SCHWERPUNKTTHEMA

Vernetzte Sicherheit – eine Herausforderung für Bund, Länder und Kommunen

Angesichts konkreter Terrorgefahren, die nicht nur mögliche reale Anschläge, sondern auch Attacken im Cyber-Raum umfassen, ist Sicherheit nicht mehr nur die Sache von Polizei und Militär. Durch das Konzept der vernetzten Sicherheit werden letztlich die gesamte öffentliche Verwaltung, die Wirtschaft und die Zivilgesellschaft in die Pflicht genommen. Das neue sicherheitspolitische Weißbuch der Bundeswehr ist Anlass, sich über die Folgen vor allem für die öffentliche Verwaltung Gedanken zu machen.

Die jüngsten Terroranschläge in Europa – unter anderem in Manchester und London sowie die Online-Attacke „Wannacry"– rücken die Debatte um innere Sicherheit immer stärker in den Vordergrund. Die Besorgnis der Bürger wächst. In 2016 hatten nach einer repräsentativen Studie 73 Prozent der Befragten in Deutschland Angst vor Terrorismus – und damit 21 Prozent mehr als noch im Vorjahr.[1] Die offenbare Verschärfung der Sicherheitslage zeigt, wie notwendig es ist, die aktuellen Sicherheitskonzepte neu auf die veränderte Gefährdungssituation auszurichten. „Klassische" Terrorangriffe sind jedoch nicht die einzige Gefahrenquelle, wenngleich sie zurzeit andere potenzielle Gefahrenquellen in der öffentlichen Wahrnehmung überlagern. Auch Betriebsstörungen im infrastrukturellen Bereich oder Naturkatastrophen können die öffentliche Sicherheit gefährden und verlangen nach einem systematischen Vorgehen in der Prävention und Reaktion. Systematische Sicherheitsstrategien sind ebenso für Großveranstaltungen notwendig, bei denen die Unversehrtheit von Besuchern und Bewohnern zu gewährleisten ist – etwa im Sport oder in der Politik, wie jüngst beim G20-Gipfel in Hamburg.

Eine Vernetzung ist sowohl ressort- als auch ebenenübergreifend gefragt

In der internationalen Sicherheitspolitik hat sich das Konzept der „Vernetzten Sicherheit" etabliert (siehe auch Seite 7). Zum einen umfasst dieses eine Kooperation der verschiedensten Behördenressorts und -ebenen in Bund, Ländern und Kommunen. Zum anderen spielt Vernetzung in unterschiedlichsten Bereichen und bei verschiedensten Themenfeldern eine Rolle, die auch das Bundesministerium der Verteidigung im neuen Weißbuch hervorhebt. Städte und Gemeinden sind wichtige Akteure für die Gewährleistung von innerer Sicherheit, nehmen jedoch in der öffentlichen Debatte einen scheinbar untergeordneten Rang ein. Im Folgenden betrachten wir daher, welche Voraussetzungen gegeben sein müssen, damit das Konzept „Vernetzte Sicherheit" insbesondere unter Einbeziehung der Kommunen fruchtbar sein kann. Außerdem beschäftigen wir uns mit dem gemeinsamen „Lernen", also dem Austausch von Wissen und Informationen. Ebenfalls im Fokus steht das gemeinsame „Handeln", also die praktische Ausgestaltung der Zusammen-

1 R+V Versicherung (2016): Die Ängste der Deutschen 2016

© kaicologne/fotolia

arbeit in präventiver Hinsicht sowie bei der Reaktion auf Gefahren am Beispiel von „Kritischen Infrastrukturen".

„Nationale Gestaltungsfelder" im Bundeswehr-Weißbuch

Das 2016 veröffentlichte „Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr" nimmt eine strategische Standort- und Kursbestimmung für die deutsche Sicherheitspolitik vor.[2] Der Vergleich mit dem letzten Weißbuch 2006 zeigt, dass Deutschlands sicherheitspolitisches Umfeld in den vergangenen Jahren deutlich komplexer, dynamischer und damit schwieriger vorhersehbar geworden ist. Auch hat sich der Aufgabenzuschnitt der Bundeswehr ausgeweitet: Der Bogen reicht dabei von einer veränderten Gewichtung in der Landes- und Bündnisverteidigung und neuen Aufgaben im Rahmen der Flüchtlingshilfe über Aufgaben der Terrorbekämpfung bis hin zur Auseinandersetzung in hybriden und asymmetrischen Bedrohungs- und Einsatzszenarien. Zu den neuen Aufgaben wird auch der Einsatz der Bundeswehr im Inland gezählt, zudem werden Herausforderungen aus dem Cyber-Raum genannt – etwa Wirtschaftsspionage und die Schädigung „Kritischer Infrastrukturen". Im April 2017 nahm das neue Bundeswehrkommando „Cyber- und Informationsraum" seine Arbeit auf. Das Weißbuch regt die Harmonisierung von Krisenbewältigung über verschiedene Ebenen in einem gesamtgesellschaftlichen Dialog an und fordert eine Sicherheitspartnerschaft von Staat, Wirtschaft und Wissenschaft. Daher richten sich die Leitlinien auch über die Bundeswehr hinaus an die gesamte Bundesregierung als eine Aufgabe für „alle Bereiche der Gesellschaft"[3].

Das Bundeswehr-Weißbuch definiert Sicherheit als gesamtgesellschaftliche Aufgabe und formuliert Resilienz als wesentliches Ziel

Die Gestaltungsfelder, die das Weißbuch auf nationaler Ebene definiert, reichen vom Ausbau der Strategiefähigkeit und der Gestaltung einer nachhaltigen Sicherheit über die Entwicklung des vernetzten Sicherheitsansatzes bis hin zu den gesamtgesellschaftlich wichtigen Aufgaben der Sicherheitsvorsorge und der Resilienz. Als Resilienz wird die Fähigkeit verstanden, die „Widerstands- und Adaptionsfähigkeit von Staat und Gesellschaft gegenüber Störungen – etwa Umweltkatastrophen, schwerwiegende Systemfehler und gezielte Angriffe"[4] – auszubauen.

„Vernetzte Sicherheit": Austausch, Durchlässigkeit und Einheitlichkeit

Das Konzept der „Vernetzten Sicherheit" wurde erstmals 2006 im Weißbuch des Bundesministeriums der Verteidigung offiziell eingeführt. Der Begriff geht davon aus, dass die künftige sicherheitspolitische Entwicklung nicht nur durch militärische Konstellationen beeinflusst wird, sondern auch durch gesellschaftliche, ökonomische, ökologische und kulturelle Bedingungen: „Sicherheit kann deshalb weder rein

2 Darüber hinaus gibt es zum Thema Sicherheit und Bevölkerungsschutz eine ganze Reihe an Konzepten des Bundesministerium des Innern, etwa die in 2016 beschlossene „Konzeption Zivile Verteidigung" (KZV).

3 Vgl. Bundesministerium der Verteidigung (2016): Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr, S. 17

4 Vgl. ebenda, S. 49

national noch allein durch Streitkräfte gewährleistet werden. Erforderlich ist vielmehr ein umfassender Ansatz, der nur in vernetzten sicherheitspolitischen Strukturen sowie im Bewusstsein eines umfassenden gesamtstaatlichen und globalen Sicherheitsverständnisses zu gewährleisten ist."[5]

„Vernetzte Sicherheit" wird oftmals auch synonym als „Comprehensive Approach" bezeichnet – ein von der NATO geprägter Begriff, der auf die Interdependenzen zwischen zivilen und militärischen Instrumenten verweist. Das Konzept gründet im Wesentlichen auf einem raschen Austausch über hierarchische Ebenen hinweg. Dieser stellt verschiedene Anforderungen: unter anderem eine Durchlässigkeit zwischen den involvierten Institutionen und Fachressorts, ein einheitliches Lagebild aller Beteiligten, Zugang zu moderner Informations- und Kommunikationstechnologie und die Ausnutzung ihrer Vorteile – aber auch ein Verständnis für deren Verwundbarkeit (Cyber Crime/Cyber Warfare). Vor allem in dem aktuellen Weißbuch wird die besondere Rolle der Gesamtgesellschaft für die Sicherheitspolitik hervorgehoben, wodurch nun auch die Zivilgesellschaft zu einem wesentlichen Akteur für Sicherheit wird. Das tägliche Leben der Zivilgesellschaft spielt sich an den Wohnorten ab – somit liegt eine besondere Verantwortung bei der Gewährleistung von Sicherheit gerade auch bei den Kommunen. Auch zivilgesellschaftliche Gruppierungen, die sich zum Beispiel für Themen wie Integration oder Prävention engagieren, werden so quasi zu Akteuren im Dienste der Sicherheit, wenngleich sie sich selbst kaum so einstufen würden. Ob der neue Blick auf die Zivilgesellschaft mit neuen Verpflichtungen einhergeht, etwa zur Weiterleitung von Informationen an Behörden, bleibt abzuwarten.

Die Kommunen spielen eine wichtige Rolle für die Gewährleistung von Sicherheit

Gemeinsames Lernen: übergreifende Wissensgrundlagen schaffen

Die gemeinsame Ausbildung und die gemeinsame Durchführung von Übungen von staatlichen und nicht staatlichen Akteuren benennt das Weißbuch als Maßnahme, um den vernetzten Ansatz weiterzuentwickeln.

Die Zuständigkeiten für innere Sicherheit sind seit jeher ebenenübergreifend ausgestaltet. So liegen beim Bund etwa das Bundeskriminalamt, das Bundesamt für Verfassungsschutz und die Bundespolizei, während bei den Ländern die überwiegenden Polizeikräfte und die jeweiligen Landeskriminal- bzw. Verfassungsschutzämter angesiedelt sind. In den Zuständigkeitsbereich der kommunalen Hand fallen der Bereich des Feuerschutzes und die kommunalen Ordnungsämter. Dagegen sind Fragen der äußeren Sicherheit – also Landesverteidigung, nationale und internationale Nachrichtengewinnung, Grenzschutz, Terrorismusabwehr etc. – ausschließlich beim Bund angesiedelt.

Gemeinsame Datenbanken oder einheitliche IT-Systeme bislang nur in wenigen Bereichen etabliert

Da Informations- und Wissensaustausch mittlerweile überwiegend digital erfolgt, setzt dies einheitliche und von allen gleichermaßen handhabbare Instrumentarien voraus – in technischer Hinsicht etwa gemeinsame Datenbanken. Der BOS-Digitalfunk ist ein solches Instrument, das über einen einheitlichen Standard die gemeinschaftliche Kommunikation aller „Behörden und Organisationen mit Sicherheitsaufgaben" (BOS) erlaubt. Einsatzkräfte der Polizeien, Feuerwehren, Rettungsdienste sowie weiterer Zivil- und Katastrophenschutzorganisationen können sich über diesen Funk organisationsübergreifend und bundesweit verständigen. Gemeinsame Arbeitssysteme wie etwa eine bundesländerübergreifende IT gibt es jedoch noch nicht. So läuft die Zusammenarbeit der insgesamt 40 für die innere Sicherheit zuständigen Bundes- und Landesbehörden im Gemeinsamen Terrorabwehrzentrum (GTAZ) laut Berliner Innensenator über insgesamt 19 unterschiedliche IT-Systeme der kooperierenden Behörden.[6]

5 Vgl. Bundesministerium der Verteidigung (2006): Weißbuch 2006 zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr, S. 29

6 Berliner Morgenpost (2017): Mit 12.000 Pistolen will Senator Geisel Berlin schützen, Interview mit Innensenator Andreas Geisel, 5.3.2017

Um einen gemeinsamen Wissensstand der unterschiedlichen für die Sicherheit zuständigen Akteure zu schaffen, kann der erste Ansatzpunkt bereits die Ausbildung sein. So propagiert das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) eine „mehrdimensionale Vernetzung" im Bereich der Aus- und Fortbildung. Bestehende Bildungseinrichtungen sollten miteinander kooperieren, um „ganzheitlich denkende Risiko- und Krisenmanager" bereitstellen zu können.[7] Beispiele dafür, wie voneinander gelernt und Neues entwickeln werden könnte, böten etwa die Landesfeuerwehrschule Niedersachsen, die JUH-Akademie (Johanniter-Akademie) Münster, die THW-Bundesschule oder das Institut der Feuerwehr NRW.

Die Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ) als eine Abteilung des BBK richtet sich etwa an Entscheider aller Verwaltungsebenen im Bereich der zivilen Sicherheit. Im Jahr 2013 wies diese darauf hin, dass die kreisangehörigen Kommunen „keineswegs frei von einer Mitwirkung im Bevölkerungsschutz" seien[8]. Da dies jedoch oft übersehen werde, spielten die Gemeinden in Übungen oft keine Rolle, obwohl die Vorbereitung auf den Ernstfall die Pflicht auch „auf der untersten Verwaltungsebene"[9] sei. Durch Seminare zum Bevölkerungsschutz speziell für kommunale Entscheidungsträger wolle die AKNZ gerade der Verantwortung der Kommunen begegnen.

Gemeinsames Handeln: Sicherheitspartnerschaften für Kritische Infrastrukturen bilden

Eine wichtige Funktion vorsorgender Sicherheitspolitik ist unter anderem der Schutz von „Kritischen Infrastrukturen" (KRITIS), die die Bevölkerung mit lebenswichtigen Gütern und Dienstleistungen versorgen. Neben den Sektoren Energie und Gesundheit zählen etwa Informationstechnik und Telekommunikation sowie die Wasserversorgung zu den betroffenen Bereichen. Resilienzaufbau steht hierbei daher für den Auftrag, diese lebensnotwendigen Versorgungssysteme für den Krisenfall widerstandsfähiger zu machen. Die Sicherheitsvorsorge bedarf laut AKNZ eines koordinierten Konzepts und der Kooperation – sowohl horizontal als auch ebenenübergreifend zwischen Bund, Land und Kommune[10] unter Einbeziehung weiterer zivilgesellschaftlicher Akteure.

Die Sicherheit Kritischer Infrastrukturen entscheidet sich wesentlich in den Kommunen

Terroristische Anschläge, Naturkatastrophen oder Betriebsstörungen sind nur einige von möglichen Gefahrenpotenzialen von Kritischen Infrastrukturen. Kommunen sind hierbei einerseits „Standort der Infrastrukturen und häufig (Mit-)Betreiber zum Beispiel in Form von städtischen Unternehmen", andererseits spürt gerade die kommunale Bevölkerung die Auswirkungen von Ausfällen und Störungen unmittelbar.[11] Darüber hinaus stellen auch Staat und Verwaltung selbst Kritische Infrastrukturen dar. Kommunen sollten daher den Kern ihrer eigenen Verwaltung als eine Kritische Infrastruktur ansehen, für die sie ein eigenes Krisenmanagement etablieren müssen.[12]

Die kommunale Ebene ist gemäß der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen" neben Bund und Ländern für deren Schutz verantwortlich. Sie wird demnach aufgefordert, die „Zusammenarbeit zwischen Staat und Wirtschaft zu intensivieren und zu verzahnen"[13]. Da die meisten Infrastrukturen nicht oder nur teilweise in kommunalem Besitz sind und damit außerhalb der kommunalen Entscheidungsbefugnis liegen, müssen die privatwirtschaftlichen Infrastrukturbetreiber sowohl

7 Vgl. Karsten, A. (2009): Ganzheitlich denkende Risiko- und Krisenmanager. Mittels Kooperationen von Bildungseinrichtungen die neuen Herausforderungen bestehen. Bevölkerungsschutz 3/2009

8 Akademie für Krisenmanagement, Notfallplanung und Zivilschutz AKNZ (2013): Jahresprogramm 2013, S. 12 f

9 Ebenda

10 Vgl. ebenda

11 Vgl. Bundesamt für Bevölkerungsschutz/Deutscher Städtetag (2010): Drei Ebenen, ein Ziel: Bevölkerungsschutz – gemeinsame Aufgabe von Bund, Ländern und Kommunen, S. 25

12 Vgl. Deutscher Städte- und Gemeindebund (2014): Bevölkerungsschutz in Städten und Gemeinden, DStGB DOKUMENTATION NO 123, S. 27

13 Bundesamt für Bevölkerungsschutz/Deutscher Städtetag (2010): Drei Ebenen, ein Ziel: Bevölkerungsschutz – gemeinsame Aufgabe von Bund, Ländern und Kommunen, S. 25

vorsorgend als auch bei der Krisenbewältigung aktiv werden. Bei der Analyse möglicher Schwachstellen sowie bei entsprechenden Vorsorgemaßnahmen sollten Staat und Kommunen eng mit den Betreibern zusammenarbeiten und gemeindeübergreifende Netzwerke bilden.[14] Ein passendes Format für die Zusammenarbeit kommunaler Stellen und lokaler Wirtschaft können Arbeitskreise oder Gespräche am runden

14 Vgl. Bundesamt für Bevölkerungsschutz/Deutscher Städtetag (2010): Drei Ebenen, ein Ziel: Bevölkerungsschutz – gemeinsame Aufgabe von Bund, Ländern und Kommunen, S. 25

„Für nachhaltige Sicherheit brauchen kommunale Entscheider umfassende Informationen"

Interview mit Hartfrid Wolff

Das Konzept der „Vernetzten Sicherheit" wird nicht erst seit Erscheinen des Bundeswehr-Weißbuches von 2016 diskutiert. In welchen Bereichen muss noch stärker als bisher vernetzt gedacht und agiert werden?
Hartfrid Wolff: Großschadenslagen, wie etwa ein flächendeckender Stromausfall, machen nicht vor Bundesländergrenzen halt. Insofern ist die Vernetzung von Akteuren, Kompetenzen und Standards im Rahmen einer „Vernetzten Sicherheit" dringend notwendig. Kooperationsmodelle gibt es zwar bereits, etwa zwischen Bund und Ländern. Das Gemeinsame Terrorabwehrzentrum GTAZ ist ein Beispiel (siehe auch Seite 11). Der Terroranschlag Ende 2016 in Berlin hat jedoch gezeigt, dass auch diese Plattform schnell an Grenzen stößt. Es fehlen noch Grundlagen für die systematische Zusammenarbeit wie einheitlichere Ausbildungsstandards, Standards zum Informations- und Datenmanagement, zum Umgang mit datenschutzrechtlichen Implikationen oder auch technische Standards. Wünschenswert wäre daher etwa im Bereich des Katastrophenschutzes ein „Inspekteur für den Bevölkerungsschutz", der von den Ländern besetzt wird, um eine systematische Kommunikation und Ressourcenplanung sowie Standards für Länder und Bund zu entwickeln.

Das Weißbuch geht auch auf die sicherheitspolitische Verantwortung der Zivilgesellschaft ein. Welche Rolle spielen etwa NGOs künftig für die innere Sicherheit?
Die Bedeutung ehrenamtlicher Organisationen und der Zivilgesellschaft für die Sicherheit in Deutschland ist sehr groß. Die Rettungsorganisationen, seien es die „weißen Kräfte", die Feuerwehren, das THW oder die DLRG, werden vor Ort häufig sogar fast ausschließlich von Ehrenamtlichen getragen. Ebenso sind NGOs wie zum Beispiel Vereine und Selbsthilfegruppen, Nachbarschaftshilfen, Arbeitnehmerorganisationen und Kirchen entscheidende Träger für den Zusammenhalt der Gesellschaft mit wesentlichen präventiven Aufgaben.

Hartfrid Wolff ist bei der KPMG AG Wirtschaftsprüfungsgesellschaft verantwortlich für Sicherheitsthemen im öffentlichen Sektor. Der Rechtsanwalt und ehemalige Bundestagsabgeordnete ist außerdem Beiratsmitglied des Deutschen Feuerwehrverbands sowie Gründer des Zukunftsforums Öffentliche Sicherheit.

Was muss die Politik beachten, wenn zivile Akteure künftig verstärkt Sicherheitsaufgaben unterstützen?
Wenn nicht institutionell organisierte Akteure beim Thema Sicherheit eingebunden werden, bedarf es einer klaren Strategie. Facebook-Gruppen, die sich zur Unterstützung der Rettungskräfte etwa bei Hochwasserlagen einbringen, sind Chance und Herausforderung zugleich. Die geschulte Hilfeleistung durch ausgebildete Kräfte kann nur ergänzt, aber nie ersetzt werden. Zu überlegen ist, wie institutionelle Kräfte das Engagement von Bürgern besser aufnehmen können, um dieses bestmöglich für das Gemeinwesen zu nutzen.

Welche Weiterentwicklungsmöglichkeiten sehen Sie für die vernetzte und sichere Kommune von morgen?
Die kommunalen Entscheider treffen hochwichtige Entscheidungen für die Sicherheit ihrer Bevölkerung. Sie sollten dies auf Basis umfassender Informationen tun können. Wichtige Überlegungen sind etwa, wie Entscheider vor Ort mehr Informationen über die Sicherheitslage erhalten können, wie eine Verknüpfung mit den Landessicherheitsbehörden ausgebaut und gesellschaftliche Entwicklungen besser prognostiziert werden können. Auch digitale Lösungen wie eine logistisch ausgerichtete Leitstellentechnik, vernetzt mit Sprachcomputern, Geo- und Wetterdaten, können neue Chancen für die Sicherheit und Rettung von Menschen bringen. Auch die Verkehrsleitung kann dazu beitragen, Gefahren abzuwehren – etwa bei sicheren Schulwegen oder sicherheitsrelevanter Sensorik auf Radwegen.

Tisch sein. Zudem ließen sich bestehende Kooperationsformate – wie beispielsweise IHK-Ausschüsse oder Planungsgremien zur interkommunalen Zusammenarbeit – um das Thema KRITIS-Sicherheit ergänzen.[15]

Auch innerhalb des öffentlichen Sektors ist Kooperation notwendig: Ebenso wie auf Bundes- oder Landesebene wird auf kommunaler Ebene empfohlen, eine koordinierende Stelle einzurichten, um die Zusammenarbeit verschiedener Ämter und Fachbereiche zu fördern – zum Beispiel die Ordnungs- und Gesundheitsämter oder Ämter für Brand-, Katastrophenschutz und Rettungsdienste.[16] Die Bundesregierung spricht im Weißbuch von behördenübergreifenden „Lage- und Organisationszentren". Auf Bundes- und Landesebene ist dafür ein Beispiel das 2004 in Berlin gegründete Gemeinsame Terrorabwehrzentrum GTAZ, das als Kooperations- und Kommunikationsplattform fungiert. Die Kooperation wird vom GTAZ als „Zusammenarbeit auf Augenhöhe" beschrieben; die Organisation hat dementsprechend keinen Leiter. Nach dem Terroranschlag eines Tunesiers auf dem Berliner Weihnachtsmarkt in 2016 forderte der Bundesinnenminister, der Bund brauche eine „Steuerungskompetenz über alle Sicherheitsbehörden", wenn es um Angelegenheiten der Sicherheit des Bundes ginge.[17]

Viele Akteursgruppen – Wirtschaft, Behörden und Zivilgesellschaft – sind an Maßnahmen für Schutz und Prävention beteiligt

Ein relevanter Akteur für den Schutz von Kritischen Infrastrukturen kann neben Wirtschaft und Behörden auch die Zivilbevölkerung selbst sein: Angelehnt an bereits bestehende Projekte verschiedener Rot-Kreuz-Gliederungen (zum Beispiel „Team Mecklenburg-Vorpommern", „Team Bayern") könnten fachkundige Bürger als zusätzliche Unterstützung für den Katastrophenfall dienen. Die Fähigkeiten der Freiwilligen würden in Informationssystemen hinterlegt werden und die Kommunikation mit ihnen könnte im Bedarfsfall über soziale Netzwerke geschehen.[18]

Bei der Präventionsarbeit muss neben dem Blick auf den Schutz möglicher Ziele das Augenmerk auf die potenziellen Gefahrenquellen gerichtet werden: NGOs oder andere Vereinigungen mit ihren vielfältigen Kompetenzen können hierbei unterstützend wirken. Nutzerorganisationen von Internetaktivisten können so etwa Sicherheitsdefizite bei Kritischen Infrastrukturen offenlegen. So spürten Aktivisten beispielsweise Lücken auf bei Kritischen Infrastrukturen wie etwa Kraftwerken, die wegen fehlendem Schutz von außen hätten manipuliert werden können. Ihr Wissen teilten die Aktivisten den Behörden mit, die wiederum die lokalen Betreiber über die Sicherheitslecks informierten.[19] Bei der Einbindung von Freiwilligen ist jedoch zu beachten, dass das Gewaltmonopol des Staates gewahrt bleibt und die hoheitliche Gefahrenabwehr somit nicht auf Freiwillige übertragen wird. Entscheidend ist daher eine klare Strategie, wie und auf welcher rechtlichen Grundlage die Einbindung von Freiwilligen in Sicherheitsfragen geschieht. Zugleich sind Konzepte notwendig, wie mit der mitunter volatilen ehrenamtlichen Beteiligung, die durch Social Media-Einflüsse einem schnellen Auf- und Abebben unterworfen sein kann, umzugehen ist.

Spitzenverband fordert lokale Präventionszentren für Kommunen

Darüber hinaus gilt es, die Präventionsarbeit bei potenziellen Tätergruppen anzusetzen. Die Kommunen sind hier wiederum besonders gefordert. Im Jahr 2016 forderte der Deutsche Städte- und Gemeindebund lokale Präventionszentren für Kommunen, um die Radikalisierung insbesondere islamistischer Jugendlicher zu erkennen und zu verhindern. Die Zentren könnten zugleich eine Plattform für den Austausch vor Ort sein – etwa für Lehrer oder Bürger – und sollten auf Landes-

15 Vgl. ebenda, S. 27

16 Vgl. ebenda, S. 25

17 De Maizière, T. (2017): Leitlinien für einen starken Staat in schwierigen Zeiten, in: Frankfurter Allgemeine Zeitung, 3.2.2017, unter: www.faz.net

18 Deutscher Städte- und Gemeindebund (2014): Bevölkerungsschutz in Städten und Gemeinden, DStGB DOKUMENTATION NO 123

19 ZDF (2017): Verbrauchermagazin WISO (Thema: Hackerangriffe auf Infrastruktur), 8.5.2017. Abrufbar unter: www.zdf.de

und Bundesebene vernetzt sein.[20] Bemühungen in diese Richtung stellt das Land Hessen bereits mit seinem 2013 initiierten Informations- und Kompetenzzentrum gegen Extremismus an. Präventive und intervenierende Maßnahmen sollen darüber koordiniert und vernetzt werden. Über ein „Beratungsmodul" seien bereits Kommunen für den Umgang mit rechtsextremistischen Aktivitäten sensibilisiert worden.[21] Auch auf Länder- und Bundesebene sind die unterschiedlichen Präventionsprojekte und -module auf den Prüfstand zu stellen, sodass deren Wirksamkeit evaluiert, die Einfachheit in der formellen Umsetzung für die Anwender gewährleistet und gemeinsame Programme aus unterschiedlichen Fachressorts im Bund und in den Ländern bestmöglich gebündelt werden.

Fazit: strategisch vorausschauen und Risiken steuern

Eine Erfolg versprechende Strategie der „Vernetzten Sicherheit" wird auch Kommunalverwaltungen und nicht zuletzt deren Unternehmen, zum Beispiel Stadtwerke, miteinschließen. Aus diesem Grund werden immer mehr kooperierende Organisationsformen entstehen müssen, auch um strategische Prognosen und Entscheidungen auf der Wissensgrundlage aller beteiligten Bereiche zusammenzufassen (vergleiche Seite 9, „Gemeinsames Handeln"). So gewinnen auch Verwaltungsstellen oder Gremien an sicherheitspolitischer Relevanz, die sich bisher kaum als Sicherheitsbehörde verstanden hätten, wie beispielsweise das kommunale Beteiligungsmanagement oder die Geschäftsleitungen und Aufsichtsgremien der betroffenen kommunalen – oder auch privaten – Unternehmen.

Risiken zu erfassen und zu steuern wird für die öffentliche Verwaltung zu einer immer wichtigeren Aufgabe

Auch dürfte eine Debatte um Risikomanagement im öffentlichen Bereich neu an Bedeutung gewinnen.[22] Hierbei geht es darum, Risiken systematisch zu erfassen, zu bewerten und den Umgang mit den wesentlichen Risiken planvoll zu steuern. Für Kommunen wurde in dieser Zeitschrift bereits ein mögliches Risikomanagementsystem vorgestellt.[23] In diesem Zusammenhang soll auch darauf aufmerksam gemacht werden, dass sich Kommunen bereits ohne ein solches System systematisch mit Risiken auseinandersetzen. Beispiele dafür sind wie erwähnt der Katastrophenschutz, die Feuerwehr, Hochwassernotfallpläne, Korruptionsprävention, IT-Sicherheitsmaßnahmen und schließlich auch die Berichterstattung über Risiken im Rechenschafts- oder Lagebericht der Kommune.

Je mehr sich eine vernetzte Zusammenarbeit über Gebietsgrenzen, Behörden und Ressorts hinweg etabliert, desto stärker wird sich die Diskussion darauf verlagern, die Zusammenarbeit der kooperierenden Behörden und zivilen Akteure auch effizient zu gestalten. Ein wichtiger Schritt wird in diesem Zusammenhang sein, die Uneinheitlichkeit von Systemen (zum Beispiel IT-Systeme und gesetzliche Grundlagen) etwa zwischen verschiedenen Bundesländern soweit wie möglich zu reduzieren, um die Zusammenarbeit auf der operationalen Ebene zu verbessern.

Nina Kairies-Lamp, Ferdinand Schuster, Christian Kaufhold, Christian Gerding

20 Deutscher Städte- und Gemeindebund (2016): Position – Statement zur Sicherheit in Kommunen, 11.8.2016

21 Hessisches Ministerium des Innern und für Sport: Hessen gegen Extremismus, siehe http://hke.hessen.de

22 Grundlegend dazu Budäus, Hilgers (2009): Öffentliches Risikomanagement – zukünftige Herausforderungen an Staat und Verwaltung. In: Scholz, Schuler, Schwintowski (Hrsg.): Risikomanagement der öffentlichen Hand, Heidelberg: Physica

23 Beck et al. (2013); Risikomanagement in Kommunen. In: PublicGovernance, Sommer 2013, S. 12 ff.