SWP-Aktuell
NR. 40 JUNI 2022

»Hybride Bedrohungen«: Vom Strategischen Kompass zur Nationalen Sicherheitsstrategie

Annegret Bendiek / Raphael Bossong

Die tschechische EU-Ratspräsidentschaft will in der Außen- und Sicherheitspolitik der EU einen Schwerpunkt auf hybride Bedrohungen legen. Konkret sollen Diskussionen zu zwei Vorhaben aus dem Strategischen Kompass vom März 2022 beschleunigt werden. Es geht um die Erstellung zweier »Werkzeugkästen«, einer zur Abwehr hybrider Bedrohungen (EU Hybrid Toolbox) und einer gegen Desinformation und ausländische Einmischung (EU Foreign Information Manipulation and Interference Toolbox). Doch das liefe hauptsächlich darauf hinaus, vorhandene Rechtsakte und Maßnahmen der EU zu bündeln. Damit wird die Union der Herausforderung nicht gerecht. Vielmehr muss das Konzept der hybriden Bedrohungen kritisch hinterfragt werden, wenn es politisch überzeugen soll. Diese Aufgabe stellt sich umso dringender, weil hybriden Bedrohungen sowohl in der Nato als auch im Zuge der geplanten Nationalen Sicherheitsstrategie Deutschlands hohe Aufmerksamkeit gilt.

Schon die Besetzung der Krim 2014 machte deutlich, dass Großmachtkonflikte wieder mit allen verfügbaren, vielfach unkonventionellen Mitteln ausgetragen werden. Hierzu zählen unter anderem niederschwellige militärische Operationen, Cyberangriffe oder Desinformationskampagnen. Diese verdeckten Formen illegitimer Einflussnahme zwecks Destabilisierung von Demokratien bezeichnen EU- und Nato-Staaten als hybride Bedrohungen. Dabei handelt es sich um transnationale Bedrohungen, welche die öffentliche Ordnung eines anderen Staates stören oder zumindest beeinflussen sollen. Urheber können auch sogenannte Proxy-Akteure sein, das heißt solche, die nur indirekt oder verdeckt von einem der beteiligten Staaten unterstützt werden.

Noch vor wenigen Jahren wurden hybride Bedrohungen in erster Linie als gleichzeitige Anwendung bewaffneter Gewalt und nicht offen gewalttätiger Instrumente zur Einflussnahme verstanden. Heute dagegen schließt der Begriff auch rein zivile, aber dennoch aggressive Ansätze ein, die sich gegen die öffentliche Ordnung eines anderen Staates richten. Seit dem russischen Einmarsch in der Ukraine bemüht sich die EU, ihre Mitgliedstaaten dazu zu bewegen, gesellschaftliche, politische und wirtschaft-

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

liche Abhängigkeiten zu diversifizieren. In diesem Sinne betont die EU in ihrem Strategischen Kompass zur Sicherheit und Verteidigung vom März 2022, welche Gefahr für die Union von hybriden Bedrohungen ausgeht. Damit will sie Maßnahmen für mehr Resilienz anstoßen. Konkret avisiert sie in dem Kompass, die nachrichtendienstlichen Auswertungskapazitäten im Europäischen Auswärtigen Dienst (EAD) zu stärken sowie Rechtsakte und Maßnahmen der EU in einem »Werkzeugkasten« gegen »hybride Bedrohungen« und einem gegen »ausländische Einmischung« zusammenzufügen. Allerdings werden weder die verwendeten Begriffe erläutert noch die institutionellen und politischen Verantwortlichkeiten geklärt. Es wird auch kein systemisches Verständnis von Resilienz entwickelt. Aus Sicht strategischer Handlungsfähigkeit der EU sollte aber deutlich werden, worum es bei hybriden Bedrohungen eigentlich geht.

Die EU-Reaktionen

Die europäische Debatte über hybride Bedrohungen reicht bis in die späten 2000er Jahre zurück. Aber erst nachdem Russland die Krim annektiert hatte, wurden substantielle Abwehrmaßnahmen vereinbart. Als Erste handelte die Nato und investierte vor allem in nachrichtendienstliche Früherkennung und strategische Kommunikation, um Russlands Kampagnen etwas entgegenzusetzen. Der EAD folgte und beschloss 2015, eine »Task Force« zur strategischen Kommunikation zu gründen. 2016 verabschiedete die EU ein »Playbook«, also einen Leitfaden für eine politisch und institutionell koordinierte Antwort auf hybride Angriffe. Parallel dazu wurde die »Hybrid Fusion Cell« im Analysezentrum INTCEN-SIAC des EAD eingerichtet, um ein gemeinsames europäisches Lagebild zu ermöglichen. Ferner formulierten EU und Nato eine Erklärung für ihre Zusammenarbeit bei der Abwehr. Unter anderem wurde in Helsinki ein Exzellenzzentrum zur Analyse hybrider Bedrohungen eröffnet, und es wurden regelmäßige Übungen für den Krisenfall abgehalten. Bisher wurden allerdings im Rahmen der jeweiligen vertraglichen Grundlagen von Nato und EU keine Regeln für eine verbindliche grenzüberschreitende Solidarität als Antwort auf hybride Angriffe festgelegt.

Als die russische Einflussnahme auf die US-amerikanischen Präsidentschaftswahlen des Jahres 2016 schrittweise aufgedeckt wurde und Cyberangriffe auf Regierungsnetze in Europa einschließlich Deutschlands bekannt wurden, mehrten sich ab etwa 2018 die Sorgen um die Integrität von Wahlen und der öffentlichen Meinungsbildung. Um Desinformation einzudämmen, vereinbarte die EU einen Verhaltenskodex mit den großen Plattformanbietern. Vor der Europawahl im Mai 2019 wurden zudem neue Überwachungs- und Warnmechanismen geschaffen. Überdies nahm eine Horizontale Gruppe »Stärkung der Resilienz und Abwehr hybrider Bedrohungen« ihre Arbeit auf. Weiterhin wurde im EAD in Abstimmung mit der G7 ein Schnellalarmsystem zu hybriden Bedrohungen eingerichtet. Vorrangig mit Blick auf China wurde außerdem ein EU-Rechtsrahmen verabschiedet. Damit sollen ausländische Direktinvestitionen darauf überprüft werden können, ob sie die Verwundbarkeit kritischer Infrastrukturen erhöhen und technologische Abhängigkeiten erzeugen.

Während der Corona-Pandemie wurden die Bemühungen intensiviert, Desinformation zu bekämpfen und demokratische Willensbildung zu stärken. So initiierte die Europäische Kommission Ende 2020 einen »Aktionsplan für Demokratie in Europa«. Weitere Gesetzesvorhaben und institutionelle Reformen zum Resilienzaufbau wurden auf den Weg gebracht, etwa zum erweiterten Schutz kritischer Infrastrukturen und zur aktiven Cyberabwehr. Seither wächst die Bandbreite der Themen, die hybride Bedrohungen und eine entsprechende EU-Sicherheitspolitik betreffen. Im Herbst 2021 führten vor allem die mittel- und osteuropäischen EU-Mitglieder die Flüchtlingsbewegungen in Belarus auf eine »hybride« Gesamtstrategie Russlands zur Destabilisierung Europas zurück.

Der Strategische Kompass und Russlands Angriffskrieg

Die vielfältigen Initiativen und Rechtsakte, die einen europäischen Mehrwert bei der Bekämpfung hybrider Bedrohungen bringen sollen, werden seit Jahren in Arbeitsdokumenten meist nur katalogisiert. Bislang existiert keine klar nachvollziehbare Strategie zum Umgang mit hybriden Bedrohungen. Der im März 2022 vorgestellte Strategische Kompass soll nun explizit als Leitdokument für die Sicherheits- und Verteidigungspolitik der EU dienen. Auf der Basis einer umfassenden Bedrohungsanalyse sollen Ziele abgeleitet werden, wie die EU in den nächsten fünf bis zehn Jahren zum Schutz der EU sicherheits- und verteidigungspolitische Investitionen tätigen und Partner hierzu engagieren kann.

Zahlreich sind die Kritikpunkte an dem Dokument. Die Auflistung verschiedener Bedrohungen übersetzt sich nicht in einen neuen Katalog an grundlegenden Reformen und dringlichen verteidigungspolitischen Aufwendungen. Stattdessen werden darin vorwiegend rüstungspolitische Vorhaben bekräftigt, über die seit Jahren wenig erfolgreich in der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) debattiert wird. Allerdings wird im Kompass die Thematik der hybriden Bedrohung deutlich stärker hervorgehoben als in früheren Strategiedokumenten. So fallen auf den 47 Seiten des Kompasses in der englischsprachigen Originalversion tatsächlich 47-mal in unterschiedlicher Diktion die Bezeichnungen hybrider Angriff, hybride Taktik oder hybride Bedrohung. Die jeweiligen Bezüge reichen von Cyberangriffen sowie der Manipulation der öffentlichen Meinung über die zunehmende Verwundbarkeit durch die technologische oder wirtschaftliche Vernetzung — vor allem mit Blick auf China — bis hin zur Destabilisierung der europäischen Nachbarschaft durch Russland. Insofern könnte irrtümlich der Schluss gezogen werden, dass die EU mit diesem Dokument hybride Bedrohungen zur zentralen Priorität erklärt hat. Diesen Eindruck verstärken die mittlerweile sechs Sanktionspakete gegenüber Russland, die Anstrengungen zum Umbau der Lieferketten und Zulieferstrukturen von fossilen Energien sowie weitere Maßnahmen zur Erhöhung der Cybersicherheit und zur Eindämmung von Propaganda und Desinformation. Zu letzteren gehört das EU-weite Verbot der russischen Medien Sputnik und Russia Today.

Die EU kann durchaus ihre Markt- und Regulierungsmacht nutzen, um mehr Entflechtung oder Widerstandsfähigkeit in wirtschaftlichen, gesellschaftlichen und technologischen Bereichen zu erwirken — mit dem Ergebnis, dass die Angriffsfläche für hybride Bedrohungen kleiner wird. Diese Stoßrichtung zeigt sich ebenso in den jüngsten Zwischenberichten des EU-US Trade and Technology Council. Sowohl die EU als auch die USA befürworten eine weitaus intensivere Zusammenarbeit in vielen entscheidenden Themenbereichen, um gemeinsam unabhängiger gegenüber Russland und China agieren zu können. Angesichts der (digitalen) geopolitischen Dynamiken ist es umso wichtiger, Ziele klar zu umreißen und Instrumente zu schärfen. Doch der Strategische Kompass enthält gravierende konzeptionelle Defizite und Unklarheiten hinsichtlich hybrider Bedrohungen. Das schlägt sich im mangelhaften Detailgrad von Reformvorschlägen nieder.

Erstens: Begriffliche Schärfung

»Verdeckte Operationen«, »aktive Maßnahmen« oder andere Formen der »Subversion« waren im Kalten Krieg an der Tagesordnung. Der digitale Wandel und die wirtschaftliche Globalisierung haben allerdings die Kontextbedingungen internationaler Sicherheitspolitik strukturell verschoben. Entgegen klassischen liberalen Annahmen zur konflikthemmenden Wirkung von Interdependenz wird diese seit Anfang der 2000er Jahre verstärkt als Machtmittel oder gar als Waffe eingesetzt (»weaponized interdependence«). Waren es zuvor die westlichen Ordnungsmächte und die USA, die Interdependenz in ihrem Sinne ausgestalteten, versuchen nun häufiger autoritäre Staaten, die

liberale Ordnung der Wirtschaft und des Internets herauszufordern. Um diese Konfrontation zu beschreiben, wird im US-amerikanischen Diskurs oftmals von »gray zone conflicts« und in Europa von hybriden Bedrohungen gesprochen.

In einer Gesamtschau listet das European Centre of Excellence for Countering Hybrid Threats in Helsinki derzeit über 40 Instrumente auf, die sowohl staatliche wie nichtstaatliche Akteure für hybride Angriffe in mindestens 13 gesellschaftlichen, wirtschaftlichen oder politischen Sektoren nutzen. Die Bandbreite dieser Instrumente reicht von einer Störung von Informationszugängen über gezielte Manipulation von Daten bis hin zu kriegerischen Maßnahmen. Intention und Gesamtstrategie gegnerischer Akteure manifestieren sich in zahlreichen Einfluss- und Angriffswegen. All dies gilt es zu bewerten. Einzelne Cyberangriffe zum Beispiel sind nicht per se eine hybride Bedrohung, sondern erst im Zusammenhang umfassender gegnerischer Kampagnen. Das European Centre of Excellence versteht hybride Bedrohungen demnach als »koordinierte und synchronisierte Maßnahmen, die mit einer Vielzahl von Mitteln auf die systemischen Schwachstellen demokratischer Staaten und Institutionen abzielen« und so konzipiert sind, dass sie unterhalb klarer Schwellen der Erkennung und entsprechender Gegenmaßnahmen bleiben.

Mit dem Begriff hybride Bedrohung konkurriert die Bezeichnung »ausländische Einmischung« (»foreign interference« oder »foreign information manipulation and interference«). Damit ist gemeint, dass gegnerische Regierungen beabsichtigen, die Funktionen kritischer gesellschaftlicher Bereiche zu stören sowie zum Teil mit illegalen Mitteln vor allem Medien, die öffentliche Meinungsbildung und demokratische Wahlen in ihrem Sinne zu beeinflussen. Inhaltlich lässt sich dieser Terminus also teilweise vom Begriff hybride Bedrohung abgrenzen, denn Letztere kann auch offensivere, wenngleich verdeckte Angriffe einschließen und sich auf weitere wirtschaftliche Sektoren richten. Zudem werden bei hybriden Bedrohungen verstärkt Proxy-Akteure und konspirative Methoden genutzt, während der Terminus ausländische Einmischung sich hauptsächlich auf staatliche Akteure bezieht. In der politischen Praxis auf EU-Ebene verschwimmen allerdings die Begriffe. Supranationale Akteure sprechen eher von ausländischer Einmischung. Dagegen favorisieren die Mitgliedstaaten die Bezeichnung hybride Bedrohung, wohl um anzudeuten, dass das Problem in ihren exklusiven Kompetenzbereich der nationalen Sicherheit fällt.

Das Nebeneinander der Begriffe hybride Bedrohung, ausländische Einmischung, Desinformation und Cybersicherheit stiftet Verwirrung in Fachkreisen und mündet in institutionelle Kompetenzstreitigkeiten. Differenzierung tut not, um die Intensität der Einflussnahme zu erfassen und verhältnismäßige Gegenmaßnahmen zu treffen.

Zweitens: Verhältnismäßigkeit und politische Verantwortlichkeit

Die Forderung nach klar definierten Begriffen ist kein Allgemeinplatz. Ein besonders sensibles Beispiel betrifft die Verbindung von irregulärer Migration und hybriden Bedrohungen. So ist umstritten, ob Belarus mit der zeitweilig gezielten Steuerung der Migration in die EU die böswillige Absicht verfolgte, die Schengen-Zone zu destabilisieren. Auch unabhängig vom nachrichtendienstlichen Lagebild gilt es, eine separate politische Bewertung vorzunehmen, der wiederum unterschiedliche Werturteile im Hinblick auf die Problematik von Flucht und Migration zugrunde liegen. Konkret ist also strittig, ob irreguläre Zuwanderung grundsätzlich in den Zusammenhang hybrider Bedrohungen gerückt werden sollte. Mit einer solchen Einordnung werden verstärkt militärische Maßnahmen oder Akteure sowie weitaus schärfere Grenzsicherungsmaßnahmen legitimiert, bis hin zur systematischen Verweigerung des Zugangs zu Asylverfahren. In dieser Gemengelage schlug die Europäische Kommission den Mitgliedstaaten vor, nicht von hybrider Bedrohung, sondern von illegitimer »Instrumentalisierung« irregulärer Migration durch Drittstaa-

ten zu sprechen. Während im Rat jüngst eine politische Einigung zur Anpassung des Schengen-Rechts erzielt wurde, bleiben die Folgewirkungen für Asylverfahren höchst umstritten und erfordern weitere Verhandlungen im Europäischen Parlament.

Maßnahmen gegen hybride Angriffe mögen also im günstigen Fall abschreckend wirken, im ungünstigen Fall jedoch negative Folgen für liberale und offene Gesellschaften haben. Verbote, Regulierungen und forcierte Kappungen der Vernetzung, die eine Angriffsfläche für hybride Attacken bietet, sollten dem Verständnis nach mit der freiheitlich-demokratischen Grundordnung vereinbar sein. Die »strategische Ambiguität« des Strategischen Kompasses, in sehr unterschiedlichen Zusammenhängen von hybriden Taktiken, Angriffen oder Bedrohungen zu sprechen, ist daher nicht unproblematisch.

Sinnvoll hingegen ist die im Kompass vorgeschlagene Aufwertung der nachrichtendienstlichen Auswertung und der Hybrid Fusion Cell im EAD. Es bedarf der Früherkennung und fallspezifischen Einordnung, ob in der Auseinandersetzung mit Drittstaaten hybride Bedrohungen auftreten. Die EU ist zudem seit dem Brexit darauf angewiesen, strategisch wichtige Attributionen und vertrauliche Informationen über den Nachrichtendienstverbund der Five Eyes (USA, Vereinigtes Königreich, Australien, Kanada, Neuseeland) zu importieren. Einige Mitgliedstaaten reagieren auf diese Informationsabhängigkeiten sehr sensibel. Insofern wäre es ratsam, die Zulieferung und systematische Auswertung nachrichtendienstlicher Informationen auf EU-Ebene weiter zu verstetigen. Konkrete Optionen für eine verstärkte Zusammenarbeit in diesem Bereich werden im Strategischen Kompass allerdings nicht benannt.

Darüber hinaus gilt es, die politischen Entscheidungsstrukturen auf EU-Ebene weiterzuentwickeln, die hybride Bedrohungen betreffen und auf nachrichtendienstliche Einschätzungen im INTCEN-SIAC zurückgreifen. Die institutionellen Verfahren und undurchsichtigen Strukturen wie die Horizontale Gruppe im Rat oder auch das »Playbook« aus dem Jahr 2016 werden in diesem Kontext den Anforderungen an exekutive und demokratische Verantwortlichkeit in der Europapolitik nicht gerecht.

Drittens: Mehr als Werkzeugkästen und statische Resilienz

Die genannten Herausforderungen — also die frühzeitige Erkennung und Einordnung hybrider Angriffe und eine verhältnismäßige Reaktion darauf — lassen sich mit einer eher allgemeinen, passiv ausgerichteten Strategie der »Deterrence« oder »Resilience by Denial« entschärfen. Regulative Maßnahmen, die weit über jene der Sicherheit und Verteidigung hinausgehen, tragen durchaus dazu bei, Demokratien wehrhaft zu machen. Ansätze zur Stärkung von IT-Mindestsicherheitsstandards sowie gesamtgesellschaftliche Cyberhygienemaßnahmen sind hilfreich und können Einfallstore für böswillige Handlungen schließen. Angestrebt wird eine gesamtgesellschaftliche Resilienz, die unterschiedliche Politikbereiche und Behörden (»whole of government«) sowie privatwirtschaftliche und gesellschaftliche Akteure (»whole of society«) einbezieht. Darüber hinaus sollte smarte Resilienz weniger als Fähigkeit zur Wiederherstellung des ursprünglichen Zustands begriffen werden, sondern vielmehr als Ausgangsbedingung für und Ergebnis von kreativen Anpassungen an Krisen und Herausforderungen.

Der Strategische Kompass wird der Vielschichtigkeit des Resilienzkonzepts ebenso wenig gerecht wie der Vielfalt der Strategien einer Resilience by Denial. Zwar soll der Kompass die bisherige breit angelegte Politik der EU zu hybriden Bedrohungen neu bündeln. Praktisch beschränkt sich dies aber darauf, dass im Rahmen der GSVP zwei »Werkzeugkästen« geschaffen werden sollen, einer zu hybriden Bedrohungen und einer zu ausländischer Einmischung.

Offensichtlich ist der Begriff Werkzeugkasten von der bereits bestehenden »Cyberdiplomacy Toolbox« in der GASP inspiriert. Darin hat die EU in Grundzügen festgelegt, wie sie in abgestufter Weise auf Cyber-

angriffe reagieren will, bis hin zu restriktiven Maßnahmen. Inhaltliche Details zu den beiden angekündigten Werkzeugkästen fehlen aber im Kompass vollständig. Wiederum wurden die Begriffe nicht eindeutig definiert, so dass unklar bleibt, welche Werkzeuge, Rechtsakte oder andere Maßnahmen mit welchen Verfahren jeweils welchem Werkzeugkasten zugeordnet werden könnten. Ungewiss ist auch, ob analog zur Cyberdiplomacy Toolbox eine Stufenlogik bis hin zu Sanktionsentscheidungen greifen soll. Die Bezeichnung Werkzeug suggeriert, dass eine Reparatur oder zielgerichtete Gegenmaßnahmen notwendig sind. Angesichts stark politisch gefärbter und kontextabhängiger Bewertungen hybrider Bedrohungen ist diese technische Metapher wenig konstruktiv.

Ein weiteres grundsätzliches Defizit der »Werkzeugkastenlogik« ist, dass damit ein systemischer Blick auf Resilienz verloren geht. So könnte eine Strategie der Resilienz dazu anleiten, Angriffe und Störungen in Kauf zu nehmen, und darauf setzen, dass offene wirtschaftliche und gesellschaftliche Systeme aus sich heraus einer Destabilisierung und Unterwanderung widerstehen können. Statt aktiver Eingriffe im Einzelfall, etwa dem Verbot bestimmter Medien oder der Löschung von Falschnachrichten, genösse die Aufrechterhaltung eines möglichst pluralistischen Mediensektors Vorrang. Gewiss können eher systemische Ansätze zur Resilienz (wie indirekte Regulierung, Aufsicht und Wettbewerb) mit einzelnen Eingriffen kombiniert werden, wie es zunehmend auch in der Cybersicherheit gehandhabt wird. Insofern wären eine Ausdifferenzierung und eine Handlungslogik jenseits von Werkzeugkästen ratsam. Schon rein rechtlich bietet die GSVP, auf die sich der Strategische Kompass primär bezieht, keine Grundlage, um eine umfassende Sicherheitspolitik gegen hybride Bedrohungen zu koordinieren.

Das Beispiel Cybersicherheit und Hybrid

Die begrifflichen Probleme und das schwierige Zusammenspiel von verhältnismäßiger Abschreckung und Resilience by Denial lassen sich exemplarisch in der Cybersicherheit beobachten. Laut der Agentur der EU für Cybersicherheit (ENISA) ist die Energieinfrastruktur ein besonders attraktives Ziel für Cyberangriffe, da die Folgen weitreichend sein und als Hebel für Erpressungen oder als Ausgangspunkt für militärische Operationen genutzt werden können. Für die Unternehmen des Energiesektors, die schon unter die alte Richtlinie der EU über die Sicherheit von Netz- und Informationssystemen (NIS) aus dem Jahr 2017 fielen, bedeuten die neuen Auflagen gemäß der NIS-2-Richtlinie strengere Berichtspflichten. Cyberangriffe müssen die Firmen binnen 24 Stunden melden, Details darüber binnen 72 Stunden. Andernfalls drohen ihnen Strafen von bis zu 10 Millionen Euro. Der Geltungsbereich der Richtlinien wurde auf elektrische Stromladeeinrichtungen erweitert. Sie ergänzen damit die als kritisch eingestuften Erzeugungs- und Transportinfrastrukturen der Energieuntersektoren Erdgas, Fernwärme, Erdöl, Elektrizität und Wasserstoff. Auf diese Weise wird in Friedenszeiten regulären Sorgfaltspflichten zur IT-Sicherheit Rechnung getragen. Dies ist eine von zahlreichen Maßnahmen zum Resilienzaufbau. Zum Eigenschutz und zur Gefahrenabwehr greifen Regierungen in einem weiteren Schritt auf elektronische Aufklärung zurück, scannen Schwachstellen und setzen gegebenenfalls Trojaner zur Strafverfolgung ein.

Im Kontinuum zwischen Frieden und Krieg werden Cyberangriffe erst dann als hybrid eingestuft, wenn sie mit der böswilligen Absicht zur Manipulation oder Störung gezielt auf Infrastrukturen gerichtet werden. Solche flächendeckend angelegten Nadelstiche gehen auf das Konto von Hackergruppen, die zielgerichtet im Auftrag von Staaten oder mit deren Duldung vorgehen. Bei den jüngsten DDoS-Attacken des prorussischen Hackerverbunds »Killnet«

seit Mai 2022 handelt es sich bislang um vergleichsweise harmlose Störangriffe, die nur die Webseiten-Präsenz westlicher Regierungsstellen beeinträchtigten. Auf ihrem Telegram-Kanal hatten die Killnet-Hacker eine Liste mit Webadressen deutscher »Ziele« veröffentlicht, vermutlich um ihre Anhängerschaft über ihr Vorhaben zu informieren und zur Teilnahme zu animieren. Aufgelistet waren Webseiten der Postbank und der Wiesbadener Aareal Bank sowie von Kliniken und Universitäten. Es stellt sich die Frage, ob dies schon als hybride Bedrohung einzustufen wäre.

Noch gibt es keine militärische Cyberdoktrin, die vorsieht, Cyberangriffe zusammen mit traditioneller militärischer Gewalt gegen einen gleichrangigen oder nahezu gleichrangigen Gegner einzusetzen. Viele der Theorien über die möglichen Auswirkungen von Cyberangriffen in modernen Konflikten werden derzeit in der Realität getestet. Die Ukraine erlebte bis zum Beginn der Invasion massive Attacken auf die digitale Infrastruktur des Landes, auf Webseiten, Banken, Regierungs- und Militärstellen. Seither sind jedoch neue weitreichende oder noch schwerere Cyberangriffe durch Russland ausgeblieben oder waren eher wirkungslos. Eine Ausnahme bildete der Angriff auf Schaltstellen der Satellitenverbindung (ViaSat), welche die Ukraine unter anderem für die Zielerfassung und -führung ihrer Artillerie nutzte. Dieser russische Cyberangriff führte Anfang März auch zu Ausfällen der Steuerung von Windrädern in Deutschland. Da aber der Unternehmer Elon Musk über das Satellitensystem Starlink ein alternatives Kommunikationsnetz bereitstellte, wurde Russlands strategische Intention, die Ukraine militärisch zu schwächen, vereitelt.

Welche Lehren sich auch für EU-eigene Informationsinfrastrukturen aus diesen Angriffen ziehen lassen, muss noch systematisch untersucht werden. Europa ist jedenfalls potentielles Ziel weiterer Attacken von Hackern, die taktische Interessen in geostrategischen Konflikten verfolgen. Beispielsweise hatte die russische Cybereinheit Sandworm, die auch den Stromausfall in der Ukraine 2015 verursacht hatte, die Kontrolle über zahlreiche Router in kleinen und mittleren Betrieben übernommen. Ob dieses Netzwerk und die verwendete Schadsoftware »Cyclops Blink« durch Gegenmaßnahmen unter Führung des FBI mittlerweile vollständig ausgeschaltet werden konnten, ist noch nicht gesichert. Die russischen Staatshacker scheinen nach weiteren Lücken zu suchen. Das Bundesamt für Sicherheit in der Informationstechnik und der Verfassungsschutz warnen vor aggressiven Scan-Aktivitäten, mit denen Sicherheitslücken aufgespürt werden sollen. Wann also ist die Schwelle überschritten, dass die Beistandsklausel in der EU aktiviert oder der Nato-Bündnisfall ausgerufen werden müsste? Nicht nur ist es außerordentlich schwierig, Faktoren festzulegen, anhand derer eine solche Entscheidung getroffen werden kann. Politisch ist es sogar beabsichtigt, sich unklar darüber zu äußern, was eine Kriegshandlung im Cyber- und Informationsraum darstellt und was nicht. Der Gegner soll laut Verteidigungsstrategen im Ungewissen gelassen werden, damit er nicht ermutigt werde, sich an eine definierte Schwelle heranzutasten, deren Erreichen eine entsprechende Reaktion auslösen könnte. Diese fehlende Klarheit über die Kriegseintrittsschwelle ist problematisch, weil sie nicht zur Erwartungsverlässlichkeit von Akteurshandeln beiträgt, die prinzipiell konfliktentschärfend wirkt. So gilt für EU und Nato im Cyber- und Informationsraum zurzeit das Konzept der strategischen Doppeldeutigkeit. Die Nato hat festgelegt, dass ein Hackerangriff Artikel 5 des Nato-Vertrages, also den Bündnisfall auslösen kann. Wie bei konventionellen Angriffen hat die Allianz bewusst offengelassen, wann genau dieser Fall eintritt. In der EU ließe sich Artikel 222 EUV oder die militärische Beistandsklausel gemäß Artikel 42 Absatz 7 EUV aktivieren.

Lessons learned für die Nationale Sicherheitsstrategie

Die bisherigen EU-Dokumente, allen voran der Strategische Kompass, weisen einige Defizite auf: Erstens mangelt es dem Terminus hybride Bedrohung an Präzision und besonders an der Abgrenzung gegenüber dem verwandten Begriff ausländische Einmischung (durch feindliche Regierungen). Allerdings markiert die intendierte begriffliche Unschärfe, die im Fall hochintensiver Cyberkonflikte zur Abschreckung dient, derzeit das obere Ende der Eskalationsdynamik. Dies gilt es nochmals kritisch zu hinterfragen, nämlich darauf, ob davon eine konfliktverschärfende Wirkung ausgehen kann. Am unteren Ende der Eskalationsspirale, also im Falle wiederkehrender Praktiken der Einmischung, sollten die Begriffe auf jeden Fall klarer sein, Verlässlichkeit im Akteurshandeln schaffen und deeskalierend wirken. Während in vielen EU-Konzeptpapieren versucht wurde, den Terminus hybride Bedrohung zu definieren, gibt es bislang keine Definition des Begriffs ausländische Einmischung.

Zweitens werden die Abwägungen und deren Konsequenzen zur Einstufung von Angriffen oder Sicherheitsrisiken als hybride Bedrohungen nicht genauer spezifiziert. In der EU wird vor allem über die Verbindung zwischen irregulärer Migration und hybriden Bedrohungen debattiert. Eine Klärung ist auch deshalb notwendig, da diese Debatte bereits auf die Nato und ihr nächstes strategisches Konzept ausstrahlt. Drittens beschränkt sich die Ausgestaltung der breit angelegten EU-Politik zur Stärkung der passiven Widerstandskraft gegenüber hybriden Bedrohungen darauf, bisher nicht genauer definierte »Werkzeugkästen« zu entwickeln. Ein dynamisches, wissenschaftlich fundiertes Verständnis von Resilienz fehlt gänzlich.

In der Diskussion über Deutschlands geplante Nationale Sicherheitsstrategie sollten diese Fehler nicht wiederholt werden. Gleichzeitig ist das Weißbuch von 2016 veraltet, da es konzeptionell und operativ durch die entsprechenden EU-Ansätze zu hybriden Bedrohungen überholt wurde. Eine tiefergehende Auseinandersetzung mit dieser Problematik ist daher dringend angeraten. 2018 wurde eine Arbeitsgruppe für die interministerielle Abstimmung zu hybriden Bedrohungen geschaffen, die seit 2019 vom Bundesministerium des Innern geleitet wird. Bislang fehlt allerdings eine weitergehende Konzeption, um im Föderalismus bzw. auf regionaler Ebene in der EU sowie in Bezug auf die europäische Integration eine kohärente Herangehensweise verfolgen zu können.

Angesichts der ebenenübergreifenden Dynamik hybrider Bedrohungen kann der Prozess hin zu einer Nationalen Sicherheitsstrategie ein wichtiger deutscher Beitrag zu einem gesamteuropäischen Ansatz sein. Im Bereich Medien und Desinformation gibt es bereits zahlreiche Ansatzpunkte für eine enge Verschränkung. Das liegt nicht zuletzt an der sich rasch entwickelnden EU-Gesetzgebung, besonders am Digital Services Act und am Digital Markets Act. Themenübergreifend sollte ein flexibles Verständnis der Subsidiarität angelegt werden. Auf supranationaler Ebene sollten im Rahmen der längst überfälligen Reform des EAD die Vorschläge des Strategischen Kompasses zur nachrichtendienstlichen Auswertungs- und Analysefähigkeit umgesetzt werden. Hierzu könnte die Bundesregierung sowohl die Verstärkte Zusammenarbeit über die GASP-Verfahren nach Artikel 328 und 329 AEUV als auch die Ständige Strukturierte Zusammenarbeit nach Artikel 42 EUV in Erwägung ziehen. Benötigt werden weniger neue Werkzeugkästen, sondern eher eine supranationale Attributionsstelle, um in puncto Verantwortlichkeiten Ross und Reiter zu nennen.

Dr. Annegret Bendiek ist Stellvertretende Leiterin der Forschungsgruppe EU/Europa.
Dr. Raphael Bossong ist Wissenschaftler der Forschungsgruppe EU/Europa.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
DOI: 10.18449/2022A40