Zum Umgang mit hybriden Bedrohungen: auf dem Weg zu einer nationalen Resilienzstrategie

Tamminga, Oliver

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

SWP-Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

Zum Umgang mit hybriden Bedrohungen

Auf dem Weg zu einer nationalen Resilienzstrategie

Oliver Tamminga

Hybride Bedrohungen sind für den betroffenen Staat eine Herausforderung: Es ist für ihn kompliziert, auf sie in angemessener Art und Weise zu reagieren, weil die Angreifenden, die oftmals verdeckt agieren, nur schwer zu identifizieren und zuzuordnen sind. Als eine mögliche Antwort auf hybride Bedrohungen wird in der sicherheitspolitischen Debatte derzeit intensiv das Konzept der Resilienz diskutiert. Es rückt die eigenen Verwundbarkeiten, den Umgang mit Gefahren und Bedrohungen sowie die Instrumente zu deren Bewältigung in den Fokus sicherheitspolitischer Überlegungen. Im Hinblick auf Deutschland geht es also darum, eigene Vulnerabilitäten zu erkennen und zu minimieren und die Widerstandsfähigkeit der Gesellschaft zu erhöhen.

Für die Ausgestaltung der deutschen Sicherheitspolitik sind bisher die konkreten, sich für die Zukunft abzeichnenden Bedrohungen und Gefahren ausschlaggebend gewesen. Das Handeln Deutschlands in diesem staatlichen Aufgabenbereich ist darauf ausgerichtet, Risiken für die eigene Sicherheit möglichst auf Distanz zu halten. Das Konzept der hybriden Bedrohungen fußt jedoch auf einer zunehmenden Komplexität, Grenzenlosigkeit und Diversität von Gefährdungen. Hauptcharakteristikum des ihm zugrundeliegenden Szenarios ist der kombinierte und orchestrierte sowie oft verdeckte Einsatz von militärischen und nichtmilitärischen Mitteln staatlicher und nichtstaatlicher Akteure zur Erreichung politischer Ziele. Das Repertoire der Gegner, die auf solche Weise operieren, reicht von der konventionellen und unkonventionellen Kriegsführung über organisierte Kriminalität, Propaganda, Desinformation, Aktionen im Cyber-Raum, Instrumentalisierung des Protestpotentials von gesellschaftlichen Minderheiten bis hin zu Terroranschlägen. Alle Politik- und Wirtschaftsbereiche sind potentiell betroffen. In einer solchen komplexen Gefahrenlage ist es nicht mehr sinnvoll, das sicherheitspolitische Handeln primär darauf auszurichten, die Vielzahl hybrider Bedrohungen zu verhindern. Ziel muss es stattdessen sein, auf eine Verminderung der eigenen Verwundbarkeit hinzuarbeiten.

Das setzt zunächst eine Analyse der eigenen Defizite und Vulnerabilitäten in Staat und Gesellschaft voraus, also der möglichen Angriffsziele. Im Falle der Ukraine während der Hochphase des Konflikts waren dies zum Beispiel politische Instabilität, schwache Regierungsführung, Korruption, eine instru-

Oberstleutnant i.G. Oliver Tamminga ist Wissenschaftler in der Forschungsgruppe Sicherheitspolitik

mentalisierbare russischsprachige Minderheit, mangelndes Vertrauen der Bürger in die staatlichen Sicherheitskräfte und die Abhängigkeit von russischen Gaslieferungen.

Bedrohung vs. Vulnerabilität

Durch den Perspektivwechsel von äußeren Bedrohungen hin zu inneren Verwundbarkeiten geraten die komplexen und störanfälligen Schwachstellen einer Gesellschaft in den Fokus der staatlichen Sicherheitsvorsorge. Potentielle Ziele hybrider Angriffe sind die Vitalfunktionen eines Staates. Dazu zählen die Wirtschaft, gerade jene Sektoren, wo Abhängigkeiten existieren, die informations- und kommunikationstechnischen Systeme, insbesondere der Cyber-Raum, die kritischen Infrastrukturen im Bereich des Finanzwesens, der Energie und Logistik und auch die Institutionen zur gesellschaftlichen Integration von Minderheiten. Die gerade in diesen Sektoren vorhandenen Interdependenzen eröffnen einem Gegner ungeahnte Möglichkeiten. Das gilt vor allem für den Bereich der kritischen Infrastrukturen und hier speziell für die Informationstechnologie. Deren Funktionsfähigkeit kann unter anderem durch technische Unfälle, menschliches Versagen, Angriffe aus dem Cyber-Raum, Kriminalität, Sabotage oder Terrorismus gefährdet sein.

Damit wird die Frage, ob die eigenen Systeme und Strukturen hinreichend anpassungs- und widerstandsfähig sind, für die Staaten immer wichtiger. Das Bundesministerium des Innern hat in der »Nationalen Strategie zum Schutz Kritischer Infrastrukturen« sogenannte technische Basisinfrastrukturen wie zum Beispiel Energieversorgungs-, Informations- oder Verkehrssysteme für besonders schutzbedürftig erklärt. Deren Sicherheit und uneingeschränkte Verfügbarkeit ist eine wesentliche Voraussetzung für die Aufrechterhaltung unseres Wirtschaftssystems und unserer Lebensweise und damit für die Gewährleistung des Wohlstands in Deutschland.

Daher haben der Bund und die Länder in unterschiedlichen Vorsorge- und Sicherstellungsgesetzen, im Zivilschutzgesetz, in den Katastrophenschutzgesetzen sowie in den Rettungsdienstgesetzen Regelungen getroffen, die Behörden und öffentliche Einrichtungen in einem Katastrophenfall befähigen sollen, gemeinsam den Schutz der Bürger zu gewährleisten. Der Großteil der kritischen Infrastrukturen wird gleichwohl von privatwirtschaftlichen Unternehmen betrieben. Für diese bestehen, neben den Vorgaben des IT-Sicherheitsgesetzes, derzeit aber kaum gesetzliche Regelungen. Vielmehr setzt der Bund beim Schutz kritischer Infrastrukturen, zum Beispiel vor einem »Blackout«, auf eine freiwillige Selbstverpflichtung der Unternehmen und behält sich nur im Ausnahmefall ein staatliches Eingreifen vor.

Insbesondere der Ausfall von Informationsinfrastrukturen oder schwerwiegende Angriffe im Cyber-Raum können zu erheblichen Beeinträchtigungen der technischen, wirtschaftlichen und administrativen Leistungsfähigkeit Deutschlands führen. Die Auswirkungen dieser Störungen können sich zu einem Sicherheitsrisiko ausweiten. In den letzten Jahren sind die Attacken immer zahlreicher, komplexer und professioneller geworden. Cyber-Angriffe stehen dabei oftmals im Zusammenhang mit aktuellen Konflikten. So hat beispielsweise eine prorussische Gruppe von Hackern aus der Ukraine namens »CyberBerkut« in der Vergangenheit erfolgreich Internetseiten der deutschen Bundesregierung als »Vergeltung« für deren politische Unterstützung der Ukraine attackiert. Ein weiteres Beispiel ist die sogenannte »Syrische Elektronische Armee«, eine Gemeinschaft von Hackern, angeblich mit Verbindungen zum syrischen Regime, die schon mehrfach die Internetpräsenz westlicher Medien angegriffen hat.

Resilienz als Antwort?

Kommt es zu einer Attacke der beschriebenen Art, so ist für den betroffenen Staat oder die betroffene Gesellschaft zunächst oft unklar, aus welcher Richtung sie erfolgt, wer der Angreifer ist und welche (politischen) Ziele er hat. Ein militärisches Gegen-

handeln ist zumeist nicht oder nur schwer möglich. Hybriden Bedrohungen kann daher nicht ausschließlich mit militärischen Mitteln begegnet werden, auch wenn eine glaubhafte und sichtbare Abschreckung und Abwehr- bzw. Verteidigungsbereitschaft eine wichtige Komponente ist und bleibt, um einen potentiellen Angreifer von seinem Vorhaben abzubringen und zu entmutigen. Es bedarf daher eines umfassenden und gesamtstaatlichen Ansatzes, der alle relevanten Akteure, inklusive der Zivilgesellschaft und der privatwirtschaftlichen Unternehmen, einbezieht. Genau hier setzt das Konzept der Resilienz an. Der ihm zugrundeliegende Kerngedanke ist keinesfalls neu, sondern findet sich bereits im deutschen Konzept der »Gesamtverteidigung« oder in dem der »Umfassenden Landesverteidigung« bzw. der »Umfassenden Sicherheitsvorsorge« in Österreich wieder.

Im sicherheitspolitischen Diskurs bezeichnet Resilienz die Widerstandsfähigkeit von Gesellschaften und politischen Systemen. Resilienz ist demnach die Fähigkeit einer Gemeinschaft oder einer Gesellschaft, Gefahren, denen sie ausgesetzt ist, und deren Folgen in angemessener Zeit und wirksam zu bewältigen bzw. sich ihnen anzupassen und sich von ihnen zu erholen, und zwar so, dass die lebensnotwendigen Grundstrukturen und Basisfunktionen bewahrt oder wiederhergestellt werden. Resilienz bezeichnet somit keinen System*zustand*, sondern eine System*eigenschaft*, die ständig aufrechterhalten und neu erworben werden muss. Sie ist also mehr als die Vorbereitungs- und Bereitschaftskomponente einer Sicherheitspolitik; sie ist vielmehr ein systematischer und holistischer Ansatz zur Bewältigung sicherheitspolitischer Gefahren. Mit dem Konzept werden bestehende Ansätze nicht etwa abgelöst, sondern der Blick wird für eine integrierte Betrachtung geweitet.

Trotz der aktuellen politischen Popularität des Resilienz-Konzepts sind die Anforderungen, die sich daraus ergeben, bisher nur in unzureichendem Maße systematisiert und operationalisiert und die sich daraus ergebenden sicherheitspolitischen Implikationen noch wenig beleuchtet worden. Zum einen werden, je nach Anwendungsgebiet, unterschiedliche Definitionen von Resilienz vertreten. Zum anderen fehlt es bisher noch an einer allgemeingültigen Festlegung der Forschung, wie Resilienz zu messen ist. Eine Messbarkeit von Resilienz setzt voraus, dass diese beobachtet und Werte systematisch zugeordnet werden können. Die Erfassung von Resilienz ist aber Voraussetzung für die Entwicklung effektiver Strategien, für das Ergreifen von Maßnahmen zur Vorbeugung oder Schadensminderung und für die Verteilung von Ressourcen.

Zudem bedeutet Resilienz auch immer, dass die Verantwortung für die Bewältigung von sicherheitspolitisch relevanten Ereignissen zu einem Teil auf die Bevölkerung oder auf privatwirtschaftliche Unternehmen übergeht und damit auch in höherem Maß gewisse Selbstverpflichtungen einhergehen. Der verstärkte Rückgriff auf nichtstaatliche Akteure und Strukturen wirft aber eine Reihe von Fragen im Hinblick auf die Beziehung zwischen Staat und Bürger auf: Welche Rolle nimmt der Staat zukünftig in der Sicherheitsvorsorge wahr? Welches Maß an Eigenverantwortung kann den Akteuren zugemutet bzw. abverlangt werden? Zur Beantwortung dieser Fragen ist ein öffentlicher Diskurs über Sicherheitsvorsorge, Risiken, Gefährdungen und Verwundbarkeiten zwischen allen relevanten politischen, wissenschaftlichen, wirtschaftlichen und gesellschaftlichen Gruppen sowie anderen Akteuren erforderlich. Gleichzeitig kann ein offener Dialog zwischen Bürgern und Staat über Risiken und Verwundbarkeiten paradoxerweise auch zu einem mehr an Unsicherheit führen, da als Begleiteffekt ein möglicher Angreifer besser einschätzen kann, an welchen Stellen er ansetzen muss, um seine Ziele möglichst leicht zu erreichen.

Auf dem Weg zu mehr Resilienz

Zunächst ist eine Bestandsaufnahme erforderlich, welche bereits vorhandenen Struk-

turen, Einrichtungen und Instrumente resilienzfördernd sind. So gibt es in Deutschland durchaus bereits Institutionen, die zur Resilienz beitragen, beispielsweise das Gemeinsame Melde- und Lagezentrum von Bund und Ländern im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, das Bundesamt für Sicherheit in der Informationstechnik, die Nachrichtendienste, die Polizeien, die Bundeswehr und ihre Reservisten, die (Freiwilligen) Feuerwehren, das Technische Hilfswerk, die Hilfs- und Rettungsorganisationen, die karitativen Verbände und bestimmte Nichtregierungsorganisationen. Auch Formen des ehrenamtlichen freiwilligen Engagements und eine unabhängige und pluralistische Medienberichterstattung gehören dazu. Zudem muss durch die Politik definiert werden, welches Maß an Resilienz überhaupt erreicht werden soll, das heißt, welche Bedrohungen und Gefährdungen akzeptiert werden können bzw. müssen. Wenn zusätzliche Resilienz erforderlich ist, bedarf es eines überparteilichen politischen Konsenses, da die Formulierung eines solchen Ansatzes hochpolitisch ist und die Ressourcen endlich sind. Konzepte von einzelnen Ressorts sind hier nicht ausreichend.

Risiken und Bedrohungen abschätzen Um auf hybride Bedrohungen reagieren zu können, sind Fähigkeiten zur vernetzten Risikoidentifikation, Krisenfrüherkennung und Gefahrenanalyse von grundlegender Bedeutung. Nur durch operationalisierbare Kenngrößen ist es möglich, Vulnerabilitäten zu erkennen und zu messen. Um die Resilienz zu erhöhen, ist es von entscheidender Wichtigkeit zu wissen, wie anfällig Deutschland für bestimmte Risiken und Bedrohungen ist. Die deutsche Sicherheitsforschung sollte sich daher interdisziplinär der Entwicklung erforderlicher Metriken und Indikatoren annehmen. Auf der Basis der Ergebnisse sollten dann bestehende Modellierungsansätze erweitert und »Stress-Tests«, bestehende Frühwarn- und Meldesysteme fortentwickelt werden.

Nationale Resilienzstrategie formulieren Weder die EU noch die Nato verfügen gegenwärtig über eine Strategie zum Umgang mit hybriden Bedrohungen, und da diese sich bevorzugt gegen die spezifischen Schwachstellen eines Staates bzw. einer Gesellschaft richten, sehen sowohl die EU als auch die Nato zuvorderst die Mitgliedstaaten in der Verantwortung, auf diese Bedrohungen zu reagieren und die Resilienz zu erhöhen. Gleichwohl können die EU und die Allianz dabei helfen, die Effektivität der nationalen Anstrengungen zu steigern, indem sie beispielsweise gemeinsame Standards (etwa im Cyber-Bereich) festlegen oder der Gemeinschaft Informationen im Rahmen der Krisenfrüherkennung und Gefahrenanalyse bereitstellen.

Die jüngsten Terroranschläge in Paris am 13. November 2015 zeigen zudem, dass die Bewältigung einer solchen Katastrophe zunächst eine nationalstaatliche Aufgabe ist. Ein erklärtes Ziel der Bundesregierung sollte es daher sein, ein gesamtstaatliches Konzept zum Umgang mit hybriden Bedrohungen und zur Operationalisierung von Resilienz zu entwickeln. Eine solche Strategie würde das Maß an angestrebter Resilienz in Deutschland definieren und das Umfeld, die Verwundbarkeiten und die Bedrohungen analysieren. Sie müsste aufzeigen, wo Deutschland am verwundbarsten ist, welche Akteure oder Objekte resilient sein müssen und entsprechende Ziele und Prioritäten vorgeben. Durch die Benennung von Ressourcen, Verantwortlichkeiten und Instrumenten müsste sie darlegen, wie Resilienz in unterschiedlichen staatlichen und gesellschaftlichen Handlungs- und Lebensbereichen erreicht bzw. gesteigert werden kann. Der Mehrwert einer solchen gesamtstaatlichen und interdisziplinären Resilienzstrategie läge darin, dass zum einen für verschiedene Handlungsfelder vergleichbare und vor allem verbindliche Maßstäbe festgelegt werden. Zum anderen würde ein höheres Maß an Koordination zwischen den verschiedenen Ressorts und relevanten Akteuren ermöglicht und vorgeschrieben.

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 1611-6364

Lektüreempfehlung
Claudia Major/Christian Mölling, *Eine hybride Sicherheitspolitik für Europa. Resilienz, Abschreckung und Verteidigung als Leitmotive*, SWP-Aktuell 31/2015