyberraum nutzt, um zu rekrutieren und Propaganda zu verbreiten. Zudem haben IS-Vertreter die Absicht erklärt, aggressive Cyberfähigkeiten erlangen zu wollen. Auch der Handel mit Software-Sicherheitslücken wird vom US-Verteidigungsministerium als Gefahr erkannt. Allerdings wird der Einfluss der staatlichen Aktivitäten auf diesen Markt nicht erwähnt und somit nicht als Gefahrenquelle benannt. Eine Stoßrichtung der amerikanischen Cybersicherheitsstrategie ist die Einbettung von Cyberfähigkeiten in konventionelle Angriffe, um beispielsweise militärische Netzwerke und Waffensysteme des Gegners zu stören oder auszuschalten. Hierzu sollen die bereits vorhandenen offensiven Fähigkeiten ausgebaut werden.[12]

Wie in anderen sicherheitspolitischen Räumen setzt die US-Regierung auch im Cyberraum auf Abschreckung: „The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law."[13] Völkerrechtlich ist jedoch strittig, ob und in welchem Maße auf einen Cyberangriff mit kinetischen (also physischen) Angriffen reagiert werden darf. Die

12 Vgl. U.S. Department of Defense, The Department of Defense Cyber Security Strategy, Washington D.C. 2015, S. 9, S. 14.

13 Ebd., S. 10.

Erfolgsaussichten der Abschreckungspolitik im Cyberraum sind zudem unklar, da diese voraussetzt, dass ein Angreifer sicher identifiziert wird. Dass die Attributionsproblematik eine glaubwürdige Abschreckungspolitik untergräbt, räumt die US-Regierung ein: Um die Anonymität von Angriffen zu reduzieren, soll die Netzüberwachung gestärkt und vor allem die Zusammenarbeit der US-Sicherheitsbehörden ausgebaut werden.

In der **Cybersicherheitsstrategie der Bundesregierung von 2011** werden dagegen die zivilen Ansätze und Maßnahmen in den Vordergrund gestellt. Die Bundeswehr soll lediglich Maßnahmen zum Schutz ihrer eigenen Handlungsfähigkeit ergreifen und auf entsprechenden Mandaten basierend zur „gesamtstaatlichen Sicherheitsvorsorge" beitragen.[14] Eine Veränderung dieses Ansatzes ist im aktuellen sicherheitspolitischen **Weißbuch der Bundesregierung** erkennbar. Hier wird der Cyberspace als einer den anderen Dimensionen (Land, Luft, Wasser, Weltraum) vergleichbarer Raum beschrieben, den es national und international zu schützen gilt. Hierzu sollen die Cyberkompetenzen sowohl im Bundesministerium für Verteidigung als auch in der Bundeswehr gebündelt werden.[15]

Die Aufgaben der Bundeswehr im Cyberbereich werden im Weißbuch als „Verteidigungsaspekte der gesamtstaatlichen Cybersicherheit, Beiträge zum gesamtstaatlichen Lagebild im Cyber- und Informationsraum im Rahmen der nationalen und multinationalen Sicherheitsvorsorge sowie der Gewährleistung der Cybersicherheit in den bundeswehreigenen Netzen" beschrieben.[16] Unklar bleibt, wie die Sicherheitsvorsorge im Cyberspace allein im nationalen Kontext umsetzbar ist, kennen die Datenflüsse doch keine Staatsgrenzen. So heißt es im Weißbuch denn auch folgerichtig: „Innere und äußere Sicherheit fallen in wenigen Bereichen so eng zusammen wie im Cyberraum. Die Bedrohungslage im Cyberraum erfordert eine ganzheitliche Betrachtung im Rahmen der Cybersicherheitspolitik."[17] Die Bundesregierung hat sich dabei darauf verständigt, die verschiedenen Aufgaben zwischen den Ministerien aufzuteilen. Während das Bundesministerium des Innern (BMI) für die aktuell in Bearbeitung stehende Cybersicherheitsstrategie federführend verantwortlich ist, übernimmt die Bundeswehr Verteidigungsaspekte der gesamtstaatlichen Cybersicherheitsstrategie. Ergänzend ist das Auswärtige Amt für die internationale Cybersicherheitspolitik zuständig.

Allerdings wird im Weißbuch die unscharfe Trennung von offensiven und defensiven Fähigkeiten nicht problematisiert. Beide sollen ausgebaut, geübt und weiterentwickelt werden. Im Gegensatz zur fortschreitenden Versicherheitlichung und Militarisierung des Cyberraumes steht das Eintreten der Bundesregierung für internationale Abkommen, Rüstungskontrolle und vertrauensbildende Maßnahmen: „Die Anpassung des Instrumentariums der Rüstungskontrolle und Vertrauensbildung an veränderte sicherheitspolitische und technologische Rahmenbedingungen schließt klassische und neue Dimensionen von Sicherheit, wie den Cyber- und Informationsraum und Weltraum sowie die Implikationen neuartiger Waffensysteme, ein."[18]

Russlands nationale Cybersicherheitsstrategie von 2013 kontrastiert den westlichen Ansatz durch einen Fokus auf territoriale Integrität und nationale Souveränität im Datenraum. Dafür soll ein internationales Kontroll- und Regulierungsregime auf Basis einer von Russland verfassten Konvention für internationale Informationssicherheit geschaffen werden. Dies spiegelt die staatszentrierte Position Russlands im Cyberbereich wider. Im Gegensatz zu den USA, Deutschland und der EU befürwortet Russland eine größtmögliche Kontrolle des Staates über die physischen Netzinfrastrukturen sowie über die Datenverarbeitung und Dateninhalte bis hin zur Regulierung des Internets auf globaler Ebene. Als größte Bedrohung aus dem Cyberraum sieht Russland die Nutzung von Cyberwaffen für militärische und politische Ziele (siehe Stuxnet). Weitere Bedrohungen aus Sicht der russischen Regierung sind terroristische Angriffe auf kritische Infrastrukturen und die Nutzung des Internets durch Extremisten für Propaganda- und Rekrutierungszwecke. Zudem wird die Einmischung in innere Angelegenheiten und die Aufwiegelung von innerrussischen Konflikten befürchtet.[19]

Die drei Beispiele nationaler Cybersicherheitsstrategien zeigen, dass Antworten auf die

14 Vgl. Bundesministerium des Innern (BMI), Cyber-Sicherheitsstrategie für Deutschland, Berlin 2011, S. 5.

15 Vgl. Bundesregierung, Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr, Berlin 2016.

16 Ebd., S. 93.

17 Ebd., S. 38.

18 Ebd., S. 82.

19 Vgl. Russian Federation, Basic Principles for State Policy of the Russian Federation in the Field of International Information Security, Moskau 2013, S. 2 f.

dringendsten konzeptionellen Fragen des Cyberspace noch fehlen. Bemerkenswert ist die weitgehende Abwesenheit von Ideen und Initiativen für Regeln und gutes Verhalten der Staaten im Netz. Eine Weiterentwicklung des klassischen Konzepts der Rüstungskontrolle auf den Cyberspace ist momentan nicht erkennbar. Die Begrenzung schädlicher Aktivitäten oder von Rüstungsdynamiken im Cyberspace liegt zurzeit, so scheint es, nicht im Interesse der Großmächte. Gleichwohl bleibt Cybersicherheit für die Interpretation und Anwendung des Völkerrechts eine Herausforderung.

CYBERSICHERHEIT ALS INTERNATIONALE HERAUSFORDERUNG

Völkerrechtliche Prinzipien wie Territorialität, staatliche Souveränität, Interventions- und Gewaltverbot sind für den Cyberraum nicht aufgehoben. Die internationale Gemeinschaft scheint sich derzeit jedoch kaum darauf einigen zu können, wie diese Prinzipien aus der analogen Welt auf den digitalen Raum übertragen werden sollen. Das Territorialprinzip, das jedem Staat auf seinem Territorium Souveränität zugesteht, stößt im Cyberspace an die Grenzen der Anwendbarkeit. Da die Aufdeckung und Zurechnung von Cyberangriffen kaum möglich ist, kann aktuell nur selten zweifelsfrei nachgewiesen werden, ob ein Verstoß gegen das Interventionsverbot vorliegt. Sollte ein Staat jedoch nachgewiesenermaßen Hackergruppen mit einer solchen Absicht finanziell unterstützen, so wäre der Tatbestand der Intervention erfüllt.[20] Unter das Verbot fallen auch das Streuen falscher Informationen und die Aufwiegelung zu politischen Unruhen. Vor allem Russland reklamiert für sich ein besonderes Schutzbedürfnis vor solchen ausländischen Eingriffen aus dem Cyberraum.

Cyberattacken können von E-Mail-Hacks bis hin zur Manipulation von Steuerungssystemen kritischer Infrastrukturen mit verheerenden und tödlichen Folgen reichen. Sollte im letzteren Fall die Attacke von einem Staat ausgehen, so läge nach Artikel 2 Absatz 4 der UN-Charta ein Verstoß gegen das Gewaltverbot vor.[21] Die Tatbestandslage bei Cyberattacken ist oft unklar, denn die Auswirkungen einer Attacke aus dem Cyberraum sind selten unmittelbar zu beobachten und erschweren damit die Definition der Gewaltschwelle. Das unverbindliche Tallinn-Manual, in dem versucht wird, Kriegführung im Cyberraum international zu verrechtlichen, beschreibt einen bewaffneten Angriff aus dem Cyberraum als „cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[22]

Völkerrechtlich unklar ist bisher auch, wie die Antwort auf eine solche Cyberattacke ausfallen darf. Die USA behalten sich Vergeltungsschläge auch mit konventionellen Gegenschlägen vor.[23] Die Mehrheit der internationalen Gemeinschaft sieht das Recht auf Selbstverteidigung durch einen militärischen Angriff erst dann gerechtfertigt, wenn der erlittene Angriff über eine gewisse Schwelle physischer Gewalt hinausgeht.[24] Völlig ausgenommen von solchen völkerrechtlichen Regelungen ist der Tatbestand der Spionage. Die flächendeckende und anlasslose Überwachung des Cyberraums kann zwar Menschenrechte wie das Recht auf Privatsphäre und die Pressefreiheit verletzen, ist aber gängige (und international ungeregelte) Praxis vieler Staaten.

CYBERTERRORISMUS

Wo das Völkerrecht in schwieriges Fahrwasser gerät, da sind nichtstaatlichen Akteuren Tür und Tor geöffnet, so möchte man denken. Tatsächlich sind einige Herausforderungen für Cybersicherheit asymmetrischer Natur, allerdings spielt dabei der sogenannte Cyberterrorismus nur eine untergeordnete Rolle. Das BMI definiert Cyberterrorismus als „eine Form von Terrorismus, bei der das Internet als Waffe genutzt wird. Es werden also mit Hilfe von Internet-Technologien Angriffe auf Computersysteme verübt."[25] Cyberterrorismus kann ein Angriff auf kritische Infrastrukturen wie die Elektrizitäts- und Trinkwasserversorgung, Staudämme, Bahnverkehr, Verkehrsleitsysteme oder die Flugsicherung sein. Jedes dieser Ziele birgt potenziell hohe Opferzahlen und ist da-

20 Vgl. Christian Schaller, Internationale Sicherheit und Völkerrecht im Cyberspace, Stiftung Wissenschaft und Politik, SWP-Studie 18/2014, S. 15.

21 Vgl. Nils Melzer, Cyberwarfare and International Law, United Nations Institute for Disarmament Research, Genf 2011, http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

22 Michael N. Schmitt (Hrsg.), Tallinn Manual on the International Law Applicable to Cyber Warfare, New York 2013, S. 106.

23 Vgl. U.S. Department of Defense (Anm. 12), S. 10.

24 Vgl. Yoram Dinstein, War, Aggression and Self-Defence, Cambridge 2011, S. 207 ff.

25 BMI, Cyberterrorismus, www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyberterrorismus/cybersterrorismus_node.html.

her für Terroristen besonders attraktiv. Allerdings schätzt das BMI die Gefahr durch Cyberterrorismus als gering ein: „Grundsätzlich ist von einer Gefährdung durch Cyberterrorismus auszugehen. Es sind aber bislang keine Hinweise auf konkrete Anschlagsplanungen bekannt. Mit Ausnahme von Staatsterrorismus ist es unwahrscheinlich, dass derzeit überhaupt die technischen Fähigkeiten vorhanden sind, um eine Cyber-Attacke diesen Ausmaßes durchzuführen."[26]

Derzeit werden bei keiner Terrororganisation die erforderlichen hohen technischen Fähigkeiten vermutet. Es besteht jedoch die Gefahr, dass eine fertige „Cyberwaffe", also schon entwickelte oder gar benutzte Schadsoftware, weitergegeben und von Kriminellen oder Terroristen verwendet wird. Bislang sind nur niedrigschwellige Angriffe ohne schwerwiegende Folgen bekannt, zum Beispiel die kurzzeitige Übernahme der Social-Media-Accounts des US-Zentralkommandos durch den IS beziehungsweise die Hackergruppe „Cyber-Kalifat" im Januar 2015.[27]

Terrorismus im Cyberraum manifestiert sich aktuell vielmehr durch die Verbreitung von Propaganda und durch die Möglichkeit der Online-Radikalisierung. Gleichwohl nutzen terroristische Gruppen gesicherte Kommunikationswege im Internet für die Planung von Anschlägen oder zur Steuerung von Terrorzellen. Auch diese Aktivitäten stellen für Staaten ein Sicherheitsrisiko dar und werfen die Frage auf, wie viel Freiheit und Privatheit im Netz der Sicherheit geopfert werden sollen. Durch Verschlüsselung gesicherte Kommunikation ist eben nur dann wirklich geschützt, wenn weder staatliche Sicherheitsbehörden noch andere Dritte mitlesen können. Absichtlich geschwächte Verschlüsselung, Hintertüren oder Generalschlüssel gefährden, so zeigen die Erfahrungen der vergangenen Jahre, die Sicherheit aller.

Wie in zwischenstaatlichen Beziehungen, stellt sich auch beim Cyberterrorismus die Frage nach der Gewaltschwelle von Cyberangriffen. So ist fraglich, ob das bloße Hacken von Social-Media-Accounts und das Stören von Sendebetrieben ohne personellen oder sachlichen Schaden Terrorismus ist. Bisher wurden jedenfalls noch keine großangelegten Angriffe aus dem Cyberraum verzeichnet, die massiven physischen Schaden angerichtet haben und einen terroristischen Hintergrund vermuten ließen.

SCHLUSS

Mit dem Cyberspace hat sich der Mensch erstmals einen (virtuellen) Raum selbst geschaffen und nutzt ihn nun für seine Auseinandersetzungen. Das Fehlen von Regelsetzungen und die schwierige Übertragbarkeit des bestehenden Völkerrechts hat dabei ein „Spielfeld" entstehen lassen, das längst überwunden geglaubtem, aggressivem Staatenverhalten zu einer Renaissance verholfen hat. Während dieser „Wilde Westen" immer mehr Akteure anzieht, ringen die Regierungen mit den Konsequenzen für den Kernbereich ihrer staatlichen Souveränität. Die Sicherheit im Cyberspace ist ein fundamentales Interesse staatlicher Vorsorge, die klassischen Durchsetzungsmechanismen aus der realen Welt versagen jedoch weitgehend.

Der Politik, auch in Deutschland, bleibt wohl nichts anderes übrig, als die Paradigmen des Cyberspace zur Grundlage einer neuen Sicherheitsarchitektur zu machen, die sehr viel mehr als bisher Verhaltensregeln und Vertrauensbildung betont und der Selbstbeschränkung bedarf (etwa durch nationale Moratorien, keine offensiven Cyberwaffen gegen zivile Infrastruktur einzusetzen). Im Zentrum neuer internationaler Vereinbarungen sollte die Frage stehen, wie die Staaten mit immer neu aufklaffenden Sicherheitslücken in Hard- und Software umgehen. Diese Risiken zu minimieren, könnte das einende Interesse aller Akteure bilden.

MARCEL DICKOW
ist promovierter Physiker und Master of Peace and Security Studies. Er leitet die Forschungsgruppe Sicherheitspolitik der Stiftung Wissenschaft und Politik (SWP) in Berlin.
marcel.dickow@swp-berlin.org

NAWID BASHIR
ist Politikwissenschaftler mit Fokus auf die Querschnittsthemen Digital- und Sicherheitspolitik.
n.bashir@zeppelin-university.net

26 Ebd.

27 Vgl. Spencer Ackerman, US Central Command Twitter Account Hacked to Read „I Love You Isis", 12.1.2015, www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack.

EUROPÄISCHE SICHERHEITSKOOPERATION

Bestandsaufnahme und Handlungsfelder

Thomas Jäger

Kurz vor dem Beginn des neuen Jahrtausends hielten Sicherheitsexperten weltweit die Luft an, ob die Umstellung auf die 2000er Jahre in den Rechenzentren reibungslos vonstattengehen würde. Über Monate waren die schlimmsten Szenarien des Datenverlustes durchgespielt worden. Doch es kam anders. Der Übergang in der virtuellen Welt funktionierte, in der realen aber schlugen Flugzeuge in New York und Washington D. C. ein und veränderten die globale Sicherheitslage von einem Moment auf den anderen.

Terrorismus, Proliferation und fragile Staaten, verbunden mit regionalen Konflikten, die ordnungspolitisch zehn Jahre lang missachtet worden waren, formten seither die sicherheitspolitischen Prioritäten. Die Sicherheitsstrategie der USA konzentrierte sich ebenso wie diejenige der Europäischen Union auf diese Herausforderungen.[01] Jede für sich war schon eine enorme sicherheitspolitische Aufgabe. Angesichts der grundlegenden Prozesse der Globalisierung und Transnationalisierung, in denen die Welt immer enger zusammenwuchs und mehr und unterschiedlichere Akteure international handlungsfähig wurden, verzahnten sie sich nun zudem miteinander. Zerfallende Staaten boten und bieten Gewaltakteuren Territorien, von denen aus sie mittels Strukturen Organisierter Kriminalität auf ganz unterschiedlichen Handlungsfeldern, insbesondere dem Drogen-, Menschen- und Waffenhandel, Profite erzielen können, die wiederum dazu dienen, politische Macht durch verschiedene Gewaltformen zu erlangen, unter anderem durch den in andere Staaten exportierten Terrorismus. Es reichte nicht mehr, Sicherheitsgefahr für Sicherheitsgefahr einzeln zu bearbeiten. Wie Zahnräder griffen sie ineinander und formten ein komplexes Gebilde aus Handlungen, Ursachen und Wirkungen. Darauf mussten die Staaten reagieren.

Der Einsatz traditioneller Sicherheitsinstrumente, insbesondere des Militärs, erwies sich als wenig zielführend. Die Kooptierung von Eliten in prekären Staaten gestaltete sich schwieriger, das eigene Militär konnte in den differenzierten Kampfformen die trainierten Fähigkeiten nicht erfolgreich einsetzen. Kombiniert wurden sie mehr oder weniger erfolgreich mit Formen der bürokratischen Beratung, politischen Reformierung und institutionellen Kooperation zwischen den Staaten, die ordnungspolitische Zwecke verfolgten, und denjenigen, die in ihrer Stabilisierung und Entwicklung unterstützt werden mussten. Den verzahnten Gefahren ließ sich nur durch eine sicherheitspolitische Neukonzeption entgegentreten.

VERNETZTE SICHERHEIT

Begleitet wurde diese Einsicht von der Ausarbeitung des Konzepts der Vernetzten Sicherheit. Aus dem militärischen Denken stammend, bezog es zunehmend auch die übrigen zivilen Sicherheitsorgane ein. Da fiel ein Stein ins Wasser und zog immer weitere Kreise: Zunächst ging es darum, die Interoperabilität der Teilstreitkräfte zu gewährleisten, denn im festgefahrenen Ost-West-Konflikt hatte die nukleare Abschreckung überdeckt, dass sowohl das Heer als auch die Marine und die Luftwaffe vieler Staaten nicht effizient kooperieren konnten. Dies betraf insbesondere auch das US-Militär, weshalb es kein Zufall ist, dass sich das Konzept der Vernetzten Sicherheit von den USA aus verbreitete.

Der zweite Kreis fand zwei Ausprägungen. Zum einen kann Vernetzte Sicherheit sinnvoll nur multinational geplant, geübt und umgesetzt werden: Die Fähigkeit, zusammen agieren zu können, betrifft zwangsläufig auch die Streitkräfte anderer Staaten. Zum anderen stellten sich nach dem

Ende des Ost-West-Konflikts auf einmal ganz andere Aufgaben. Mit vielen waren die Streitkräfte schlicht überfordert. Deshalb mussten sie mit Nichtregierungsorganisationen auf ganz verschiedenen Gebieten – von der Entwicklungszusammenarbeit bis zur Konfliktmediation, von der Bildungsarbeit bis zum Migrationsmanagement – zusammenarbeiten.

Vernetzte Sicherheit als strategisches Konzept[02] verband multilateral ganz unterschiedliche Fähigkeiten staatlicher und privater Akteure, internationaler Organisationen und transnationaler Player. Konzeptionell waren die Regierungen damit komplex und umfassend aufgestellt, um Sicherheitsgefahren zu begegnen. Nur in der Praxis klemmte das Konzept an allen möglichen Stellen. Verschiedene Akteure wollten nicht miteinander kooperieren, ihr Wissen nicht miteinander teilen. So verfolgten sie in der Umsetzung der gemeinsam beschlossenen Ziele zum Teil unterschiedliche Interessen und scheiterten daran, ihr taktisches und operatives Vorgehen den veränderten Lagen anzupassen.

INFORMATIONSMANAGEMENT

Gemeinsames Handeln war aber notwendig, und das setzte gemeinsames Wissen voraus. In der internationalen Politik ist Wissen jedoch häufig unsicher. Wer über welche Ressourcen verfügt und mit welchen Motiven handelt, wird von Regierungen meist unterschiedlich bewertet. Deshalb ist das Informationsmanagement, um zu gemeinsamem Wissen zu gelangen, ein Kernbereich der Sicherheitskooperation. Informationen sind allerdings etwas anderes als Wissen. Insbesondere Informationen aus den Bereichen des staatlichen und gesellschaftlichen Lebens, die geheim gehalten werden sollen, müssen erst hinsichtlich ihrer Umstände, Motive und Wirkungen interpretiert werden. Es ist das tägliche Geschäft von Geheimdiensten und Polizei, Informationen über Dritte zu sammeln und zu analysieren und gleichzeitig geheim zu halten, woher sie was auf welchem Wege erfahren haben. Deshalb gilt meistens die Regel des *need to know*. Es werden nur diejenigen Informationen weitergegeben, die unbedingt nötig sind und nur an diejenigen Akteure, die es unbedingt wissen müssen. Wissen ist Macht, und Informationen sind die Währung auf diesem Gebiet.[03]

Dabei ist allen Beteiligten klar, dass ein deutlicheres Bild der Gefahren entsteht, wenn alle relevanten Informationen zusammengetragen werden. Doch funktionierte dies, wie die Anschläge vom 11. September 2001 zeigten, nicht einmal innerhalb derselben Dienste oder zwischen den Organen eines Staates. Die US-Behörden hatten über die Attentäter ausreichende Informationen, aber sie wussten nichts von deren Vorhaben. Sie hatten die Informationen nicht zusammengetragen. Was aber innerhalb eines Dienstes schon schwierig ist, ist zwischen verschiedenen Staaten fast unmöglich. Sensible Informationen zu teilen, setzt höchstes Vertrauen voraus. Denn mit jedem Hinweis verrät der hinweisgebende Dienst, was er weiß. Und das sollte eigentlich kein anderer Dienst wissen.

Indem das Prinzip des *need to know* nach 9/11 zumindest durch das Prinzip des *need to share* ergänzt wurde – viele Akteure sollen Zugriff auf möglichst viele Informationen haben und diese in Datenbanken miteinander verknüpfen können – wurden neue Kooperationsformate ins Leben gerufen und alte Formate mit geänderten Aufgaben konfrontiert. Informiert euch gegenseitig!, hieß die Devise, die sehr bald jedoch ihre Kehrseite zeigte. Indem mehr und mehr Daten miteinander verknüpft wurden, konnten Zusammenhänge der Informationsbeschaffung sichtbar werden, die zuvor verdeckt waren. Seitdem der ehemalige NSA-Mitarbeiter Edward Snowden mit Millionen von Dateien über Hongkong nach Russland flüchtete, hat das Prinzip des *need to know* wieder größere Relevanz erhalten. Doch ändert das nichts an der richtigen Einsicht: In einer Welt, in der sich terroristische Gewalttäter und Akteure der Organisierten Kriminalität, Menschen-, Waffen- und Drogenhändler vernetzen, müssen sich auch Sicherheitsorgane dieser Aufgabe stellen. Abschottung und Eigenbrötlerei führen dazu, Sicherheitsgefahren nicht effektiv entgegentreten zu können.

01 Vgl. Thomas Jäger/Alexander Höse/Kai Oppermann (Hrsg.), Die Sicherheitsstrategien Europas und der USA, Baden-Baden 2005.

02 Vgl. Heiko Borchert/Ralph Thiele (Hrsg.), Vernetzte Sicherheit. Eine konstruktive Zwischenbilanz, Wiesbaden 2012.

03 Vgl. William M. Nolte, Intelligence Analysis in an Uncertain Environment, in: Loch K. Johnson (Hrsg.), The Oxford Handbook of National Security Analysis, Oxford 2010, S. 404–421. Zur Geheimdienstkooperation siehe auch den Beitrag von Christopher Nehring in dieser Ausgabe (*Anm. d. Red.*).

SICHERHEITSKOOPERATION IN EUROPA

Sicherheit für die eigene Bevölkerung zu garantieren, gilt als erste und besonders wichtige Aufgabe von Staaten. Diese bezog sich lange Zeit insbesondere auf die nationale Sicherheit, die Sicherung von Grenzen und Territorium vor Angriffen von außen. Mit der Erweiterung der Sicherheitsaufgaben[04] zersplitterte diese Bestimmung. Sicherheit wurde nicht mehr zuerst als territoriale Sicherheit wahrgenommen und bewertet, sondern als soziale, ökonomische, ökologische und kulturelle Sicherheit, als Sicherheit der Energieversorgung sowie als Sicherheit vor den Folgen von Klimawandel und Pandemien. Allein auf nationaler Ebene war da nichts mehr zu bewegen. Des einen Sicherheit war nicht mehr des anderen Unsicherheit. Entweder waren alle (oder zumindest die Mehrzahl einer Region) sicher oder keiner. Die Ebola-Epidemie ab 2014, um ein Beispiel zu nennen, war zwar territorial zu verorten, aber die Vernetzung der Welt ließ sie zu einem globalen Problem werden, weshalb sich auch die noch nicht betroffenen Staaten um Einhegung und Bekämpfung bemühten.

Gemeinsame Sicherheit, ein Begriff, mit dem einst die paradoxen Folgen der gegenseitigen nuklearen Abschreckung beschrieben wurden, hatte sich über alle Bereiche des gesellschaftlichen Lebens gelegt. Sicherheit wurde wichtiger, weil sie umfassender definiert wurde; sie wurde komplexer, weil sie in dynamischer Vernetzung betrachtet wurde; und sie wurde konkreter, weil die Bearbeitung institutionalisiert werden musste. Es reichte nicht mehr aus, Kooperation locker zu verabreden, sie musste bürokratisch aufgesetzt werden. Das gilt auch für die Sicherheitsgewährleistung innerhalb der EU. Nun sind die dafür zuständigen Innenminister nicht die Speerspitze der Integrationsbemühungen. Sie wachen eifersüchtig über ihre jeweiligen Fähigkeiten und Kompetenzen. Dadurch wurde die Aufgabe der Sicherheitskooperation in der EU noch herausfordernder.

Bewältigt ist die Aufgabe noch nicht. Doch vieles ist angestoßen, manches zumindest auf den Weg gebracht worden und in einigen Bereichen gibt es Erfolge zu verzeichnen. Um die vorstehenden Punkte zusammenzufassen:

1. Für europäische Sicherheitskooperation reicht es nicht aus, sich auf einzelne Handlungsfelder zu beschränken, da diese ineinandergreifen. Sie müssen in ihrer Komplexität erfasst und bearbeitet werden.

2. Dabei kommt dem gemeinsamen Wissen um Gefahren und Wege, ihnen zu begegnen, eine besondere Bedeutung zu. Informationsmanagement ist für Sicherheitsorgane allerdings ein äußerst sensibler Punkt.

3. Handlungsansätze sollen vernetzt ausgebildet werden, sowohl was die eigenen Sicherheitsorgane angeht, aber auch darüber hinaus mit Nichtregierungsorganisationen und anderen Staaten. Das erfordert Koordinierung.

Der Ruf nach mehr Kooperation auf dem Gebiet der Sicherheit erschallt in der EU immer dann besonders laut, wenn die Prävention versagt hat und eine Gefahr nicht abgewendet werden konnte. Die 2015/16 verübten Anschläge in Paris und Brüssel, die Furcht vor der Ausbreitung des Ebolafiebers, die Folgen des Staatszerfalls in Libyen, aber auch generell die Furcht vor der Vielfalt terroristischer Handlungsmöglichkeiten, gerade auch in Verbindung mit Organisierter Kriminalität, Menschen-, Drogen- und Waffenhandel, werden geradezu ritualisiert mit der Forderung nach mehr Sicherheitskooperation beantwortet. Diese herzustellen, ist schwierig, institutionell jedoch bereits angelegt, wie ein Blick auf einige Kooperationsforen zeigt. Die Sicherheitskooperation in der EU und darüber hinaus mit anderen Staaten hat sich dabei besonders wegen der wahrgenommenen Terrorgefahr entwickelt, auch wenn innere Sicherheit weiterhin im Kompetenzbereich der Mitgliedsstaaten verbleibt.

Im Mittelpunkt der europäischen Sicherheitskooperation stehen der Austausch von Informationen sowie die Bereitstellung von Kooperationsforen, um die Zusammenarbeit zwischen den Staaten zu erleichtern. Im Folgenden werden zuerst einige europäische Informationsplattformen vorgestellt, im zweiten Schritt verschiedene Koordinierungsstellen; sodann wird kurz auf die internationale Dimension eingegangen.

04 Vgl. Thomas Jäger (Hrsg.), Handbuch Sicherheitsgefahren, Wiesbaden 2015.

INFORMATION UND WISSEN

EU Intelligence Analysis Centre

Das EU Intelligence Analysis Centre (EU INTCEN) hat sich für die Bewältigung seiner Aufgaben im Laufe der vergangenen Jahre immer weiter entwickelt. Es ging aus dem Joint Situation Centre (SitCen) hervor, das als semi-geheimdienstliches Organ eingerichtet worden war. Zuerst war diese Behörde beim Generalsekretariat des Rates angesiedelt, seit 2009 ist sie dem Hohen Repräsentanten der EU für Außen- und Sicherheitspolitik zugeordnet. Seit März 2012 trägt es den Namen EU INTCEN und ist eine Institution des Europäischen Auswärtigen Dienstes, aus dessen Budget es auch bezahlt wird. Damit ist es weiter in die Struktur der EU eingegliedert worden.

Seine Aufgaben sind die eines nachrichtendienstlichen Knotenpunktes. Das INTCEN verfügt nicht über eigene Aufklärungskapazitäten, sondern erhält seine Informationen von den Diensten der Mitgliedsstaaten, den rund 140 EU-Delegationen (EU-Auslandsvertretungen) sowie aus weiteren EU-Institutionen, unter anderem den EU-Beobachtermissionen (EUMM), dem Intelligence Directorate des EU-Militärstabs und dem Satellitenzentrum der EU (EUSC). Die derart zusammengetragenen Informationen und Analysen werden sodann verarbeitet, um die Organe der EU mit Analysen zu versorgen und einen gemeinsamen Wissenstand herzustellen. Dies geschieht in unterschiedlichen Formaten, die einerseits auf akutes Krisenmanagement gerichtet sind, andererseits durch langfristig angelegte Analysen und Strategiepapiere auch die Angleichung der politischen Einschätzungen über gemeinsames Wissen anstreben. Bedrohungsanalysen fokussieren unterschiedliche Sicherheitsgefahren. Dabei geht es auch um die frühe Identifizierung von und Warnung vor Krisen sowie die möglichen Folgen für EU-Mitarbeiter. Seine Auswertungen und Analysen stellt das INTCEN dem Hohen Vertreter für Außen- und Sicherheitspolitik, dem EU-Militärstab, dem EU-Militärkomitee, der Strategie- und Frühwarneinheit des Hohen Repräsentanten und der Generaldirektion für Außenbeziehungen zur Verfügung. Anders als frühere Kooperationsformen auf diesem Gebiet ist das Analysezentrum nicht mehr an das geheime Netzwerk der NATO angeschlossen. Denn einige EU-Mitgliedsstaaten gehören der NATO nicht an, zudem gibt es noch kein gemeinsames Klassifizierungsregelwerk.

Trägt das INTCEN zu einem gemeinsamen Wissensstand und damit zu einer Grundlage für koordiniertes Handeln der EU-Mitglieder gegenüber Sicherheitsgefahren bei? Auf der einen Seite spricht dafür, dass jährlich mehr als 200 strategische Lagebeurteilungen und mehr als 50 Sonderberichte ausgearbeitet werden. Hierüber wird eine gemeinsame Sicht auf die internationalen Beziehungen und die anstehenden Herausforderungen gefördert. Auf der anderen Seite ist das Analysezentrum darauf angewiesen, dass die Dienste der Mitgliedsstaaten Informationen liefern. Das führt in jedem einzelnen Fall zu zwei Fragen: Konnten die nationalen Dienste die Informationen gewinnen? Und sind sie bereit, diese zu teilen? Eine weitere Herausforderung besteht darin, den Informationsaustausch zwischen INTCEN und Eurojust, der Kooperationsplattform der Justizbehörden, sowie dem Europäischen Polizeiamt Europol zu gestalten, also den vernetzten Ansatz von Sicherheit in seiner zivil-militärischen Dimension abzubilden.

Europol

Das European Police Office (Europol) konnte nach einem für europäische Institutionen typischen längeren Anlauf 1999 seine Arbeit aufnehmen und wurde 2010 zu einer Agentur der EU. Europol ist kein europäisches FBI, sondern dient der Abstimmung, gegenseitigen Informierung und Unterstützung der Polizeien aus den EU-Mitgliedsländern. Die in Den Haag angesiedelte Agentur arbeitet als zentrale Kooperationsplattform der Polizeibehörden und verfügt in jedem Mitgliedsstaat über eine Zweigstelle. Sie besitzt keine umfassende Exekutivbefugnis, auch wenn ihr inzwischen einige operative Aufgaben zugewiesen wurden. Organisierte Kriminalität, Drogen- und Waffenhandel sowie Geldwäsche sind zentrale Arbeitsbereiche von Europol.

European Counter Terrorism Centre

Über das European Counter Terrorism Centre (ECTC), das Europol im Januar 2016 nach den Terrorerfahrungen der vergangenen Jahre gründete, sollen spezifische Fähigkeiten der Terrorismusbekämpfung institutionalisiert werden. Zentrale Aufgaben des ECTC sind der Informationsaustausch sowie die Koordinierung von präventiven und operativen Maßnahmen. Hierzu sind gemeinsame strategische Einschätzungen durch die Mitgliedsstaaten grundlegend. Im Einzelnen sind die Arbeitsaufträge auf ausländische Kämpfer terro-

ristischer Organisationen, die Finanzierung von Terrorgruppen, die Terrorpropaganda im Internet sowie den illegalen Waffenhandel fokussiert. Die Analysen des ECTC sollen laufende Europol-Ermittlungen unterstützen, zudem soll das ECTC den einzelnen Staaten im Falle von Terroranschlägen helfend zur Seite stehen.

Institutionell ist das ECTC in die bestehenden Strukturen von Europol eingebettet. Nach den Anschlägen von Paris 2015 wurden etwa die französischen und belgischen Behörden durch 60 Beamte von Europol unterstützt. Dabei stand der Informationsaustausch im Mittelpunkt. Das ECTC kann hierfür auf Informationssysteme zurückgreifen, die Europol mit den EU-Mitgliedsstaaten zur Bekämpfung von Drogenkriminalität, Geldwäsche und irregulärer Migration aufgebaut hat: das European Information System (EIS) und SIENA (Secure Information Exchange Network Application). In den Informationsaustausch sind auch die finanziellen Transaktionen in der EU integriert, die dort im Terrorist Finance Tracking Programme (TFTP) bearbeitet werden.

Das ECTC ist aus einem akuten Bedarf an gemeinsamem Informationsmanagement entstanden. Das könnte den nötigen Schwung geben, um den Informationsaustausch erfolgreich zu gestalten. Die Einbettung in etablierte Strukturen der Kriminalitätsbekämpfung kann sich als Effizienzvorteil erweisen. Allerdings hängt der Erfolg letztlich an der Kooperationsbereitschaft der Mitgliedsländer, nicht zuletzt auf dem Gebiet der justiziellen Zusammenarbeit. Für eine Bewertung der Arbeit ist es indes noch zu früh.

Schengener Informationssystem

Informationen werden zwischen den Sicherheitsorganen schon länger geteilt. Der Freizügigkeit innerhalb der Union entspricht (zumindest dem Anspruch nach) die Kontrolle an den EU-Außengrenzen. Mit dem Schengener Informationssystem (SIS)[05] sollen die Sicherheitsbehörden der EU-Mitgliedsstaaten sowie Europol und Eurojust Zugriff auf einheitliche und umfassende Daten haben. Gespeichert werden sowohl unerwünschte oder gesuchte Personen als auch Fahrzeuge und Banknoten, deren Umlauf überwacht werden soll. Zudem werden gestohlene Waffen und Ausweispapiere sowie Blanko-Dokumente erfasst. Das SIS besteht aus den nationalen Systemen in jedem EU-Land sowie einem zentralen System, das in Straßburg angesiedelt ist. Auf dieses Zentralsystem können die Sicherheitsbehörden aus den einzelnen Mitgliedsstaaten zugreifen. Der Aufbau einer neuen Version des SIS nach 2013 ermöglicht es auch, biometrische Daten zu speichern. Der Zugriff erfolgt über Knotenpunkte in den einzelnen Staaten, sogenannte SIRENE-Büros, in Deutschland über das Bundeskriminalamt in Wiesbaden.

KOORDINIERUNG

Ständiger Ausschuss COSI

Neben den Informationssystemen sind die Koordinierungsforen von besonderer Bedeutung für die Sicherheitskooperation in der EU. Der Ständige Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit (COSI) setzt sich aus hohen Beamten der Innen- oder Justizministerien der EU-Mitgliedsstaaten sowie aus Vertretern der Kommission und des Europäischen Auswärtigen Dienstes zusammen. Als Beobachter können auch Mitarbeiter von Europol, Eurojust oder der Grenzschutzagentur Frontex hinzugezogen werden. COSI soll zu einer wirksamen operativen Zusammenarbeit in Fragen der inneren Sicherheit beitragen, nicht zuletzt bei Strafverfolgungen und Grenzkontrollen. Die allgemeine Ausrichtung und die Wirksamkeit der operativen Zusammenarbeit werden hier gemeinsam beurteilt. COSI unterstützt den Rat auch bei der Reaktion auf Terroranschläge.

European Police Chiefs Task Force

Eine weitere Koordinationsplattform ist die European Police Chiefs Task Force (EPCTF). Es handelt sich dabei um ein zweimal jährlich tagendes, informelles Forum, das die Arbeit der nationalen Polizeien enger miteinander verbinden soll. Ziel der EPCTF ist, die institutionellen und persönlichen Beziehungen zwischen den nationalen Exekutivbehörden zu intensivieren, den Informationsaustausch zu fördern und sich gegenseitig – auch bei Maßnahmen gegen terroristische Gefahren – zu unterstützen. Gleichzeitig soll auf diese Weise die Verbindung zwischen Europol und den

05 Zum Schengener Informationssystem der zweiten Generation SIS II finden sich umfassende Informationen unter: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=URISERV%3Al14544.

nationalen und lokalen Polizeikräften verstärkt werden. Seit 2007 umfassen die Aufgaben auch operative Maßnahmen.

Der informelle Charakter wird insbesondere auch von der Europäischen Kommission kritisiert. Die EPCTF ist nicht rechtlich fundiert und keinem Parlament gegenüber verantwortlich. Die großen Unterschiede im institutionellen Aufbau der nationalen Polizeien wird als wichtiges Hindernis einer weiteren Koordination angesehen, ebenso der Umstand, dass in den Beratungen häufig nationale Themen die europäischen überlagern. Gleichwohl existiert das Forum bereits seit 1999, was als Ausweis dafür angesehen werden mag, dass es den Beteiligten (zumindest einigen) vorteilhaft erscheint.

Eurojust

Eurojust wurde 2002 als zentrale Kooperationsplattform der Justizbehörden gegründet,[06] um die Zusammenarbeit der nationalen Justizbehörden bei der Verfolgung schwerer grenzüberschreitender Kriminalität und Organisierter Kriminalität in der EU zu verbessern. Zu der in Den Haag angesiedelten Behörde entsendet jeder Mitgliedsstaat nationale Vertreter, die von 260 Mitarbeitern unterstützt werden. Auch Norwegen und die USA haben Verbindungsbeamte entsandt. Eurojust organisiert nach eigenen Angaben jährlich etwa 200 Koordinierungstreffen und bearbeitet rund 2000 Fälle. Die Schwerpunkte der Arbeit sind Terrorismus, Drogenhandel, Menschenhandel, Betrug, Korruption, Computerkriminalität, Geldwäsche sowie sonstige Aktivitäten des organisierten wirtschaftlichen Verbrechens. Dies sind die Handlungsfelder, die vom Rat der Europäischen Union als vorrangig eingestuft wurden. Eurojust hat keine Exekutivbefugnis, sondern dient ausschließlich als Plattform.

Koordinator für Terrorismusbekämpfung

Nach den Terroranschlägen in Madrid am 11. März 2004 setzte der Europäische Rat einen Koordinator für Terrorismusbekämpfung ein. Zum ersten Amtsinhaber wurde 2007 der belgische Jurist Gilles de Kerchove ernannt. Er soll dem Rat Politikempfehlungen geben und diejenigen Handlungsbereiche identifizieren, in denen vorrangig Antiterrormaßnahmen umgesetzt werden sollen. Hierbei stützt er sich auf die Bedrohungsanalysen der EU. Zudem soll er die Umsetzung beschlossener Maßnahmen überwachen und darüber hinaus überblicken, welche Instrumente der EU überhaupt zur Verfügung stehen, und sicherstellen, dass die EU in der Terrorismusbekämpfung aktiv bleibt. Schließlich gehört auch die Verbesserung der Kommunikation mit Drittstaaten zu seinen Aufgaben. So gehörte die internationale Zusammenarbeit in den vergangenen Jahren zu seinen Tätigkeitsschwerpunkten, der inhaltliche Fokus lag insbesondere auf ausländischen (also europäischen) Kämpfern in Syrien und sogenannten Rückkehrern.

Europäische Polizeiakademie

Die Europäische Polizeiakademie (EPA) ist ein Kooperationsnetz, das aus einzelstaatlichen Ausbildungseinrichtungen für hochrangige Führungskräfte der Polizeidienste besteht. Ihr Ziel ist die Entwicklung gemeinsamer Lösungen für die zentralen Probleme der Kriminalitätsbekämpfung und -verhütung. Ihr Hauptinstrument sind Schulungen für Polizeikräfte.

Police Working Group on Terrorism

Zweimal pro Jahr treffen sich zudem die 31 Mitgliedsstaaten der Police Working Group on Terrorism (PWGT), als Beobachter sind auch Mitarbeiter von Europol beteiligt. Die Gruppe ist ein permanentes und informelles Forum, das 1979 gegründet wurde und über keine zentrale Geschäftsführung verfügt. Seit 1999 sind die nationalen Behörden über ein vom Bundeskriminalamt eingerichtetes Informationssystem miteinander vernetzt. Das Handlungsfeld der Zusammenarbeit ist politisch motivierte Gewalt. Zu diesem Thema tauschen sich die beteiligten Behörden intensiv aus, informieren sich gegenseitig über relevante Fälle und gleichen Ermittlungsweisen bei terroristischen Herausforderungen und anderen gewalttätigen Handlungen miteinander ab. Die Bundesregierung bewertete die PWGT in einer Antwort auf eine Kleine Anfrage 2013 als „wichtiges Gremium zum fachlichen Austausch“ sowie als „bedeutende(s) Instrument der Terrorismusbekämpfung“ und bewährten „Kommunikationskanal“. Insbeson-

06 Ein Überblick über die Grundlagendokumente ist zu finden unter: www.eurojust.europa.eu/about/legal-framework/Pages/eurojust-legal-framework.aspx.

dere hob sie dabei auch die persönlichen Kontakte hervor, die auf den regelmäßigen Treffen geknüpft werden können.[07]

Radicalisation Awareness Network

Ein Schwerpunkt der Arbeit des Koordinators für Terrorismusbekämpfung sind Radikalisierungsprozesse. Das 2011 gegründete Radicalisation Awareness Network (RAN) ist ein Informationsnetzwerk der Europäischen Kommission, um diejenigen miteinander ins Gespräch zu bringen, die in der EU Deradikalisierungsarbeit und Resozialisiation von radikalisierten Menschen leisten. Polizei und Zivilgesellschaft arbeiten in diesem Netzwerk zusammen, das sich unter einer Steuerungsgruppe in neun Arbeitsgruppen gliedert, die sich unter anderem mit Fragen von Bildung, Gesundheit, Gefängnishaft und lokalen Strukturen befassen. Über 2000 Beteiligte haben sich im Rahmen von RAN bisher ausgetauscht. Die verlautbarten Reaktionen sind ausgesprochen positiv, wobei die Datenlage eine fundierte Einschätzung nicht begründen kann.

Militärstab der EU

Sofern militärische Fragen betroffen sind, wird der Militärstab der EU (EUMS) eingeschaltet. Dieser erarbeitet gemeinsame Lageeinschätzungen und befasst sich mit strategischer Planung, wofür er Konzepte entwickelt. Training, Ausbildung und die Betreuung der Partnerschaften gehören ebenso zu seinen Aufgaben.

Europäische Grenz- und Küstenwache

Nachdem der Rat die Europäische Agentur für die Grenz- und Küstenwache (die bestehende Agentur Frontex mit erweiterten Aufgaben) im September 2016 endgültig gebilligt hat, wird sie in den kommenden Monaten ihre Arbeit vollumfänglich aufnehmen. Der Druck der Herausforderungen an den Außengrenzen der EU hat dazu beigetragen, dass dieses Koordinierungsorgan nun mit neuen Zuständigkeiten ausgestattet wurde. Die Hauptaufgabe besteht in der Unterstützung eines integrierten Grenzmanagements der EU, das in der erforderlichen Weise (als korrespondierendes Element für die Freizügigkeit im Schengenraum) bisher nicht zustande kam und nun aufgebaut werden soll. Dazu arbeitet die Agentur mit den für das Grenzmanagement zuständigen nationalen Behörden zusammen. Ihre Aufgaben umfassen unter anderem gemeinsame Maßnahmen zur Verstärkung der Grenzkontrollen angesichts irregulärer Migration und grenzüberschreitender Kriminalität, die Unterstützung von Such- und Rettungsaktionen, die Organisation von Rückführungsmaßnahmen sowie die Förderung der operativen Zusammenarbeit zwischen EU-Ländern und Drittstaaten beim Grenzmanagement.[08] Hierfür sollen ein Soforteinsatzpool von 1500 Grenzschützern eingerichtet und Verbindungsbeamte in den Mitgliedsstaaten ernannt werden. Ob und wann die Agentur diese Aufgaben effektiv erfüllt, wird sich spätestens im Frühjahr 2017 erweisen, wenn ihr alle Kompetenzen zugewiesen worden sind.

INTERNATIONALE ZUSAMMENARBEIT

Entsprechend ihrer globalen Strategie[09] kooperiert die EU mit verschiedenen internationalen Organisationen, von denen einige hier nur illustrierend angeführt werden können. Im Rahmen der Zusammenarbeit in der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) spielen Konfliktprävention, Krisenmanagement und Postkonflikt-Unterstützung eine herausgehobene Rolle. Auch die Grenzüberwachung und das Training von Polizeieinheiten gehört zum Aufgabenspektrum. Mit der NATO, einzelnen wichtigen Staaten wie der Türkei und der Afrikanischen Union werden die für die Arbeit innerhalb der EU angesprochenen Handlungsfelder bi- und multilateral bearbeitet.[10]

Auf Nicht-EU-Ebene gibt es gleichfalls wichtige Kooperationsforen, etwa den Berner Club, der 1971 gegründet wurde und die meisten europäischen Geheimdienstchefs (beteiligt sind die

07 Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE (Europäische Zusammenarbeit in der Police Working Group on Terrorism), 10.5.2013, Bundestagsdrucksache 17/13440.

08 Eine erste Listung der Aufgaben findet sich unter www.consilium.europa.eu/de/press/press-releases/2016/09/14-european-border-coast-guard.

09 Vgl. Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy, Juni 2016, http://europa.eu/globalstrategy.

10 Die Breite an Herausforderungen durchmessen die Autoren in Sven Gareis/Gunther Hauser/Franz Kernic (Hrsg.), The European Union – A Global Actor?, Opladen u.a. 2013.

EU-Länder sowie Norwegen und die Schweiz) regelmäßig zusammenführt. Seit Beginn spielt auf Initiative Israels der Austausch terrorismusrelevanter Daten eine wichtige Rolle. Die vom Club 2001 initiierte Counter Terrorism Group (CTG) intensiviert diesen Austausch.

Weiterhin zu nennen ist die Europäische Gendarmerietruppe/European Gendarmerie Force (EGF/Eurogendfor), die Aufgaben in der Schnittmenge polizeilicher und militärischer Anforderungen wahrnimmt und sich aus den entsprechenden Polizeieinheiten von Frankreich, Italien, Spanien, Portugal, den Niederlanden und Rumänien zusammensetzt. Sie übernimmt zwar keine innereuropäischen Einsätze, war aber bereits in Bosnien, Haiti, Mali, Zentralafrika und Afghanistan im Einsatz. Litauen ist Partner, die Türkei hat einen Beobachterstatus.

FAZIT

Die Anfänge der verstärkten Sicherheitskooperation in der Europäischen Union reichen bis in die 1970er Jahre zurück; die zunehmende wirtschaftliche Integration erforderte schon nach kurzer Zeit auch engere Abstimmungen auf den Gebieten der Außen- und Sicherheitspolitik. Sie blieben aber stets und bis heute hinter dem Integrationsniveau anderer Politikfelder, der Handelspolitik etwa, zurück.

Nach den Terroranschlägen vom 11. September 2001 intensivierte sich die sicherheitspolitische Zusammenarbeit, insbesondere durch das auf andere Bereiche ausstrahlende Handlungsfeld der Terrorismusbekämpfung. Um zukünftige Anschläge zu verhindern, sollten die Informationen verschiedener Sicherheitsorgane und insbesondere auch der Finanzströme zusammengeführt werden. Rasch wurde evident, dass dieses Vorgehen national nur eine beschränkte Wirkung entfaltet und die grenzüberschreitende Kooperation effektiver sein könnte. Das galt auch für die verschiedenen Formen der grenzüberschreitenden Organisierten Kriminalität, die weiterhin als sicherheitspolitische Priorität in der EU angesehen werden.

Zwischen den EU-Mitgliedsstaaten wurden deshalb vor allem der Informationsaustausch und die Zugriffsmöglichkeiten auf gemeinsame Datenbanken ausgebaut und spezifische Formate der polizeilichen Koordination aufgebaut. Auf diesem Weg sollte ein Äquivalent für integrierte Strukturen geschaffen werden, die bisher nicht vereinbart werden konnten. Die intensiveren Kooperationen gingen aber nicht so weit, dass heute von integrierten Strukturen gesprochen werden kann, weil es deutliche Vorbehalte der einzelnen Staaten gibt.

Deshalb wurden parallel die Koordinierungsformationen verbreitert, um weitere Aufgaben erfüllen zu können. Man konnte unter anderem auf die jahrzehntelange Erfahrung aus dem Berner Club zurückgreifen. Die Sicherung der EU-Außengrenzen ist die jüngste dieser Maßnahmen, wird aber sicher nicht die letzte bleiben. Es ist ein stückweises Vorgehen, das einerseits versucht, gemeinsam Fähigkeiten zu bündeln und Asymmetrien auszugleichen, andererseits auch das Ziel verfolgt, im internationalen sicherheitspolitischen Austausch handlungsfähiger zu werden. Denn die EU sieht nie nur nach innen, sondern immer auch nach außen. Wie groß der Vorsprung anderer Mächte ist, ist in den vergangenen Jahren deutlich geworden. Im internationalen Vergleich mangelt es den EU-Mitgliedsstaaten an Abwehrfähigkeiten. Auch gemeinsam können sie diese derzeit noch nicht aufbringen.

Da es an weitergehendem Willen zur Integration der Fähigkeiten, häufig aber auch an diesen selbst mangelt, scheint die Vielzahl der Koordinierungs- und Informationsformate derzeit das politisch mögliche Maß an effektiver sicherheitspolitischer Koordinierung widerzuspiegeln. Das ist sicher nicht der effizienteste Weg, um Sicherheit zu gewährleisten, weshalb die Debatte über weitere Integrationsschritte auch auf diesem Gebiet weitergehen wird. Aber es ist eine souveränitätsschonende Kooperation, die angesichts der Sensibilität des Gegenstandes und der aktuell disparaten politischen Entwicklungen in den EU-Mitgliedsstaaten derzeit wohl die einzige mögliche Form der Zusammenarbeit ist.

THOMAS JÄGER
ist Professor für Politikwissenschaft, Inhaber des Lehrstuhls für internationale Politik und Außenpolitik an der Wirtschafts- und Sozialwissenschaftlichen Fakultät der Universität zu Köln und Herausgeber der Zeitschrift für Außen- und Sicherheitspolitik.
thomas.jaeger@uni-koeln.de

Politikfelder im Wettstreit?

INNERE SICHERHEIT, MIGRATION UND TERRORISMUS

Michaela Wendekamm

Die Themen innere Sicherheit, Migration und Terrorismus sind seit rund 15 Jahren im öffentlichen Diskurs konstant präsent. Nach den islamistisch motivierten Terroranschlägen in den USA am 11. September 2001 schien die Welt eine andere geworden zu sein. Nicht nur in Deutschland entfachten die Ereignisse eine Debatte über verschärfte Sicherheitsgesetze und ein restriktives Ausländerrecht. Die Anschläge in Madrid 2004 und in London 2005 befeuerten die Diskussion zusätzlich. Parallel dazu verstärkten sich ab 2006 Fluchtbewegungen aus dem arabischen Raum und Afrika. Der größte Teil der Flüchtlinge gelangte jedoch nicht nach Europa beziehungsweise wurde an dessen Außengrenzen gestoppt.

Darüber hinaus führte die Euro- und Finanzkrise zu einem Anstieg der EU-Binnenmigration, vor allem Deutschland wurde zu einem bevorzugten Zielland. Als sich zum Jahreswechsel 2013/14 die EU-Freizügigkeit auf Bulgarien und Rumänien ausweitete, kam in Teilen Europas die Sorge vor einem überproportionalen Zuzug aus diesen Ländern auf. Einige befürchteten einen verstärkten „Zustrom" osteuropäischer Arbeitskräfte, wobei häufig unterstellt wurde, dass das eigentliche Ziel der Migration der Erhalt von Sozialleistungen sei.

Seit einigen Jahren nehmen nun die Aktionen, die im Kontext des islamistischen Terrorismus stehen, wieder zu, und mit ihnen intensiviert sich die öffentliche Diskussion über Zuwanderung, Integration und deren sicherheitspolitische Implikationen erneut. In diesem Kontext können auch die Wahlerfolge der AfD in Mecklenburg-Vorpommern und anderen Bundesländern gesehen werden. Um aufzuzeigen, warum das Thema Migration in der öffentlichen Diskussion vielfach als bedrohlich wahrgenommen wird und inwiefern die innere Sicherheit mit der Migrationspolitik verzahnt ist, werde ich im Folgenden zunächst die Ausgangslage hinsichtlich der Zuwanderung nach Deutschland sowie zum Thema islamistischer Terrorismus beschreiben. Danach folgt eine Erläuterung der politischen Dimension von Sicherheit und Migration. Abschließend werde ich die Ereignisse des Spätsommers 2015 in den dargelegten Gesamtkontext einordnen.[01]

EINWANDERUNG

Kurz nach der deutschen Wiedervereinigung stieg die Zuwanderung in die Bundesrepublik auf einen historischen Höchststand. Die Ursachen für den Anstieg waren das Ende des Kalten Krieges, die Jugoslawienkriege sowie der zunehmend eskalierende Konflikt zwischen der Türkei und der kurdischen Untergrundorganisation PKK. Ab Mitte der 1990er Jahre nahmen die Zahlen der jährlich neu Eingewanderten jedoch stark ab und verblieben auf einem niedrigen Niveau.[02] Erst ab 2006 setzte wieder ein Trend deutlich steigender Zuwanderungszahlen ein. Mit über 1,2 Millionen Zuwanderern wurde 2013 der höchste Stand seit 20 Jahren erreicht. 2014 gab es einen weiteren Anstieg um 19 Prozent, und 2015 wanderten über 2,1 Millionen Menschen in die Bundesrepublik ein – so viele wie nie zuvor. Ungeachtet dessen, dass über die Hälfte der Einwanderer immer noch aus europäischen Ländern kommt – vorrangig aus Mittel- und Osteuropa sowie mit etwas Abstand aus Südeuropa, das stark von der Finanz- und Schuldenkrise betroffen ist – steigt seit einigen Jahren die Zuwanderung aus Afghanistan, Syrien und Irak erkennbar. Aufgrund des Bürgerkrieges in ihrer Heimat kamen 2014 fast drei Mal so viele Syrer nach Deutschland wie im Jahr zuvor; 2015 erhöhte sich die Quote nochmals um das 4,5-Fache.[03]

Diese Werte geben indessen keine Auskunft über die Länge des Aufenthalts der Zugewan-

derten. Die kommunalen Einwohnermeldeämter nehmen sowohl temporäre als auch dauerhafte Zuwanderungen auf. Allerdings melden sich Bürgerinnen und Bürger anderer EU-Staaten, die sich nur kurzfristig in Deutschland aufhalten, nicht immer bei den Behörden. Dieser blinde Fleck resultiert aus der innerhalb der EU geltenden Freizügigkeit. Jedoch wird davon ausgegangen, dass sich bei Aufenthalten von mehreren Monaten die europäischen Zuwanderer bei den entsprechenden Stellen melden. Für 2015 machte das Statistische Bundesamt zudem explizit darauf aufmerksam, dass zum einen nicht alle Schutzsuchenden registriert, zum anderen einige mehrfach erfasst wurden.[04]

ISLAMISTISCHER TERRORISMUS

Das Phänomen des islamistischen Terrorismus rückte spätestens durch die Ereignisse vom 11. September 2001 verstärkt in das Bewusstsein der westlichen Gesellschaften. Islamistische Selbstmordattentäter entführten vier Passagiermaschinen, um diese an neuralgischen Orten in den USA zum Absturz zu bringen. Zwei Flugzeuge flogen in die Türme des New Yorker World Trade Centers, das dritte stürzte in das US-Verteidigungsministerium in Arlington bei Washington D.C., das vierte zerschellte bei Pittsburgh, Pennsylvania, und erreichte sein unbekanntes Ziel nicht. Das für die Anschläge verantwortliche Netzwerk al-Qaida verübte in der Folge zahlreiche weitere Terrorakte auf der ganzen Welt.

Am 11. März 2004 erreichte der islamistische Terrorismus mit den Anschlägen auf mehrere Vorortzüge in Madrid europäischen Boden. Im Jahr darauf, am 7. Juli, wurden in London drei Bomben in U-Bahnen und eine weitere in einem Doppeldeckerbus gezündet. Der erste islamistisch motivierte Anschlag in Deutschland, der nicht verhindert werden konnte, geschah am 2. März 2011, als ein Einzeltäter am Frankfurter Flughafen zwei US-Soldaten erschoss.

In Europa ist in der jüngeren Vergangenheit vor allem Frankreich von Terrorakten betroffen: Die Anschläge auf die Redaktion der Satirezeitschrift „Charlie Hebdo“ am 7. Januar 2015, an mehreren Orten in Paris und Saint-Denis am 13. November 2015 sowie in Nizza am 14. Juli 2014 bilden eine traurige Reihe mit zahlreichen Todesopfern. Auch in der Türkei wurden zuletzt mehrere Selbstmordattentate verübt: am 20. Juli 2015 in Suruç, am 10. Oktober 2015 in Ankara, am 12. Januar 2016 in Istanbul und am 20. August 2016 in Gaziantep. Aber auch Dänemark, Belgien und Deutschland wurden zu Zielen von Anschlägen: In Kopenhagen wurden am 14. und 15. Februar 2015 ein Kulturzentrum und eine Synagoge attackiert, in Brüssel sprengten sich am 22. März 2016 am Flughafen und in der Innenstadt drei Terroristen in die Luft, und in Ansbach kam es am 24. Juli 2016 zu einem Selbstmordanschlag.

CHARAKTERISTIKA DER POLITIKFELDER INNERE SICHERHEIT UND MIGRATION

Die derzeitige Flüchtlingssituation in Europa ist eine Herausforderung für verschiedene Politikressorts geworden – vor dem Hintergrund der allgemeinen terroristischen Bedrohung besonders auch für die Sicherheitspolitik. In der öffentlichen Debatte werden vor allem das Verhältnis von Sicherheit und Freiheit sowie das von Exklusion und Integration neu ausgehandelt. Zum besseren Verständnis der angesprochenen Politikfelder sollen im Folgenden die innere Sicherheit und die Migrationspolitik näher betrachtet werden.

In der Gründungsphase der Bundesrepublik konnte von einem eigenständigen **Politikfeld innere Sicherheit** noch nicht die Rede sein. Erst mit den umstrittenen Notstandsgesetzen 1968 und deren Umsetzung änderte sich dies. Durch sie wurden die Aufgaben von Militär und Polizei durch den inneren und äußeren Notstand voneinander abgegrenzt. Zudem wurden die Polizeien reorganisiert, das Polizeirecht vereinheitlicht und die Entwicklung von Sicherheitsbehörden auf Bundesebene vorangetrieben. Die Ausformung des Politikfeldes war einerseits geprägt durch die Radikalisierung von Teilen der Außerparlamentarischen Opposition (APO), die in die Gründung der Roten Armee Fraktion (RAF) mündete, und andererseits durch die Kriminalitätsentwicklung im Land. In der Folge institutionalisierte sich ein Si-

01 Dieser Beitrag basiert in Teilen auf Michaela Wendekamm, Die Wahrnehmung von Migration als Bedrohung. Zur Verzahnung der Politikfelder Innere Sicherheit und Migrationspolitik, Wiesbaden 2015.
02 Vgl. Wolfgang Seifert, Geschichte der Zuwanderung nach Deutschland nach 1950, 31.5.2012, www.bpb.de/138012.
03 Zahlen vom Statistischen Bundesamt, siehe etwa die Pressemitteilung vom 14.7.2016 unter www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2016/07/PD16_246_12421.html.
04 Vgl. ebd.

cherheitsverbund und damit das Politikfeld. Eine inhaltliche Erweiterung erfuhr die innere Sicherheit danach durch den europäischen Integrationsprozess und ihre neue Bedeutung im EU-System.[05]

Mit Blick auf die innere Sicherheit lassen sich drei Grundpositionen identifizieren, die in politischen Debatten stets präsent sind. Die erste richtet sich auf den Umbau der Sicherheitsarchitektur mit Zentralisierung der wichtigsten Zuständigkeiten beim Bund. Vertreter der zweiten Grundposition fordern eine engere Verzahnung von innerer und äußerer Sicherheit. Ein aktuelles Beispiel ist die erneute Diskussion über den Einsatz der Bundeswehr im Innern und gemeinsame Einsatztrainings von Bundeswehr und Polizei. Diesen beiden Positionen steht die dritte Haltung gegenüber, dass die bürgerlichen Freiheitsrechte zu schützen seien. Entsprechend sehen ihre Vertreter die Zentralisierungstendenzen auf Bundesebene kritisch und verweisen auf die Achtung der Grundrechte sowie das Trennungsgebot zwischen Nachrichtendiensten und Polizei.[06]

Im Vergleich zur inneren Sicherheit ist die Entstehung und Abgrenzung des **Politikfeldes Migrationspolitik** schwerer zu fassen. Trotz der Faktenlage, dass spätestens seit den „Gastarbeiter"-Anwerbeabkommen der 1950er/60er Jahre zahlreiche Zuwanderer und Kinder von Zuwanderern in Deutschland leben, hat sich die Bundesrepublik lange nicht als Einwanderungsland verstanden. Migrationspolitik ist zudem ein Querschnittsthema und weist Überschneidungen zu anderen Politikfeldern wie der Entwicklungspolitik auf. Das Politikfeld zielt zum einen auf die bewusste Steuerung von „weltweite(r) Migration über Staatsgrenzen hinweg" ab,[07] andererseits auf die Organisation der Aufnahme und Integration von Zuwanderern. Ein besonderes Augenmerk liegt dabei auf qualifizierten Migranten, die aufgrund ihrer Fähigkeiten und ihres Nutzens für den deutschen Arbeitsmarkt einreisen dürfen. Ein Großteil der Integrationsmaßnahmen gilt jedoch der generellen Gestaltung des Zusammenlebens. Im Gegenzug soll irreguläre Migration verhindert werden.[08] Diese zwei Ziele orientieren sich an einem dritten: „der Gewährleistung der Sicherheit der Menschen in Deutschland und Europa".[09]

Hier spiegeln sich bereits die Grundpositionen dieses Politikfeldes wider. Sie bewegen sich im Spannungsfeld zwischen den Fragen, wieviel „Fremdes" ein System verträgt und wieviel Gemeinsames es braucht. Die erste Position befürwortet die Steuerung von Zuwanderung, während die zweite eine Begrenzung von Zuwanderung fordert. Da beide Positionen starke Fürsprecher haben, fanden sowohl Steuerung als auch Begrenzung Eingang in das Zuwanderungsgesetz von 2005. Vertreter der dritten Grundposition setzen sich für eine Stärkung des Standortes Deutschlands ein, um in den Wettbewerb um die bestqualifizierten ausländischen Fachkräfte treten zu können. Dies fordert jedoch gewisse Lockerungen der Zuwanderungsvoraussetzungen. Allgemein sind in diesem Politikfeld wirtschaftliche Überlegungen neben Sicherheitsaspekten sehr präsent.

Das Netzwerk der zivilen Akteure eines Politikfeldes lässt sich anhand der Intensität ihrer institutionalisierten Interaktionsbeziehungen in drei Einflussbereiche unterteilen:

1. Im *Zentralraum* befinden sich die staatlichen politikfeldspezifischen Behörden, die unmittelbare „Zugriffsrechte" auf die Bevölkerung besitzen und dementsprechend im Rahmen gesetzlicher Grenzen in die Grundrechte eingreifen dürfen. Sie bilden die Exekutive und werden in der Bevölkerung als die eigentlichen Akteure wahrgenommen. Im Bereich der inneren Sicherheit sind dies die Sicherheitsbehörden wie die Polizeien der Länder und des Bundes. In der Migrationspolitik sind beispielsweise die Ausländerämter im Zentralraum anzusiedeln.

2. Der Zentralraum ist vom *politisch-institutionellen Umfeld* umgeben. Hierzu gehören all jene Akteure, die die Arbeitsvoraussetzungen

05 Vgl. Hans-Jürgen Lange, Innere Sicherheit, in: ders. (Hrsg.), Wörterbuch zur Inneren Sicherheit, Wiesbaden 2006, S. 123–134, hier S. 127 ff.; ders., Innere Sicherheit im Politischen System der Bundesrepublik Deutschland, Opladen 1999, S. 75–105.
06 Vgl. Martin H. W. Möllers, Innenpolitische Dimensionen der Sicherheitspolitik in Deutschland, in: Stephan Böckenförde/Sven Bernhard Gareis (Hrsg.), Deutsche Sicherheitspolitik, Opladen 2009, S. 131–172, hier S. 157 f.; Hans-Jürgen Lange, Eckpunkte einer veränderten Sicherheitsarchitektur für die Bundesrepublik, in: Martin H. W. Möllers/Robert van Ooyen (Hrsg.), Jahrbuch Öffentliche Sicherheit 2006/2007, Frankfurt/M. 2007, S. 179–209.
07 Bundesministerium des Innern (BMI), Migration und Integration. Aufenthaltsrecht, Migrations- und Integrationspolitik in Deutschland, Berlin 2011, S. 10.
08 Vgl. Brain Keeley, Internationale Migration. Die menschliche Seite der Globalisierung, Bonn 2010, S. 57.
09 BMI (Anm. 7), S. 12.

für die politikfeldspezifischen Behörden schaffen. Im Gegensatz zur Exekutive haben sie in der Regel keinen unmittelbaren „Zugriff" auf die Bevölkerung. Als Beispiel lassen sich hier die Innenministerien und, sofern vorhanden, die Integrationsministerien anführen.

3. Den äußersten Bereich des Netzwerks bildet das *korrespondierende politische Umfeld*. Die hierzu zählenden Akteure versuchen im Sinne ihrer Interessen Einfluss auf das politisch-institutionelle Umfeld auszuüben. Zu ihnen zählen etwa Gewerkschaften und Nichtregierungsorganisation wie zum Beispiel Migrantenselbstorganisationen.[10]

Für das **Politikfeld innere Sicherheit** ist das Bundesministerium des Innern (BMI) der dominante Akteur. Dies ist darin begründet, dass es Kontrolle über die meisten anderen Akteure ausübt und dadurch Macht auf sich konzentriert. Bei der inneren Sicherheit handelt es sich um ein homogenes Politikfeld, in dem die staatlichen Akteure im Rahmen einer vertikal orientierten Integration zusammenarbeiten. Die Geschlossenheit des Akteursnetzwerks behindert dabei den Zugang anderer Akteure. So nehmen Verbände, Vereine oder sonstige Interessenvertretungen weniger Einfluss auf die politischen Inhalte als in anderen Politikfeldern. Gleichzeitig differenziert sich die innere Sicherheit in den Bereich private Sicherheitswirtschaft aus, wenn zum Beispiel staatliche Sicherheitsaufgaben privatisiert werden. Des Weiteren werden Adressaten von sicherheitspolitischen Maßnahmen kaum in die Prozesse des Politikfeldes einbezogen, sondern bleiben Gegenstand von Kommunikation.

Im Gegensatz dazu zeichnet sich das **Politikfeld Migrationspolitik** durch eine stärkere Heterogenität aus. Hierdurch entsteht ein höherer Koordinierungsbedarf zwischen den Akteuren, da diese in Form der diagonalen Integration über alle Ebenen des Mehrebenensystems miteinander verflochten sind. Infolgedessen ist ein einzelner zentraler Akteur nicht identifizierbar. Der Zugang des Politikfeldes ist verhältnismäßig offen, wobei die Partizipation an den politischen Prozessen auf ausgewählte Akteure beschränkt ist.

VERFLECHTUNGEN

Neben den politikfeldinternen Prozessen und Strukturen nehmen auch die wechselseitigen Abhängigkeiten zwischen den Politikfeldern sowie die Vernetzung im föderal organisierten Mehrebenensystem Einfluss auf die jeweiligen Prozesse und Programme.[11] Die Verzahnung von Politikfeldern lässt sich, ebenso wie die einzelnen Politikfelder für sich, anhand der drei Politikdimensionen *Polity* (Institutionen), *Politics* (Prozesse) und *Policy* (Inhalte) beschreiben.

Bei Politikfeldern sind Verflechtungen in der **Polity-Dimension** vorhanden, wenn Akteure in verschiedenen Politikfeldern vertreten sind. Dies trifft auf die Verzahnung der Politikfelder innere Sicherheit und Migrationspolitik zu: So befinden sich im Zentralraum beider Politikfelder die Bundespolizei, das Bundeskriminalamt (BKA), die Länderpolizeien sowie das Bundesamt für Migration und Flüchtlinge (BAMF). Darüber hinaus sind die behördenübergreifenden Plattformen Gemeinsames Analyse- und Strategiezentrum illegale Migration (GASiM) und Gemeinsames Terrorismusabwehrzentrum (GTAZ) beiden Politikfeldern zuzuordnen. Dem politisch-institutionellen Umfeld beider Politikfelder gehören unter anderem das BMI, die Innenministerkonferenz (IMK), Innensenate und Innenministerien der Länder, aber auch Bundestag, Landtage und Bundesrat mit entsprechenden Ausschüssen an. Parteien und Medien zählen in beiden Politikfeldern zum korrespondierenden politischen Umfeld.

Dementsprechend überlappen sich auch die beiden Policy-Communities und beeinflussen die politikfeldinternen Prozesse. Von einer Verflechtung in der **Policy-Dimension** wird gesprochen, wenn funktionale Abhängigkeiten zwischen den Politikfeldern bestehen. Liegen diese vor, haben Maßnahmen des einen Politikfelds auch Effekte auf das andere, sowohl mittelbar als auch unmittelbar. Das Terrorismusbekämpfungsgesetz von 2002 zum Beispiel, auch bekannt als „Sicherheitspaket II", hatte als Maßnahmenpaket der Sicherheitspolitik erhebliche Konsequenzen für die Migrationspolitik, da es auch Änderungen im Ausländer- und Asylrecht vornahm. So wurde die informationelle Sonderbehandlung von Aus-

10 Vgl. Hans-Jürgen Lange, Innere Sicherheit als Netzwerk, in: ders. (Hrsg.), Staat, Demokratie und Innere Sicherheit in Deutschland, Opladen 2000, S. 235–255, hier S. 242 ff.; Möllers (Anm. 6), S. 134.

11 Vgl. Frank Bönker, Interdependenzen zwischen Politikfeldern, in: Frank Janning/Katrin Toens (Hrsg.), Die Zukunft der Policy-Forschung, Wiesbaden 2008, S. 315–330, hier S. 315 f.

ländern ausgeweitet, die Einreise und der Familiennachzug erschwert und die Ausweisung und Abschiebung erleichtert, um sich besser gegen gewaltbereite Extremisten aus dem Ausland schützen zu können. Das Zuwanderungsgesetz von 2005 setzte die Linie des Sicherheitspaketes fort. Dies zeigte sich vor allem im neu geschaffenen Aufenthaltsgesetz (Artikel 1), das unter anderem die Abschiebung erleichtert. Gleiches gilt für die 2015/16 beschlossenen Asylpakete I und II.

Eine Verzahnung der **Politics-Dimension** ist gegeben, wenn Willensbildungs- und Entscheidungsprozesse in den Politikfeldern nicht unabhängig voneinander ablaufen. Je relevanter ein Politikfeld ist, desto weniger Rücksicht müssen Akteure dieses Politikfelds auf andere Politikfelder nehmen und desto leichter werden ihre Entscheidungen von anderen als gesetzt akzeptiert. Prinzipiell werden die Diskussionen und Entscheidungen in der Migrationspolitik durch die Ziele beziehungsweise Strategien der inneren Sicherheit maßgeblich mitbestimmt. Dies liegt jedoch nicht nur an der allgemeinen Bedeutung der Sicherheitspolitik für die Legitimität des Staates, sondern gleichfalls am großen Problemdruck, der aus den Wanderungsbewegungen entspringt.[12] In der Folge wird Integration nicht nur allein zum Ziel an sich, sondern auch zu einem Faktor, um Sicherheit gewährleisten zu können, in dem Sinne, dass sich über Migrationspolitik keine Bedrohungspotenziale entwickeln. Dies begünstigt den Eindruck, dass Zuwanderer unter Generalverdacht gestellt werden.

SPANNUNGEN

Im Feld der inneren Sicherheit besteht ein grundsätzlicher Konflikt zwischen individueller Freiheit und kollektiver Sicherheit. Insbesondere durch die Anschläge vom 11. September 2001 und deren Folgeereignisse wurde das Spannungsverhältnis zwischen Freiheit und Sicherheit verschärft und formte sich aus als Entgegensetzung von Terrorismusbekämpfung und Menschenrechten. Dies wird etwa in Diskussionen zum Abschiebeschutz und den „sicheren Herkunftsländern" deutlich. Die terroristische Vereinigung „Islamischer Staat" (IS) versucht seit geraumer Zeit, die Migrationssituation auszunutzen, um eigene Leute als Flüchtlinge getarnt in europäische Staaten einzuschleusen – was teilweise auch gelingt, wie vor allem die Anschläge in Paris im November 2015 gezeigt haben. Hierdurch verschränkt sich in der öffentlichen Wahrnehmung Terrorismus mit Zuwanderung.

Zugleich setzte seit 2001 in der Migrations- und Integrationsdebatte ein auf den Islam fokussierter Religionsdiskurs ein, der diese bis heute dominiert. Im Rahmen dessen wird der Islam teilweise als Integrationshemmnis oder gar -hindernis gesehen; auch von mangelnder Integrationsbereitschaft ist die Rede. Integrationsprobleme werden somit auf die Zugehörigkeit zu einer Glaubensgemeinschaft oder Ethnie reduziert.[13] Insbesondere die sexuellen Übergriffe an Silvester 2015 auf Frauen durch junge Männer aus dem nordafrikanischen Raum haben diese Sichtweisen erneut befeuert. Folglich kann der generelle Konflikt im Politikfeld Migrationspolitik als Frage, wie viel „Fremdes" ein gesellschaftliches System verträgt, zusammengefasst werden. Dies lässt sich im Gegensatzpaar restriktive Zuwanderungssteuerung versus liberale Aufnahmepraxis präzisieren, das sich ebenfalls in der öffentlichen Diskussion wiederfindet.

Die Konflikte beider Politikfelder wirken generell wechselseitig aufeinander ein. Fühlt sich die Mehrheitsgesellschaft durch „Fremdes" bedroht, führt dies zu einem Streben nach mehr Sicherheit, für dessen Einlösung freiwillig Freiheiten aufgegeben werden. Zugleich werden jedoch auch spezifische Freiheitsbeschränkungen für die vermeintlichen Bedrohungsurheber gefordert. Somit wirkt auf Letztere eine doppelte Freiheitsbeschränkung ein. Dies wird auch im Hinblick auf die Regelungen des Sicherheitspaketes II und des Zuwanderungsgesetzes deutlich. Während bei Ersterem prinzipiell die gesamte Wohnbevölkerung Deutschlands, mit Ausnahme der ausländerrechtlichen Anteile und dem Vereinsrecht, von den Maßnahmen betroffen ist, bezieht sich das Letztere nur auf Zuwanderer.

Dies gilt nicht nur für die deutsche Politik, sondern für ganz Europa. So wird auf europäischer Ebene über die Speicherung europäischer Fluggastdaten und eine Verschärfung des Waffenrechts verhandelt – auch dies ist eine Sache der Abwägung zwischen Sicherheit und Freiheit. Ein Beispiel für die potenzielle Einschränkung von

12 Vgl. ebd., S. 317–321.

13 Vgl. Nimet Şeker, Ist der Islam ein Integrationshindernis?, in: APuZ 13–14/2011, S. 16–21; Ulrike Davy, Terrorismusbekämpfung und Einwanderungsgesetzgebung, in: dies./Albrecht Weber (Hrsg.), Paradigmenwechsel in Einwanderungsfragen? Überlegungen zum neuen Zuwanderungsgesetz, Baden-Baden 2006, S. 210–245.

Minderheiten ist die Diskussion um ein Burka-Verbot, die nicht nur in Deutschland, sondern unter anderem auch in Frankreich, Estland, Spanien, Österreich und den Niederlanden geführt wird beziehungsweise wurde. Auch wenn das Verbot in einen sicherheitspolitischen Kontext gesetzt wird, steht dahinter vorrangig die Frage der Integration von Muslimen in die Mehrheitsgesellschaft.

SONDERFALL SPÄTSOMMER 2015

Das Verhältnis von innerer Sicherheit und Migrationspolitik wird den vorherigen Ausführungen folgend weniger als gegensätzlich gedacht, sondern vielmehr als Korrelativ. So dient die Migrationspolitik durch Integration dem präventiven Paradigma, während innere Sicherheit durch die Setzung eines restriktiven Rahmens die Voraussetzungen schafft, damit die Mehrheitsgesellschaft Zuwanderung innerhalb entsprechend definierter Grenzen akzeptiert. Dabei ist die Migrationspolitik in erster Linie jedoch eine Ergänzung der inneren Sicherheit und ihr somit tendenziell untergeordnet.

Die Ausnahme bilden die Ereignisse im Spätsommer 2015: Wenige Tage nachdem sie ihr inzwischen berühmtes „Wir schaffen das!“ gesagt hatte, öffnete Bundeskanzlerin Angela Merkel angesichts der sich verschlimmernden Lage für die in Ungarn festsitzenden Flüchtlinge am 5. September die Grenzen und erhob so die Humanität zum Primat. Für kurze Zeit war damit eine Einreise ohne jede Voraussetzung möglich, der bis dahin restriktive Rahmen suspendiert. Gesellschaftlich wurde diese Maßnahme von einer breiten „Willkommenskultur“ getragen. Eine Folge war jedoch, dass zwischen der Zahl der vom BAMF registrierten Personen und der Zahl der tatsächlichen Erstanträge auf Asyl eine größere „Lücke“ entstand („EASY-Gap“), auch wenn die Zahl der 2015 in Deutschland angekommenen Asylsuchenden jüngst von ursprünglich angenommenen 1,1 Millionen auf 890 000 korrigiert wurde.[14] Nicht nur im öffentlichen Diskurs hatte diese migrationspolitische beziehungsweise humanitäre Entscheidung durchaus auch Auswirkungen auf sich anschließende sicherheitspolitische Erwägungen.

Spätestens mit den Vorkommnissen in Köln zu Silvester stabilisierte sich das ursprüngliche Verhältnis der beiden Politikfelder wieder. Belege hierfür sind unter anderem die personelle Verstärkung der Polizeien, insbesondere bei der Bundespolizei und dem BKA, sowie die Präsenz der Themen Terrorismus und Organisierte Kriminalität im öffentlichen und innerorganisationalen Diskurs. Dabei ist zu beobachten, dass der Erfolg beziehungsweise die Durchsetzungsfähigkeit der Akteure steigt, wenn migrations- und sicherheitspolitische Themen gekoppelt werden.

Zusammenfassend lässt sich feststellen, dass die Themen Migration und Terrorismus anfangs einzeln in Relation zur inneren Sicherheit standen und in den vergangenen rund 15 Jahren zunehmend miteinander vermischt wurden. Speziell seit 2015 ist die diskursive Verknüpfung von Migration und Terrorismus im europäischen Raum verstärkt wahrnehmbar. Politik und Medien nehmen hier bei der Vermittlung beziehungsweise Konstruktion der Wahrnehmung eine wichtige Rolle ein. So wurde etwa im Juli 2016 ein Amoklauf in einem Münchener Einkaufszentrum von Medienvertretern und einzelnen internationalen Politikern in einen terroristischen und islamistischen Zusammenhang gesetzt. Der IS versuchte dies sogleich propagandistisch für sich zu nutzen. Schon bald stellte sich jedoch heraus, dass es sich um die Tat eines psychisch kranken Schülers handelte, der in München aufgewachsen war und keinerlei Bezug zum Islamismus hatte.

In der Pflicht stehen aber nicht nur Politik und Medien, sondern die Gesellschaft insgesamt: Um den Herausforderungen Zuwanderung und Terrorismus angemessen und verantwortungsvoll begegnen zu können, gilt es, genau hinzuschauen, wenn die Themen Migration und innere Sicherheit vermischt werden.

14 EASY steht kurz für „Erstverteilung der Asylbegehrenden“ und ist der Name der IT-Anwendung, mittels derer das BAMF die Flüchtlinge auf die Bundesländer verteilt. Für die korrigierten Zahlen vgl. BMI, Bundesinnenminister de Maizière gibt aktuelle Flüchtlingszahlen bekannt, Pressemitteilung, 30.9.2016, www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2016/09/asylsuchende-2015.html.

MICHAELA WENDEKAMM
ist promovierte Politikwissenschaftlerin und wissenschaftliche Referentin des Präsidenten an der Deutschen Hochschule der Polizei in Münster.
michaela.wendekamm@dhpol.de

SPYING ON ENEMIES – KNOWING YOUR FRIENDS

Zur Geheimdienstkooperation und Aufklärung unter Verbündeten

Christopher Nehring

„Ausspähen unter Freunden – das geht gar nicht!" Mit diesen Worten reagierte Bundeskanzlerin Angela Merkel im Herbst 2013 ungewöhnlich deutlich auf sich verdichtende Hinweise, dass US-Geheimdienste auch Personen und Institutionen in Deutschland ausspionieren. Ihrer Kritik und ihrem Tonfall schlossen sich zahlreiche Medienvertreter an; den meisten Kommentaren war dabei ein moralisch-ethischer Impetus gemein, der verdeutlicht, dass sich das „geht gar nicht" nicht auf die technische Machbarkeit bezog: Der Einsatz von Spionagetechniken zur Informationsgewinnung über nicht verfeindete Staaten wurde fast einhellig als ethisch wie rechtlich falsch beschrieben.

Hier zeigte sich einerseits eine verbreitete, historisch gewachsene Skepsis gegenüber Geheimdiensten, die auf den Erfahrungen mit Geheimdiensten (eher jedoch Geheimpolizeien) als Instrumente staatlicher Repression in Kaiserreich, NS-Diktatur und der DDR beruht. Andererseits spielten aber auch rechtlich verargumentierte Sorgen über Rechtsüberschreitungen durch Geheimdienste beziehungsweise deren Agieren im rechtsfreien Raum eine große Rolle. Nicht zu übersehen war jedoch die Diskrepanz zwischen der vornehmlich in der deutschen Öffentlichkeit zum Ausdruck gebrachten moralischen Entrüstung und dem internationalen Fachdiskurs zum Thema *spying on friends*. Ein Blick in das Nischengebiet der Intelligence Studies offenbart, dass Spionage zwischen befreundeten Staaten und miteinander kooperierenden Geheimdiensten beileibe keine Seltenheit und auch kein Paradoxon ist, sondern ein durchaus logisch zu erklärendes Phänomen.

Im Folgenden werde ich mich diesem Thema aus zwei Richtungen nähern: Zum einen sollen die im deutschen Diskurs weitgehend unbekannten theoretischen Annahmen aus den Intelligence Studies vorgestellt werden, zum anderen soll aus historischer Warte und anhand von Beispielen untersucht werden, was sich über die Häufigkeit dieser Erscheinung sagen lässt. Auf diese Weise soll der aktuellen Debatte ein Impuls in Richtung einer realpolitischen Herangehensweise gegeben werden.

INTELLIGENCE THEORY

Der sozialwissenschaftlich modellierten Intelligence Theory liegt ein rationalistischer Ansatz der internationalen Beziehungen zugrunde, demgemäß Staaten unter anarchischen äußeren Bedingungen nach Kosten-Nutzen-Maximierung streben. Dieser Handlungslogik folgen auch staatliche Geheimdienste, deren Hauptaufgabe im politischen System der Ausbau von Informationsgrundlagen für politische Entscheidungsträger ist. Als eine Möglichkeit hierzu dient die Zusammenarbeit mit anderen Geheimdiensten. Diese kann die Form eines einfachen Informationsaustauschs (*intelligence sharing*) oder darüber hinausgehende Kooperationsbeziehungen (*intelligence liaison*) annehmen.[01] Hauptantrieb für geheimdienstliche Zusammenarbeit ist die Maximierung von Informationsgewinnung beziehungsweise Vergrößerung operativer Möglichkeiten zu möglichst geringen Kosten. Die praktischen Formen solcher Quid-pro-quo-Arrangements sind variabel. Die Logik eines „Tauschhandels" (*give and take*) liegt auch Verabredungen über Informationsaustausch zugrunde.

Die Hauptfrage theoretischer Modelle von Geheimdienstkooperation ist die Frage nach den Gründen für eine Zusammenarbeit in diesem sensiblen Bereich. Hierbei wird von ei-

ner direkten Kausalbeziehung zwischen der ursprünglichen Motivation und der späteren Form ausgegangen sowie davon, dass geheimdienstliche Zusammenarbeit aufgrund von Hemmnissen generell unwahrscheinlich beziehungsweise schwierig ist. Als größte Hindernisse gelten Kosten-Nutzen-Abwägungen (*bargaining problem*) und Vertrauensfragen – wenn etwa Zweifel bestehen, ob Vereinbarungen auch eingehalten werden (*enforcement problem*).[02] Eine wichtige Rolle spielen das im Sicherheitsbereich grundsätzlich verbreitete Misstrauen sowie der Umstand, dass eine gleichzeitige Nutzenmaximierung für beide Kooperationspartner nur selten zu erreichen ist.

Das theoretische Instrumentarium bietet jedoch Erklärungsmuster, wie und warum diese Hindernisse überwunden werden können. Bedenken gegen Kooperationsengagements können zum Beispiel zurückgestellt werden, wenn der zu erwartende Nutzen überwiegt, die Teilnehmer also entweder gemeinsame Interessen verfolgen oder sich Einzelinteressen durch die Zusammenarbeit effizienter verfolgen lassen. Kooperationsvereinbarungen müssen jedoch nicht notwendigerweise auf Geheimdienstaktivitäten beschränkt bleiben. Bei unterschiedlichen Möglichkeiten oder Nutzen einer Seite aus der Kooperation können auch andere „Waren" (*goods*), wie Entwicklungs- oder Militärhilfe oder diplomatische Unterstützung einbezogen werden. Wichtig ist dabei allein das Prinzip, dass keine der beiden Seiten zur Ausweitung der Möglichkeiten eines anderen Dienstes beitragen wird, ohne im Gegenzug selbst davon in irgendeiner Art zu profitieren. In diesem Fall können strategische Verbündete asymmetrische Kooperationsarrangements – zum Beispiel in Allianzen – eingehen, wenn ihre Kosten im Wettbewerb für unabhängige, eigenständige Möglichkeiten höher wären.

Deutlich komplexeren Charakter erhält Geheimdienstkooperation in multilateralen Bündnissen, da davon ausgegangen wird, dass sich die Risiken um ein Vielfaches erhöhen. Dies führt dazu, dass erstens die Qualität der Zusammenarbeit am schwächsten beziehungsweise vertrauensunwürdigsten Partner ausgerichtet wird. Daraus folgt zweitens, dass jeder Teilnehmer prinzipiell die als sicherer angesehene bilaterale Kooperation bevorzugen wird. Bedenken einzelner Dienste können in einem multilateralen System drittens jedoch unwichtig werden, wenn die Liaison weniger den geheimdienstlichen Interessen als der Festigung eines politischen oder militärischen Bündnisses gilt. Dies kann viertens wiederum eine ungewünschte Entwicklung wie die Aushöhlung der Kooperation (*hollow liaison*), eine verfeindete Zusammenarbeit (*adversarial liaison*) oder das gesteigerte Bedürfnis zur „Aufklärung" beziehungsweise „Gegenaufklärung" der eigenen Kooperationspartner (*knowing your friends*)[03] hervorrufen, um deren Absichten herauszufinden beziehungsweise eine Infiltration durch eine dritte Partei auszuschließen. Spionage gegen Verbündete muss somit als eine mögliche Konsequenz und feste Eigenschaft geheimdienstlicher Kooperation angesehen werden.

Neben den bereits genannten typologischen Klassifikationen von Geheimdienstzusammenarbeit lassen sich fünf Kategorien unterscheiden, die sich jedoch teilweise überschneiden können:[04]

1. Die vollwertige Kooperation (*full-fledged liaison*) beschreibt eine offizielle, formale, autorisierte und stabile Zusammenarbeit über einen längeren Zeitraum hinweg und zeichnet sich durch folgende Merkmale aus: abgestimmte Sicherheitsklassifikationen und -vorkehrungen, Austausch von Verbindungsoffizieren, gemeinsame Kommunikationskanäle, gemeinsame Personalausstattung von Einrichtungen sowie persönliche Kontakte auf Leitungsebene.

2. Nachrichtendienstlicher Informationsaustausch (*intelligence information sharing*).

3. Gemeinsame Aufklärungsoperationen (*intelligence operations sharing*).

01 Zum gesamten Abschnitt vgl. Jennifer E. Sims, Foreign Intelligence Liaison: Devils, Deals, and Details, in: International Journal of Intelligence and Counterintelligence 2/2006, S. 195–217; James Walsh, The International Politics of Intelligence Sharing, New York 2010.

02 Vgl. Bradford Westerfield, America and the World of Intelligence Liaison, in: Intelligence and National Security 3/1996, S. 523–560; Chris Clough, Quid pro Quo: The Challenges of International Strategic Intelligence Cooperation, in: International Journal of Intelligence and Counterintelligence 4/2004, S. 601–613.

03 Vgl. Martin Alexander, Knowing Your Friends, in: ders. (Hrsg.), Knowing your Friends. Intelligence Inside the Alliances and Coalitions from 1914 to the Cold War, London 1998, S. 3–14.

04 Vgl. Jeffrey T. Richelson/Desmond Ball, The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries, Boston 1985, S. 160 f.

4. Nachrichtendienstliche Unterstützungsleistungen (*intelligence support*), zum Beispiel technische Hilfe oder Ausbildung.

5. Nachrichtendienstliche Zusammenarbeit als eine Form verdeckter Diplomatie (*crypto diplomacy*).

Obgleich die in den Intelligence Studies nach wie vor nur als Randströmung existierende Forschung zur Geheimdienstzusammenarbeit also plausible Modelle hervorgebracht hat, können nichtsdestotrotz auch einige Kritikpunkte geltend gemacht werden. So folgte dieser Forschungszweig bislang vor allem der allgemeinen Fixierung der Intelligence Studies auf die Geheimdienste der sogenannten Five-Eyes-Staaten USA, Vereinigtes Königreich, Kanada, Australien und Neuseeland. Alle Modellierungen beruhen demnach hauptsächlich auf den US-Geheimdiensten und ihrer Kooperation. Dies wirft die Frage auf, ob die Grundannahmen der Theoriebildung – vor allem jene über rationale und selbstständige Akteure – ohne Einschränkung auf nicht westliche oder autoritäre Staaten übertragbar ist. Untersuchungen hat es hierzu bislang kaum gegeben.[05] Ebenso kann argumentiert werden, dass jeweils nur passende historische Beispiele herangezogen sowie nichtlineare Entwicklungen und Rückschritte weitgehend ausgeklammert wurden, um die Modellierungen zu stützen. Dass etwa auch die *special relationship* zwischen den britischen und US-Geheimdiensten Phasen distanzierterer Zusammenarbeit hatte, wurde von der Theorie kaum rezipiert.

AUFKLÄRUNG IN DER PRAXIS: HISTORISCHE BEISPIELE

Den theoretischen Annahmen über Geheimdienstkooperation ist inhärent, dass Kooperationshindernisse, allen voran Misstrauen und Selbstschutz, zu einem natürlichen Interesse an der Aufklärung von Partnern führen können. Wenn etwa ein Geheimdienst eine neue Zusammenarbeit mit einem anderen eingeht oder aber eine bestehende in weitere Bereiche ausdehnt, wird er in seine Überlegungen einbeziehen, ob der Partner „sicher" ist, das heißt, dass geteilte Informationen nicht durchsickern oder Agenten kompromittiert werden. Ein prominentes Beispiel hierfür war aus US-amerikanischer Sicht die BND-Quelle „Curveball": Dies war der Deckname für den 1999 aus dem Irak geflohenen Ingenieur Rafid Ahmed Alwan, der behauptete, an irakischen Programmen zur Herstellung von Massenvernichtungswaffen mitgearbeitet zu haben.[06] Diese Erkenntnisse wurden vom BND an die CIA weitergeleitet, ohne dass ein direkter Quellenzugang ermöglicht wurde. Später bauten die USA ihre Argumentation für einen Einmarsch in den Irak unter anderem auf die – unwahren – Aussagen von „Curveball" auf. Der Fall wurde als Paradebeispiel für die in der Theorie beschriebenen Kooperationsschwierigkeiten angeführt: Hätte die CIA direkten Zugang zur Quelle oder aber durch eigene Aufklärung Erkenntnisse aus dem BND selbst gehabt, so hätte dies zu einer anderen Einschätzung führen können.[07]

In der Geschichte der Geheimdienste und ihrer Kooperation gibt es zahlreiche weitere Beispiele dieser Art. So soll gegen Ende des Ersten Weltkrieges eine Priorität des britischen Nachrichtendienstes gewesen sein, angebliche US-amerikanische Vorbereitungen für einen Chemiewaffeneinsatz aufzuklären.[08] Und bereits während des Zweiten Weltkrieges war weitestgehend bekannt, dass die UdSSR ihr Bündnis mit den USA auch für Zwecke der Aufklärung nutzte.[09] Doch erst für die Zeit des Kalten Krieges lassen sich regelmäßig Beispiele systematischer Aufklärung zwischen verbündeten Staaten dokumentieren. Besonders bemerkenswert ist dabei, dass sich dieses Phänomen auf beiden Seiten des Eisernen Vorhangs beobachten ließ.

Zunächst zur östlichen Seite: Spätestens nach dem Untergang des Kommunismus wurde klar, dass das sowjetische KGB nicht nur gegen den Westen und Dissidenten gearbeitet hatte, sondern auch in den „Bruderstaaten" extrem aktiv gewe-

05 Vgl. Philip H. J. Davies/Kristian C. Gustafson, An Agenda for the Comparative Study of Intelligence, in: dies. (Hrsg.), Intelligence Elsewhere. Spies and Espionage Outside the Anglosphere, Washington D. C. 2013, S. 3–12.

06 Vgl. Bob Drogin, Curveball: Spies, Lies, and the Con Man Who Caused a War, Washington D. C. 2007.

07 Vgl. Walsh (Anm. 1), S. 3. Allerdings wurde der Fall „Curveball" von amerikanischer Seite durchaus dazu benutzt, die Schuld für das eigene Versagen im Vorfeld des Irak-Krieges von sich zu schieben. Es erscheint höchst fraglich, dass die US-Regierung sich einzig auf die vom BND übergebenen Informationen stützte.

08 Vgl. Christopher Andrew, The British Secret Service and Anglo-Soviet Relations in the 1970's, Part I, in: The Historical Journal 3/1977, S. 673–706.

09 Vgl. Bradley Smith, Sharing Secrets With Stalin, Lawrence 1996.

sen war.[10] Wie der Prager Frühling 1968, der sowjetische Einmarsch in Afghanistan 1979 oder die polnische Krise ab 1980 zeigten, unternahm die sowjetische Geheimpolizei zahlreiche Operationen in verbündeten Staaten. Diese liefen zumeist unter dem Decknamen „PROGRESS“ und hatten – vereinfacht ausgedrückt – die Stabilisierung des sozialistischen Machtbereichs zum Ziel. Im Bereich der Fernmeldeaufklärung gehörte es darüber hinaus mindestens zum allgemeinen Vorgehen, dass das KGB zwar mit seinen Verbündeten kooperierte, dabei jedoch niemals den neuesten Stand seiner kryptografischen Technik offenbarte.[11] Auch das Ministerium für Staatssicherheit der DDR betrieb spätestens ab 1980 eine eigenständige Aufklärung der eigentlich verbündeten Volksrepublik Polen, deren innere Unruhen als Gefahr wahrgenommen wurden. Dabei kamen keineswegs nur Mittel der „offenen Informationsgewinnung“ zum Einsatz, sondern es wurde gezielt auf alle Mittel der Spionage zurückgegriffen.[12] Ließen sich die Aktivitäten des KGB gegen seine Verbündeten noch mit dem Konzept der Geheimdienstkooperation in asymmetrischen Allianzen erklären, war die DDR-Aufklärung gegen Polen ein Musterbeispiel für eine gegnerische Liaison.

Auch für die westlichen Geheimdienste gehörte die gegenseitige Aufklärung verbündeter Staaten im Kalten Krieg mehr oder weniger zum Alltag, was spätestens seit den 1980er Jahren gut dokumentiert ist. Dabei standen vor allem die Geheimdienste der NATO-Staaten sowie in Überschneidung die Five-Eyes-Staaten im Mittelpunkt. Die dominierende Stellung der US-Geheimdienste brachte es dabei mit sich, dass sie besonders oft im Fokus standen. Ähnlich wie im Zuge der „Snowden-Affäre“ ab 2013 betraf dies vor allem die Fernmelde- und Kommunikationsüberwachung der NSA. Durch Überläufer und kritische Mitarbeiter wurde bereits seit Mitte der 1970er Jahre in die Öffentlichkeit getragen, dass die NSA im Zuge ihrer Feindaufklärung auch die Kommunikation ihrer Verbündeten täglich aufklärte.[13] Selbst das eng verbündete Vereinigte Königreich war davon betroffen. Technisch wurden zumeist die eigentlich gegen den Ostblock gerichteten Abhörstationen auf dem Territorium befreundeter Staaten genutzt – etwa im bayerischen Bad Aibling.

IM DIENSTE NATIONALER INTERESSEN

Misstrauen und Selbstschutz können die Aufklärung unter Partnern jedoch nur teilweise erklären. Weitaus häufiger verweist ein *spying on friends* auf die enge Verquickung nachrichtendienstlicher Arbeit mit den Interessen der maßgeblichen Akteure im internationalen politischen System – den Nationalstaaten. Ihre Bedeutung hat im Zuge der wirtschaftlichen Globalisierung und der Herausbildung supranationaler Akteure wie der Europäischen Union oder den Vereinten Nationen abgenommen, sodass Geheimdienste in der neuen Welt(un)ordnung geradezu als Herzstück und Verkörperung der legitimen Eigeninteressen einzelner Staaten beschrieben werden.[14] Diese Interessen wiederum konvergieren oftmals miteinander, und so kommt es gerade auf geheimdienstlicher Ebene zu Nullsummenrechnungen, bei denen die Akteure – auch wenn sie auf anderen Ebenen zusammenarbeiten – miteinander konkurrieren und nur einer sein Interesse durchsetzen kann. Eine Zusammenarbeit von Geheimdiensten erscheint daher teilweise als extrem unwahrscheinlich.

Ein Beispiel für gelingende Kooperation findet sich in der geheimdienstlichen Zusammenarbeit gegen den internationalen Terrorismus: Hier haben viele Akteure das gleiche Ziel, weshalb der Nutzen des einen Partners nicht zwangsläufig einen Nachteil für einen anderen Partner bedeuten muss. Gleichzeitig jedoch bleiben dieselben Akteure in außenpolitischen oder wirtschaftlichen Bereichen nach wie vor in einem Konkurrenzverhältnis. So können westliche Staaten bei der Bekämpfung des islamistischen Terrorismus durchaus mit Russland kooperieren, obgleich die außenpolitische Aufklärung gegeneinander unvermindert fortgeführt wird.

10 Vgl. Richard Popplewell, The KGB and the Control of the Soviet Bloc: The Case of East Germany, in: Alexander (Anm. 3), S. 254–284.

11 Vgl. Christopher Andrew/Wassily Mitrochin, Schwarzbuch des KGB, Bd. 1, Berlin 1999, S. 346–380, S. 441 f.

12 Vgl. Tytus Jaskulowski, Przyjazn, ktorej nie bylo. Ministerstwo Bezpieczenstwa Panstwowego NRD wobec MSW 1974–1990, Warschau 2014.

13 Vgl. Richelson/Ball (Anm. 4), S. 265–268.

14 Etwa vom ehemaligen Leiter des britischen Inlandsgeheimdienstes MI5, Stephen Landers, International Intelligence Cooperation: An Inside Perspective, in: Cambridge Review of International Affairs 3/2010, S. 481–493.

Das nationale Eigeninteresse, mit dem Geheimdienste im Auftrag ihrer Regierungen handeln, ist dabei in bestimmten Bereichen eher kompatibel als in anderen. Hierzu gehört zum Beispiel der militärische Bereich, in dem es öfter zur Bildung von Allianzen und geheimdienstlicher Kooperation gegen gemeinsame Gegner kommt. Ein weiterer Bereich ist der Kampf gegen grenzübergreifendes organisiertes Verbrechen. Andere Tätigkeitsfelder hingegen scheinen besonders anfällig für geheimdienstliche Konkurrenz zu sein. Dies sind etwa die Bereiche Wirtschaft sowie Wissenschaft und Technik, in denen aufgrund direkter Verbindungen zu finanziellen und wirtschaftlichen Vorteilen eines Akteurs ein besonders hohes Ausmaß an Wettbewerb und Konkurrenz ausgemacht werden kann. Dies trifft auch auf Partner zu, die bereits in anderen Bereichen in einer Allianz kooperieren.[15]

Gänzlich diffus verhält es sich hingegen im äußerst weiten Bereich der Außenpolitik. Unzweifelhaft werden hier die meisten politischen Allianzen zwischen Staaten geschlossen. Die Annahme, dass zwischen verbündeten Staaten gegenseitige Aufklärung durch Geheimdienste gebannt sei, hält indes keinem Praxistest stand. Denn auch die politischen Interessen, Handlungen und Absichten eines befreundeten Staates sind wichtige Faktoren, die jede Regierung in Entscheidungen und Programme einbeziehen muss – sie ist daher auf entsprechende Informationen angewiesen. Nicht nur US-Geheimdienste nutzten ihr dichtes Netz aus Funk- und Fernmeldeüberwachung immer wieder zur Aufklärung über Verbündete, auch für kleinere Staaten des westlichen Militärbündnisses lassen sich ähnliche Hinweise finden.

Der MI5-Veteran Peter Wright beispielsweise berichtete detailliert darüber, wie seine Kollegen des britischen Geheimdienstes die französische Botschaft in London abhörten, um französische Reaktionen auf den britischen Beitritt zum Europäischen Wirtschaftsraum zu erkunden.[16] Wrights Darstellung mag hier exemplarisch für die Sichtweise und inneren Geheimdienstzusammenhänge solcher Aktionen stehen: Keineswegs nämlich sah er in Frankreich einen feindlichen Staat, dessen Pläne und Handlungen zum Abwenden von potenziellem Schaden notwendig waren. Stattdessen beschrieb Wright es als für die britische Regierung notwendig, zur bestmöglichen Ausgestaltung ihrer eigenen Politik über die Pläne und Absichten eines wesentlichen Akteurs informiert zu sein. Dass dieser Akteur gleichzeitig ein Partner und Verbündeter im Kalten Krieg war, war dabei zweitrangig.

In den meisten der im Bereich Außenpolitik bekannten Beispielen geht es um Fernmelde- und Kommunikationsüberwachung. *Spying on friends* beschränkt sich jedoch keinesfalls auf dieses vermeintlich geräuschlose Vorgehen. So gibt es – wenn auch zumeist schlecht dokumentiert – einige Fälle von politischer Einmischung in die Innenpolitik verbündeter Staaten. Die wenigen Beispiele beziehen sich ausnahmslos auf US-Geheimdienste in der Zeit nach 1945. Erst 2016 konnte etwa belegt werden, dass Willy Brandt als Regierender Bürgermeister von Berlin über Umwege Geld aus CIA-Kassen erhielt, um Kampagnen führen zu können.[17] Ähnlich sollen auch Wahlkämpfe in Kanada oder Australien durch Geld und gezielte Aktionen der CIA beeinflusst worden sein.[18]

Schon seit jeher enthält beinahe jede Form der politischen Informationsarbeit über befreundete Staaten nahezu alle wesentlichen Komponenten von Aufklärung. Die klassische außenpolitische Informationsgewinnung, etwa durch diplomatische Gespräche und Berichte, Militärbeobachter oder in vergangen Epochen durch Gesandtschaften, Boten und Militärattachés, unterscheidet sich dabei nur manchmal, oftmals auch gar nicht, von der „bösen Spionage" des digitalen Zeitalters. Die wesentliche Trennlinie verläuft entlang der Frage, ob die entsprechenden Informationen „offen" oder aber im Geheimen gesammelt werden. Vertrauliche Kamingespräche zwischen offiziellen und inoffiziellen Gesprächspartnern zweier Länder stellen hier bereits eine Grauzone dar. Noch besser hingegen eignen sich aber Beobachtungsmissionen von Militärattachés und Gesandten,[19] um zu verdeutlichen, wie dünn und oftmals verwischt die Grenze zwischen akzeptierter Informationsarbeit und Spionage ist.

15 Vgl. Peter Schweizer, The Friendly Spies, New York 1995; James Adams, The New Spies: Exploring the Frontiers of Espionage, London 1994.

16 Vgl. Peter Wright, Enthüllungen aus dem Secret Service, Frankfurt/M.–Berlin 1988, S. 116.

17 Vgl. Washington unterstützte Willy Brandt mit geheimen Zahlungen, 10.6.2016, www.faz.net/-14280080.html.

18 Vgl. Richelson/Ball (Anm. 4), S. 265–268.

19 Vgl. Alexander (Anm. 3), S. 5f.

FAZIT

Zusammenfassend lassen sich einige Ergebnisse festhalten, die konträr zu den im öffentlichen Diskurs vorherrschenden Annahmen verlaufen: So zeigt sich anhand der gängigen Theorien der Intelligence Studies, dass Geheimdienstkooperation im aktuellen internationalen System eher eine Ausnahme ist, nicht der Regelfall. Es lassen sich zahlreiche Kooperationshindernisse identifizieren, die eine Zusammenarbeit in diesem sensiblen Feld zumindest deutlich erschweren. Diese Hindernisse, ständige Sicherheits- und Vertrauensdefizite sowie das vorherrschende nationale Interesse der Akteure führen dabei – gerade auch innerhalb von Allianzen und Bündnissen – zu Aufklärungsbemühungen gegenüber Verbündeten. Je heterogener und asymmetrischer Allianzen sind beziehungsweise je dominanter ein Partner in ihnen ist, desto höher ist die Wahrscheinlichkeit eines *spying on friends*. Dabei muss diese Form der Aufklärung nicht zwangsläufig zu größerem Misstrauen zwischen den Partnern führen oder als Begrenzung für deren Kooperation wirken. Stattdessen – so zumindest ein theoretisches Argument – könnte sie auch kooperationsfördernd wirken, wenn sie Sicherheitsbedenken eines Partners durch eigene Informationsgewinnung zerstreuen kann.

Die Aufklärung von Verbündeten kann dabei unterschiedliche Formen und Methoden annehmen, die grundsätzlich das gesamte methodische Instrumentarium der Spionage ausschöpfen. Eine allgemeine Tendenz deutet jedoch daraufhin, dass „grobe“ und „rabiate“ Methoden wie Einflussoperationen, paramilitärische Einsätze oder auch die direkte Werbung von Agenten weniger häufig zum Einsatz kommen als bei der Aufklärung feindlicher Staaten. Ein unmoralisches *spying on friends* scheint sich fernerhin nicht selten nur durch diffuse und unbestimmte Trennlinien von allgemein akzeptierten Verhaltensweisen zu unterscheiden. Diplomatische Informationsgewinnung oder militärische Verbindungsmissionen gehören nach wie vor zu international anerkannten Tätigkeiten, obwohl auch sie die Grenze zur Aufklärung in verbündeten Staaten oftmals überschreiten. Hingegen gilt die Fernmeldeüberwachung beziehungsweise das Abhören eines Verbündeten als Tabubruch, was darauf hindeutet, dass die gewählte Methode der Informationsgewinnung über einen Partner von erheblicher Relevanz ist.

Aus historischer Sicht ist zu konstatieren, dass das Aufklären von Verbündeten zum geheimdienstlichen Alltagsgeschäft gehört. Aus nahezu allen historischen Epochen, Gesellschafts- und Bündnissystemen lassen sich Beispiele hierfür anführen. Dies mag zwar teils unterschiedliche Ursachen haben, nichtsdestoweniger lässt sich aber eine Tendenz erkennen, die darauf hindeutet, dass auch Partner untereinander ein genuines Interesse der Informationsgewinnung übereinander haben. Dies scheint auch in der vernetzten Welt von heute eine Konstante zu bleiben. In den entsprechenden Fachdiskursen ist diese Tatsache allerdings schon seit Langem – weit vor der NSA-Affäre – bekannt. Eine tiefere Rezeption der Erkenntnisse der angelsächsischen *intelligence communities* hätte hier auch in der deutschen Öffentlichkeit zu einer besseren Einordnung beitragen können.

Zu guter Letzt bleibt die Frage nach „Gegenmaßnahmen“ gegen Aufklärungsbemühungen durch verbündete Staaten. Die Bundesregierung wählte einen besonders interessanten Ansatz, als sie 2013 versuchte, ein „No-Spy-Abkommen“ mit den USA zu erreichen.[20] Ein solcher Ansatz war vor allem deshalb interessant, weil er historisch ohne Präzedenzfall ist und daher ein Novum gewesen wäre. Das Scheitern der Verhandlungen zeigt jedoch, warum ein solches Abkommen eher im Bereich des Wunschdenkens anzusiedeln ist: Die beschriebenen Hindernisse, allen voran der allgegenwärtige Sicherheitsvorbehalt, waren einfach zu groß. Ebenso wurde erneut die überragende Stellung des einen dominanten Partners deutlich, der zu so weitreichenden Konzessionen nicht bereit ist und dem keine gleichrangige Gegenleistung angeboten werden kann. Die zukünftigen Schutz- beziehungsweise Gegenmaßnahmen greifen daher auch weiterhin auf das einzige Mittel zurück, das in der Geschichte der Geheimdienste seit jeher angewandt wird: verschärfte eigene Sicherheitsvorkehrungen und eine aktive Spionageabwehr.

CHRISTOPHER NEHRING
ist Historiker. Nach dem Studium der Osteuropäischen, Mittleren und Neueren Geschichte in Heidelberg und Sankt Petersburg hat er über die Zusammenarbeit der Auslandsaufklärung der DDR und Bulgariens promoviert.

20 Vgl. John Goetz et al., All the Best, in: Süddeutsche Zeitung, 9.5.2015.

„Shoot their hearts and blow their minds"

TERRORISMUSBEKÄMPFUNG IN ISRAEL: VORBILD FÜR EUROPA?

Marcel Serr

Israels Geschichte ist auch eine Geschichte des Terrorismus und seiner Bekämpfung. Der jüdische Staat wird seit seiner Gründung 1948 mit allen erdenklichen Formen terroristischer Gewalt konfrontiert. Trotz gelegentlicher Rückschläge sind die Erfolge des Landes eindrucksvoll: Obgleich es in den vergangenen knapp 70 Jahren stetig Anschlägen und Angriffen ausgesetzt war, behauptet sich Israel als wohlhabende Demokratie. Die Terroranschläge, die Frankreich, Belgien und Deutschland jüngst erschütterten, deuten darauf hin, dass sich auch Europa zukünftig verstärkt mit Terrorbekämpfung zu befassen hat. Daher lohnt ein Blick auf die Erfahrungen Israels.

Die Ursprünge israelischer Terrorismusbekämpfung wurzeln in vorstaatlicher Zeit. In den 1930er Jahren baute der Brite Orde Wingate zum Schutz der zionistischen Siedlungen vor arabischen Überfällen die „Special Night Squads" auf. Er setzte auf demonstrativ gewalttätige, offensive Operationen zur Abschreckung – bis heute ein wesentlicher Bestandteil israelischer Militärdoktrin.

Im Israelischen Unabhängigkeitskrieg von 1948/49 flohen rund 700 000 Palästinenser in die Nachbarländer beziehungsweise wurden dorthin vertrieben. Einzelpersonen und Gruppen aus diesen palästinensischen Exilgemeinden wurden zur primären nichtstaatlichen Bedrohung für Israel. In den 1950er Jahren kosteten Sabotage-, Mord- und Raubüberfälle palästinensischer Eindringlinge 286 Israelis das Leben und richteten einen erheblichen wirtschaftlichen Schaden an. Die Israel Defence Forces (IDF) verübten massive Vergeltungsschläge in angrenzenden Staatsgebieten. Der spätere Ministerpräsident Ariel Sharon baute 1953 hierzu Israels erste Spezialeinheit auf (Unit 101).[01]

VOM SECHSTAGEKRIEG BIS IN DIE 1980ER JAHRE

Mit der Eroberung der Westbank und des Gazastreifens im Sechstagekrieg 1967 waren die IDF mit der Kontrolle einer feindlich gesonnenen Bevölkerung konfrontiert. Insbesondere in Gaza war die Gewaltbereitschaft gegen die Besatzer hoch. Innerhalb kurzer Zeit ergaben sich die Palästinenser jedoch nach Ausgangssperren, Verhaftungen und flächendeckender Geheimdienstarbeit Israels in ihr Schicksal.[02]

Ein wesentlich größeres Sicherheitsproblem waren die Terrorgruppen, die sich in den palästinensischen Flüchtlingslagern in den arabischen Nachbarländern bildeten. Unter dem Dach der Palestine Liberation Organisation (PLO) hatten sie zunächst in Jordanien ihre Operationsbasis. Zu den bedrohlichsten gehörte neben Jassir Arafats Fatah die Popular Front for the Liberation of Palestine (PFLP). Diese Gruppe „erfand" 1968 die Flugzeugentführung und leitete damit die Entstehung des modernen internationalen Terrorismus ein. Bis 1976 sollten palästinensische Terroristen 16 Flugzeuge entführen, oft mit dem Ziel, inhaftierte Mitstreiter freizupressen.

Israel war zunächst unvorbereitet, entwickelte dann jedoch effektive Gegentaktiken: Die Sicherheitskontrollen der Flugpassagiere wurden verschärft, und Piloten wurden geschult, Flugzeugentführer durch unerwartete Manöver zu überraschen. Außerdem war Israel eines der ersten Länder, das Flugsicherheitsbegleiter einsetzte und Spezialeinheiten zur Geiselbefreiung aufbaute. Als geradezu legendär gilt in diesem Zusammenhang der erfolgreiche Sturm auf eine entführte Air-France-Maschine in Entebbe (Uganda) im Juni 1976.[03]

Die Geiselnahme und Ermordung israelischer Athleten bei den Olympischen Spielen in München 1972 durch die Fatah-nahe Organisation „Schwarzer September" beantwortete Israel mit Vergeltungsaktionen durch den Mossad: Der israelische Auslandsgeheimdienst tötete in der Folge weltweit mehr als 20 palästinensische Terroristen.[04]

Nach ihrer Vertreibung aus Jordanien 1970/71 setzten die palästinensischen Terrorgruppen ihre Anschläge auf Israel von ihrer neuen Operationsbasis im Libanon fort. Nach einer besonders verlustreichen Attacke im März 1978, bei der 35 Israelis starben, drangen die IDF mit 25 000 Soldaten zeitweise im Libanon ein, um die PLO-Basen an der Grenze zu zerstören („Operation Litani"); allerdings ohne nachhaltigen Erfolg. Israel begann daher im August 1982 eine Invasion des Libanon („Operation Peace for Galilee"). Zwar gelang es den IDF, die PLO zur Flucht nach Tunis zu zwingen, doch Israels ausgedehnte Militärpräsenz im Libanon geriet mit fast 3000 Terroranschlägen zwischen 1982 und 1985 zum Fiasko. Schließlich zogen sich die IDF auf einen schmalen Sicherheitskorridor im Süden des Landes zurück.[05]

INTIFADA I + II

Im Dezember 1987 begannen die Palästinenser in der Westbank und dem Gazastreifen einen Aufstand gegen die Besatzung – die Intifada (arabisch: „abschütteln"). Auf Demonstrationen, Streiks und Straßenkämpfe waren die IDF zunächst nicht eingestellt. Anstelle von Panzerschlachten auf den Golanhöhen galt es nun, Steine werfende Teenager unter Kontrolle zu bekommen. Mit dem harten Einsatz von Schlagstöcken und Gummigeschossen bei Demonstrationen sowie Ausgangssperren und der Schließung von Schulen und Universitäten sorgte Israel schließlich für Ruhe. Die Frustration über die Wirkungslosigkeit des Aufstands führte jedoch zu einer stärkeren Rolle islamistischer Bewegungen und zum Aufstieg der Hamas.

Die PLO verlor im tunesischen Exil an Einfluss. Daher wandte sich Arafat Friedensverhandlungen zu, die im Rahmen der Oslo-Abkommen 1993/95 zur weitgehenden Selbstverwaltung des Gazastreifens und Teilen der Westbank unter der Palästinensischen Autonomiebehörde (PA) führten. Doch die Hamas positionierte sich gegen den Friedensprozess und beförderte dessen Scheitern durch Terrorakte, häufig Selbstmordattentate. Palästinensische Anschläge forderten bis 2000 über 250 Tote. Zwar setzte Israel die Verhandlungen fort, doch die mangelnde Bereitschaft der PA, gegen die Hamas vorzugehen, vergiftete die Atmosphäre. Die IDF setzten der Hamas vor allem durch eine Verhaftungswelle heftig zu. Die Zahl der Anschläge und Opfer nahm erheblich ab.[06]

Bereits im September 2000 eskalierte die Lage mit dem Beginn der zweiten Intifada erneut. Sogenannte *drive-by-shootings*, Heckenschützen und Selbstmordattentate rückten vorrangig israelische Zivilisten ins Visier. Rund 1000 Israelis fielen Anschlägen zum Opfer. 2002 wurde mit 53 Selbstmordattentaten, 277 getöteten israelischen Zivilisten und 149 getöteten Soldaten das blutigste Jahr der Intifada. Das öffentliche Leben in Israel war aus der Bahn geworfen. Selbst die zentralen Küstenstädte wie Tel Aviv und Netanya waren nicht mehr sicher. Entsprechend hoch war der Druck auf die Regierung, Entschlossenheit zu zeigen.

Premierminister Ariel Sharon reagierte mit der „Operation Defensive Shield": Es wurden 30 000 Reservisten einberufen, anschließend isolierten die IDF die arabischen Städte, besetzten sie und verhafteten zahlreiche Palästinenser. Die Operation inmitten der palästinensischen Bevölkerungszentren war ein militärischer Albtraum. Besonders heikel gestaltete sich die Einnahme von Jenin, wo sich

01 Vgl. Ben-Horin/Barry Posen, Israel's Strategic Doctrine, Santa Monica 1981; Simon Anglim, Orde Wingate and the Special Night Squads: A Feasible Policy for Counter-Terrorism, in: Contemporary Security Policy 1/2007, S. 28–41; David Landau, Arik. The Life of Ariel Sharon, New York 2014, S. 20–29; Benny Morris, Israel's Border Wars 1949–1956, Oxford u. a. 1993, S. 28, S. 32, S. 49–54, S. 70, S. 83 ff., S. 262, S. 419 f.

02 Vgl. Daniel Byman, A High Price. The Triumphs and Failures of Israeli Counterterrorism, Oxford u. a. 2011, S. 34–38; Ahron Bregman, Cursed Victory. A History of Israel and the Occupied Territories, London 2014, S. 3–34, S. 56–66.

03 Vgl. Ami Pedahzur, The Israeli Secret Services and the Struggle Against Terrorism, New York 2010, S. 34 ff.

04 Vgl. Aaron Klein, Striking Back. The 1972 Munich Olympics Massacre and Israel's Deadly Response, Tel Aviv 2006.

05 Vgl. Eyal Zisser, The 1982 „Peace for Galilee" War. Looking Back in Anger – Between an Option of a War and a War of No Option, in: Mordechai Bar-On (Hrsg.), A Never-Ending Conflict, Westport 2004, S. 193–211, hier S. 196 f., S. 203–208; Benny Michelsohn, Insurgency and Counterinsurgency in Israel, 1965–1985, in: ebd., S. 179–192, hier S. 189 f.

06 Vgl. Reuven Aharoni, The Palestinian Intifada, 1987–1991, in: ebd., S. 211–230; Ahron Bregman, Israel's Wars. A History Since 1947, Abingdon–New York 2010, S. 179–203; Byman (Anm. 2), S. 79 f., S. 99 f., S. 109 f.

die IDF einen Häuserkampf mit gut vorbereiteten Terroristen lieferten, die Tausende Sprengfallen gelegt hatten. Ab Mitte 2003 zogen sich die Streitkräfte aus den palästinensischen Städten zurück und kontrollierten lediglich die Zugangswege.

Dennoch brach der palästinensische Widerstand sukzessive zusammen. Die Erkenntnisse, die durch den Einsatz des israelischen Inlandsgeheimdienstes Shin Bet in den palästinensischen Städten gewonnen wurden, waren beträchtlich. Nach der Verhaftung von schätzungsweise 7000 Palästinensern und entsprechenden Verhören verfügte der Dienst über beinahe lückenlose Informationen über die Terrorgruppen. Der permanente Druck durch gezielte Tötungen und Verhaftungen zermürbte sie. Schon bald konnten die israelischen Sicherheitskräfte Selbstmordanschläge fast vollständig neutralisieren.[07]

HISBOLLAH

Die schiitische Hisbollah gilt als eine der gefährlichsten Terrororganisationen der Welt. Ihre Entstehung war eine unbeabsichtigte Folge von Israels Militärpräsenz im Libanon. Seit dem Rückzug der IDF in die Sicherheitszone fügte sie den Israelis durch ständige Angriffe permanent Verluste zu. Neben Sprengfallen nutzte die Hisbollah auch Selbstmordattentäter und terrorisierte Nordisrael mit Raketenangriffen. Die IDF reagierten 1993 und 1996 mit größeren Militäroperationen. Obgleich sie die Hisbollah nicht ernsthaft gefährdeten, gewährleistete dies den Israelis von 1996 bis 2006 eine Periode relativer Ruhe an der Nordgrenze.

Anfang 2000 leitete Israel schließlich den endgültigen Rückzug aus dem Libanon ein. Die Hisbollah bezog nun direkt an der Grenze Stellung und bereite sich auf den nächsten größeren Konflikt vor. Sie lagerte Raketen und installierte Abschussvorrichtungen in Privathäusern, legte Bunker und Tunnelsysteme an und bereitete Hinterhalte vor. Währenddessen versäumte es die israelische Aufklärung, systematisch Informationen über die Stellungen und Fähigkeiten der Hisbollah anzulegen.

Im Juli 2006 löste die Entführung von zwei verwundeten Soldaten durch die Hisbollah eine erneute Militäroperation der IDF aus. Die Israel Air Force (IAF) zerstörte zunächst die Langstrecken-Raketenstellungen sowie den Hisbollah-Bezirk in Beirut, Dahiya. Die Hisbollah konterte mit 4000 Raketenabschüssen, die erstmals Israels Bevölkerungszentren Haifa, Tiberias und Afula erreichten, wo 53 Zivilisten starben. 500 000 Israelis flohen in den Süden des Landes. Da sich Luftangriffe als wirkungslos erwiesen, entschied sich Jerusalem zu einer halbherzigen Bodenoffensive. Darauf hatte die Hisbollah gewartet; sie fügte den IDF empfindliche Verluste zu und konnte den Raketenbeschuss bis zum Waffenstillstand fortsetzen. Dagegen blieb die Durchschlagkraft der IDF-Bodentruppen unbefriedigend. Durch die Konzentration auf den Antiterrorkampf hatten die Fähigkeiten zum Bewegungskrieg nachgelassen. Andererseits verlor auch die Hisbollah viele Kämpfer. Insofern scheint die Operation die israelische Abschreckung wiederhergestellt zu haben – dafür spricht auch die seitdem an der Nordfront herrschende Ruhe.[08]

Seit 2011 geht diese Ruhe vor allem auf den syrischen Bürgerkrieg zurück, der die Hisbollah bindet. Es besteht allerdings die Gefahr, dass sich die Organisation aus dem Arsenal Assads bedient und damit ihre militärischen Fähigkeiten deutlich ausweitet. Israel hat bereits mehrfach den Waffenschmuggel mit präzisen Luftschlägen verhindert. Außerdem gehen die IDF davon aus, dass die Hisbollah den Südlibanon in eine ausgeklügelte Kampfzone mit unterirdischen Gefechtsständen und Tunneln ausgebaut hat. Ferner verfügt die Terrororganisation über 100 000 Kurzstreckenraketen und Hunderte Raketen, die ganz Israel erreichen können.

Mit dem sogenannten Islamischen Staat (IS) erwächst Israel zudem eine schwer kalkulierbare Bedrohung in unmittelbarer Nachbarschaft. Schon jetzt fällt die Ideologie des IS im islamistischen Spektrum der Palästinenser teilweise auf fruchtbaren Boden.[09]

07 Vgl. Sergio Catignani, Israeli Counter-Insurgency and the Intifadas. Dilemmas of a Conventional Army, Abingdon–New York 2008, S. 102–141; Byman (Anm. 2), S. 115f., S. 121–128, S. 139–159; Hirsh Goodman/Jonathan Cummings (Hrsg.), The Battle of Jenin. A Case Study in Israel's Communications Strategy, Tel Aviv 2003.

08 Vgl. Bregman (Anm. 6), S. 252–292; David E. Johnson, Hard Fighting. Israel in Lebanon and Gaza, Santa Monica u. a. 2011, S. 9–94.

09 Vgl. Benedetta Berti, The Syrian Civil War and Its Consequences for Hezbollah, 28. 12. 2015, www.fpri.org/article/2015/12/the-syrian-civil-war-and-its-consequences-for-hezbollah; Shlomo Brom, Israel and the Islamic State, in: Yoram Schweitzer/Omer Einav (Hrsg.), The Islamic State: How Viable Is It?, Tel Aviv 2016, S. 187–195.

HAMAS

2005 zog sich Israel aus dem Gazastreifen zurück. Kurze Zeit später siegte die Hamas überraschend bei den Wahlen zum palästinensischen Parlament 2006. Die Wahl löste zunächst Chaos, dann einen Bürgerkrieg zwischen Hamas und Fatah aus. Im Juni 2007 übernahm die Hamas die Macht im Gazastreifen. Damit wurden Raketenangriffe aus Gaza zur primären Sicherheitsbedrohung; 2007 gingen rund 1600 Raketen und Mörser auf Israel nieder. Im Juni 2006 entführte die Hamas zudem den IDF-Soldaten Gilad Shalit durch einen Tunnel.[10]

Israel kontrolliert alle Zugänge zum Gazastreifen (mit Ausnahme des Rafah-Übergangs nach Ägypten) und kann das Gebiet daher nahezu vollständig abriegeln. Es erlaubt zwar die Arbeit internationaler Organisationen, schränkt aber bisweilen den Warenverkehr nach Gaza ein, um den Raketen- und Tunnelbau zu erschweren. Aufgrund der anhaltenden Raketenangriffe startete Israel 2008/09, 2012 und 2014 jeweils umfassende Militäroperationen gegen die Hamas im Gazastreifen, die für eine gewisse Zeit die Attacken stoppten beziehungsweise reduzierten. Dabei bombardierte die IAF zunächst die Hamas-Infrastruktur und Raketenabschussrampen. 2008/09 und 2014 wurden die Angriffe aus der Luft zudem von Bodenoffensiven der IDF begleitet.

Obgleich Israel versuchte, durch Warnungen mit Flugblättern und Anrufen die Zahl der zivilen Opfer so gering wie möglich zu halten, kam es zu erheblichen Verlusten, da die Hamas die Zivilbevölkerung als Schutzschilde missbrauchte, indem sie Raketen in Schulen und Krankenhäusern lagerte und abschoss. Seit 2012 konnte Israel die Bedrohung durch Raketenangriffe dank der Inbetriebnahme eines Raketenabwehrsystems („Iron Dome“) eindämmen. Obgleich der Erfolg des Systems unbestritten ist, gelang es der Hamas 2014, durch den Einsatz von Raketen mit einer Reichweite von mehr als 70 Kilometern einen Großteil der israelischen Zivilbevölkerung in der Metropolregion um Tel Aviv unter Beschuss zu nehmen. 2014 trat zudem die Bedrohung durch Tunnel auf israelisches Territorium in den Vordergrund, die die Hamas zur Infiltration und für Entführungen nutzen konnte. Diese zeitigten eine erhebliche Wirkung: Während der Militäroperation 2014 verließen die Anwohner der Kibbuzim um den Gazastreifen erstmals mehrheitlich ihr Zuhause.[11]

2015 war das friedlichste Jahr an der Gaza-Front seit 2005. Dennoch ist die Hamas weiterhin eine akute Bedrohung. Die IDF hat mit Bohrvorrichtungen die Suche nach Tunneln bereits aufgenommen. Die nächste Eskalation am Gazastreifen ist daher nur eine Frage der Zeit.

Zwischen Herbst 2015 und Frühjahr 2016 war Israel zudem einer neuen Terrorwelle ausgesetzt, die 40 Tote und über 500 Verletzte forderte. Es kam beinahe täglich zu Attentaten mit Messern, Schusswaffen und Autos auf Israelis, vor allem in Jerusalem. Bemerkenswert ist jedoch die Tatsache, dass es sich fast ausschließlich um Einzeltäter handelte, die sich kaum in ein einheitliches Profil bringen lassen.[12]

ISRAELS ANTITERRORINSTRUMENTE

Israel hat ein breites Spektrum offensiver Antiterrortaktiken entwickelt, die darauf abzielen, Terroristen zu neutralisieren. Zu den wichtigsten Instrumenten zählt die **Inhaftierung**. Die Verwaltungshaft erlaubt es israelischen Sicherheitsbehörden, Angehörige von Terrororganisationen auch ohne juristisches Verfahren auf unbestimmte Zeit einzusperren. Die Ausnahmeregelung ist rechtlich umstritten und wird seitens Israels mit dem Schutz geheimdienstlicher Erkenntnisse und Quellen gerechtfertigt.[13]

Eng verknüpft mit der Inhaftierung sind die **Verhöre**. Dabei steht bei Terroristen weniger ein Geständnis als vielmehr die Gewinnung zusätzlicher Informationen im Mittelpunkt – der Kern der Terrorismusbekämpfung. Lange Zeit praktizierte Israel äußerst harte Verhörmethoden. 1999 verbot der Oberste Gerichthof allerdings die Anwendung physischer Gewalt.

Wenn sich Terroristen einer Verhaftung entziehen, greift Israel zu **gezielten Tötungen**. Zwi-

10 Seine Freilassung erkaufte Jerusalem im Oktober 2011 mit der Entlassung von 1027 palästinensischen Häftlingen.

11 Vgl. Byman (Anm. 2), S. 178–186, S. 193–203; International Crisis Group, Ruling Palestine I: Gaza under Hamas, Middle East Report 73/2008; Marcel Serr, Das israelische Iron Dome-System, in: Europäische Sicherheit und Technik 2/2014, S. 66 f.; ders., Operation Protective Edge, in: Allgemeine Schweizer Militärzeitschrift 12/2014, S. 26 f.

12 Vgl. Marcel Serr, Israels Sicherheit. Aktuelle Bedrohungen und Trends, in: Allgemeine Schweizer Militärzeitschrift 5/2016, S. 13 ff.

13 Derzeit befinden sich rund 6000 Palästinenser in israelischer Haft, davon etwa 700 in Verwaltungshaft.

schen 2000 und 2008 veranlasste Israel 234 gezielte Tötungen, bei denen 387 Palästinenser starben.[14] Obgleich diese Taktik aus rechtlicher und ethischer Perspektive häufig kritisiert wird, war sie aus operativer Sicht oft erfolgreich. Die Tötungen haben die Terrorgruppen schwer getroffen, indem sie die Anzahl fähiger Terroristen dezimierten und die Überlebenden zwangen, im Untergrund zu leben. Die Taktik ist jedoch nur dann effektiv, wenn sie konsequent umgesetzt wird und die Führungspositionen stetig im Visier behalten werden. Hinzu kommt, dass die Tötungen Politikern dabei helfen, der Bevölkerung Entschlossenheit zu demonstrieren. Terrorismus ist eine Form der psychologischen Kriegführung, die Angst und Schrecken verbreiten soll. Insofern muss eine effektive Terrorbekämpfung dies kontern. Maßnahmen, die das Vertrauen der Bevölkerung in die Regierung stärken, sind daher notwendig.

Weitere Offensivtaktiken sind **Hauszerstörungen** und **Ausweisungen**. Die Zerstörung von Häusern der Terroristen beziehungsweise ihrer Familien zielt als Abschreckungsmaßnahme auf die familiäre Disziplinierung junger Männer; ihr Nutzen ist allerdings umstritten. Durch Ausweisungen entledigt sich Israel zwar der unmittelbaren Gefährdung durch Terroristen, doch die Langzeitfolgen sind nicht absehbar: Die Abschiebung von über 400 Hamas-Anhängern in den Libanon 1992 führte dazu, dass ein Teil der palästinensischen Islamisten von der Hisbollah in die Herstellung von Selbstmordbombengürteln eingeführt wurde.

Diese offensiven Methoden können nur erfolgreich sein, wenn sie von defensiven Taktiken ergänzt werden. **Checkpoints** schränken die Mobilität der Terroristen – allerdings auch aller anderen – ein. Außerdem erlauben sie den IDF, jegliche palästinensische Bewegung in der Westbank zum Erliegen zu bringen. Bei Informationen zu unmittelbar bevorstehenden Terroranschlägen ermöglicht dies die notwendige Reaktionszeit.

Israels **Sicherheitsbarriere** entlang des Gazastreifens und der Westbank ist ein weiteres defensives Element der Terrorbekämpfung. Die Gaza-Barriere existiert seit 1994 und ist mit überlappenden Beobachtungsposten und ferngesteuerten Waffensystemen ausgestattet. Bei der Westbank-Barriere handelt es sich größtenteils um einen Zaun mit elektronischen Überwachungssystemen, in bewohnten Gebieten besteht sie aus Betonwänden. Der 2001 beschlossene Bau wird international kritisiert, weil er stellenweise auf palästinensischem Territorium verläuft, genießt aber einen großen Rückhalt in der israelischen Bevölkerung.

Weitere Maßnahmen des Bevölkerungsschutzes umfassen die Panzerung von Bussen, die durch problematische Gebiete fahren. Kindergärten, Schulen, Einkaufszentren sowie öffentliche Gebäude werden von bewaffnetem Sicherheitspersonal beschützt. Schließlich baut Israel die medizinische Notfallversorgung aus und bereitet die entsprechenden Einrichtungen auf plötzliche, große Opferzahlen vor.[15]

ELEMENTE DER ANTITERRORSTRATEGIE

Zentrales Element von Israels Terrorbekämpfung ist die Abschreckung: Durch überproportionale Vergeltungsschläge sollen potenzielle Terroristen von Attacken abgehalten werden. Israels Premierminister David Ben-Gurion brachte dies schon Mitte der 1950er Jahre auf den Punkt: „Wenn wir den Arabern nicht zeigen, dass sie einen hohen Preis dafür zahlen, Juden zu ermorden, werden wir nicht überleben."[16]

Während der in der westlichen Welt bevorzugte Ansatz der bevölkerungszentrierten Aufstandsbekämpfung große Aufmerksamkeit bekam, insbesondere im Rahmen der Kriege in Afghanistan und im Irak, setzt Israel auf eine feindzentrierte Terrorbekämpfung. Der bevölkerungszentrierte Ansatz geht davon aus, dass Terrorgruppen eine hinreichend unzufriedene Bevölkerung benötigen, aus der sie ihre Kämpfer und Unterstützer rekrutieren können. Ihre Handlungsfähigkeit lasse sich nur reduzieren, wenn man die „hearts and minds" der Bevölkerung gewinne und diese so der Terrororganisation entfremde. Dies ist ein Ansatz, der sehr hohe

14 Vgl. Byman (Anm. 2), S. 311.

15 Vgl. Gal Luft, The Logic of Israel's Targeted Killing, in: Middle East Quarterly 1/2003, S. 3–13; Danny Tirza, Why the Barrier Had to Be Built, 1.7.2012, www.al-monitor.com/pulse/originals/2012/al-monitor/israeli-security-fence-architect.html; Adam Hoffmann, No Magic Solution. The Effectiveness of Deporting Terrorists as a Counterterrorism Policy Measure, in: Institute for International Security Studies, Strategic Assessment 2/2016, S. 67–79; Byman (Anm. 2), S. 158–164, S. 297–302, S. 311ff., S. 320–332; Mark Bowden, The Dark Art of Interrogation, in: The Atlantic 10/2003, www.theatlantic.com/magazine/archive/2003/10/the-dark-art-of-interrogation/302791.

16 Zit. nach Byman (Anm. 2), S. 21.

Ansprüche an die zivil-militärische Kooperation stellt und viel Geduld, Geld und Opferbereitschaft erfordert. Wie die Einsätze im Irak und in Afghanistan gezeigt haben, ist der Erfolg ungewiss und das militärische Risiko hoch.

Mit Blick auf die tiefe Verbitterung im israelisch-palästinensischen Konflikt scheint dieser Ansatz kaum aussichtsreich. Zumal die Prämisse, dass hochrangige Terroristen ohne Weiteres ersetzbar sind, eine Fehlannahme ist. Die Anzahl erfahrener Terroristen mit Schlüsselkompetenzen ist begrenzt. Bombenbauer, Dokumentenfälscher und charismatische Anführer kommen nur in kleinen Zahlen vor. Wenn diese Schlüsselpersonen durch Tötungen oder Verhaftungen neutralisiert werden, kann eine Terrorgruppe zwar immer noch Rekruten gewinnen, doch ohne die besonderen Fähigkeiten der Schlüsselfiguren kann die Organisation nicht effektiv agieren.[17] Insofern basiert Israels Terrorverständnis auf einer endlichen Zahl von entscheidenden Terroristen, deren Wirkungsraum es einzuschränken gilt. Pointiert: Anstelle von „winning their hearts and minds", setzt Israel auf „shoot their hearts and blow their minds". Die Wirksamkeit dieses Ansatzes zeigt sich unter anderem darin, dass die Hamas zumindest in der Westbank kaum noch handlungsfähig ist; ohne Anleitung bleibt den Terroristen nur, allein zu agieren, was die „Tödlichkeit" ihrer Anschläge massiv reduziert – mangels einer organisatorischen Unterstützung durch eine Terrorgruppe verwenden sie hauptsächlich Messer und keine Bombengürtel.

LEHREN

Aus den Erfahrungen Israels lassen sich einige allgemeine Erkenntnisse ableiten:

1. Terrorismusbekämpfung, auch dann, wenn sie effektiv ist, führt oft nur zu weniger Anschlägen und weniger Opfern – nicht zu einem Ende des Terrorismus. Regierungen sollten dies zur realistischen Zielsetzung verinnerlichen.

2. Kern der Terrorismusbekämpfung ist die Geheimdienstarbeit zur Informationsgewinnung. Israel nutzt sämtliche administrativen Handlungen (Bewilligung von Reisegenehmigungen, Arbeitsgenehmigungen und anderes mehr), um Palästinenser als Informanten anzuwerben. Europa sollte das geheimdienstliche Potenzial der Geflüchteten in ähnlicher Weise nutzen, Informanten in gefährlichen Bewegungen (in erster Linie im islamistischen Spektrum) rekrutieren und diese aktiv unterwandern. Das Teilen von Informationen unter den Sicherheitsbehörden ist dabei eine grundlegende Erfolgsbedingung.

3. Auf der taktischen Ebene erweist sich ein Mix aus offensiven Methoden zur Neutralisierung hochrangiger Terroristen und defensiven Maßnahmen zum Schutz der Bevölkerung als zielführend. Insbesondere um die Mobilität der Terroristen einzuschränken, wird Europa nicht um engmaschigere Grenzkontrollen umhinkommen.

Diese Lehren hören sich für europäische Ohren zunächst harsch, vielleicht sogar teilweise inakzeptabel an. Doch Terroristen halten sich nicht an Regeln und moralische Grundsätze. Im Gegenteil: Sie nutzen diese zu ihrem Vorteil, indem sie die Zivilbevölkerung ins Visier nehmen oder als menschliche Schutzschilde missbrauchen. Die Terrorismusbekämpfung von Demokratien ist daher stets mit dem Dilemma konfrontiert, Sicherheit und Rechtsstaatlichkeit ausbalancieren zu müssen. Zu den primären Aufgaben eines Staates zählt jedoch, die Unversehrtheit seiner Bürger zu gewährleisten. Vor dem Hintergrund der Shoah gilt dies für Israel in einem besonderen Maße. Doch mit der steigenden Zahl von Anschlägen werden wohl auch Europas Staaten die Sicherheitsaspekte stärker in den Vordergrund rücken.

MARCEL SERR
ist Historiker und Politikwissenschaftler. Er ist wissenschaftlicher Assistent am Deutschen Evangelischen Institut für Altertumswissenschaft des Heiligen Landes (DEI) und promoviert an der Universität Haifa über die israelischen Streitkräfte in asymmetrischen Konflikten.
marcel-serr@web.de

17 Vgl. John A. Nagl, Learning to Eat Soup with Knife. Counterinsurgency Lessons from Malaya and Vietnam, Westport–London 2002, S. 26–29; Binard Finel, A Substitute for Victory, 8.4.2010, www.foreignaffairs.com/articles/afghanistan/2010-04-08/substitute-victory; Gian Gentile, A Strategy of Tactics: Population-centric COIN and the Army, in: Parameters 3/2009; Byman (Anm. 2), S. 367; Jason Rineheart, Counterterrorism and Counterinsurgency, in: Perspectives on Terrorism 5/2010, S. 31–47.

Herausgegeben von der
Bundeszentrale für politische Bildung
Adenauerallee 86, 53113 Bonn
Telefon: (0228) 9 95 15-0

Redaktionsschluss dieser Ausgabe: 14. Oktober 2016

REDAKTION
Lorenz Abu Ayyash (Volontär)
Anne-Sophie Friedel
Johannes Piepenbrink (verantwortlich für diese Ausgabe)
Anne Seibring
apuz@bpb.de
www.bpb.de/apuz
twitter.com/APuZ_bpb

Newsletter abonnieren: www.bpb.de/apuz-aktuell
Einzelausgaben bestellen: www.bpb.de/shop/apuz

GRAFISCHES KONZEPT
Charlotte Cassel/Meiré und Meiré, Köln

SATZ
le-tex publishing services GmbH, Leipzig

DRUCK
Frankfurter Societäts-Druckerei GmbH, Mörfelden-Walldorf

ABONNEMENT
Aus Politik und Zeitgeschichte wird mit der Wochenzeitung
Das **Parlament** ausgeliefert.
Jahresabonnement 25,80 Euro; ermäßigt 13,80 Euro.
Im Ausland zzgl. Versandkosten.
Frankfurter Societäts-Medien GmbH, Frankfurt am Main
parlament@fs-medien.de

Die Veröffentlichungen in Aus Politik und Zeitgeschichte
stellen keine Meinungsäußerung der Herausgeberin dar;
sie dienen der Unterrichtung und Urteilsbildung.

ISSN 0479-611 X

APuZ
Nächste Ausgabe
46–47/2016,
14. November 2016

LAND UND LÄNDLICHKEIT

APuZ
AUS POLITIK UND ZEITGESCHICHTE
www.bpb.de/apuz