Schock und Stress standhalten

Ralph D. Thiele

Januar 2017

Zusammenfassung

Während Globalisierung, Urbanisierung, Klimawandel und die Akteure einer entstehenden neuen Weltordnung kollidieren, entwickeln sich Krisen zum Dauerphänomen. Stress und Schock sind Weggefährten des Alltags – keine Woche ohne Kriegstraumata und Flüchtlinge, Terror- und Cyberangriffe, Naturkatastrophen und sozialen Aufruhr, finanzielle und wirtschaftliche Krisen. Diese tiefgreifenden, höchst dynamischen Veränderungen lassen in der Bevölkerung ein wachsendes Gefühl von Unsicherheit und Zukunftsangst entstehen. „*Resilienz*" als Fähigkeit, Rückschläge einzustecken, wieder aufzustehen und weiterzumachen, ist in unser Leben „*zurückgesprungen*" und wird zu einer zentralen Aufgabe nationaler und internationaler Krisenvorsorge und Stabilitätspolitik. Resilienz ist insbesondere bei der Begegnung hybrider Gefahren von Bedeutung. In Europäischer Union und NATO hat man erkannt, dass die Begegnung hybrider Bedrohungen, Krisenmanagement und Resilienz Hand in Hand entwickelt werden müssen. EU und NATO verstehen dies als eine dringliche gemeinsame Aufgabe.

Das ISPSW

Das Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung (ISPSW) ist ein privates, überparteiliches Forschungs- und Beratungsinstitut.

In einem immer komplexer werdenden internationalen Umfeld globalisierter Wirtschaftsprozesse, weltumspannender politischer, ökologischer und soziokultureller Veränderungen, die zugleich große Chancen, aber auch Risiken beinhalten, sind unternehmerische wie politische Entscheidungsträger heute mehr denn je auf den Rat hochqualifizierter Experten angewiesen.

Das ISPSW bietet verschiedene Dienstleistungen – einschließlich strategischer Analysen, Sicherheitsberatung, Executive Coaching und interkulturelles Führungstraining – an.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analyse

Kollisionskurs

„*Resilienz*" als Fähigkeit, Rückschläge einzustecken, wieder aufzustehen und weiterzumachen, ist – seiner lateinischen Bedeutung folgend – in unser Leben „*zurückgesprungen*". Sie soll unsere Städte und Gesellschaften künftig widerstandsfähiger machen gegen die Auswüchse von Terrorismus, Klima- und anderen Katastrophen oder auch gegen Angriffe auf kritische Infrastrukturen.

Während Globalisierung, Urbanisierung, Klimawandel und die Akteure einer entstehenden neuen Weltordnung kollidieren, entwickeln sich Krisen zum Dauerphänomen. Stress und Schock sind Weggefährten des Alltags – keine Woche ohne Kriegstraumata und Flüchtlinge, Terror- und Cyberangriffe, Naturkatastrophen und sozialen Aufruhr, finanzielle und wirtschaftliche Krisen. Faktoren wie Überbevölkerung, Armut, Migration, Korruption, Staatszerfall, organisierte Kriminalität und tödliche Infektionskrankheiten verschärfen die Lage.

Europa wankt unter Krisenstress, Haushaltsproblemen und terroristischen Schockerfahrungen. Die NATO ist nur noch ein Schatten ihres früheren *Ich*. Die Vereinten Nationen werden als vormaliger Schutzpatron globaler Friedenspolitik, Menschenrechte und rechtsstaatlicher Normen von Warlords, Terroristen und *Coalitions of the Willing* zu einem Akteur marginaler Bedeutung degradiert. Auch die OSZE hat Mühe, sich relevant in ihre Kernaufgabe *Friedenssicherung* einzubringen.

Auch wenn sich manche Katastrophen – insbesondere Naturkatastrophen – nicht verhindern lassen, können wir dennoch die damit verbundenen Risiken erkennen und absehbare Wirkungen eindämmen. Genau dies haben die Europäische Union und die NATO im Sinn. Zwei Gipfeltreffen der Organisationen Mitte 2016 mündeten im Dezember in 42 Maßnahme Paketen und einer gemeinsamen Erklärung: *„Gemeinsam können beide Organisationen (...) einen besseren Nutzen aus den vorhandenen Ressourcen ziehen, um für Sicherheit in Europa und darüber hinaus zu sorgen.*"

Beide Organisationen sind derzeit dabei, die gemeinsame Arbeit zu strukturieren. Erste Maßnahmenpakete zielen auf eine engere Zusammenarbeit in der maritimen Sicherheit, beim Schutz von kritischer Infrastruktur und insbesondere auch bei der Abwehr von Cyber-Angriffen im Netz. Man befürchtet, dass es Angreifern gelingen kann, ganze Stromnetze und Bankensysteme lahmlegen. Auch vor Desinformationskampagnen ist man besorgt und plant gemeinsame Analysen sowie parallele und koordinierte Übungen im Krisenmanagement. Weiterhin ist eine engere Zusammenarbeit in der Forschung und bei der Ausbildung von Experten vorgesehen.

Hybride Gefahren

Resilienz ist insbesondere bei der Begegnung hybrider Gefahren von Bedeutung. In Europäischer Union und NATO hat man erkannt, dass die Begegnung hybrider Bedrohungen, Krisenmanagement und Resilienz Hand in Hand entwickelt werden müssen. Sie verstehend dies als eine gemeinsame Aufgabe von strategischer Bedeutung. Russland wird vorgeworfen, solche hybriden Ansätze bei der Krim-Annexion angewandt zu haben. Diese Ansätze machen den westlichen Staaten und Gesellschaften politisch, militärisch und sogar gesellschaftlich sichtbar zu schaffen trotz der eigenen scheinbar überwältigenden wirtschaftlichen, technologischen und militärischen Überlegenheit.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Seit Putins „grüne Männchen" – Soldaten in Tarnuniformen ohne Rang- und Nationalitätenabzeichen – im Jahr 2014 auf der Krim auftauchten, die Kontrolle über den Regierungssitz, das Parlament und den Flughafen in Simferopol übernahmen, sowie Einrichtungen der ukrainischen Armee abriegelten, sind Europäische Union und NATO alarmiert. Die Hauptverantwortung für die Abwehr hybrider Bedrohungen für die nationale Sicherheit und Verteidigung und die Aufrechterhaltung von Recht und Ordnung liegt zwar bei den Mitgliedstaaten selbst. Gemeinsamen Bedrohungen werden allerdings besser auf multinationaler Ebene begegnet, insbesondere, wenn sie sich gegen länderübergreifende Netze oder Infrastrukturen richten. Finnland plant für 2017 den Aufbau eines sogenannten „*Europäischen Zentrums zur Abwehr Hybrider Gefahren*". NATO und EU-Mitgliedstaaten sind gehalten, sich daran zu beteiligen.

Für die Einsätze auf der Krim und in der Ostukraine zeigten sich die zivilen und militärischen Instrumente russischer Machtpolitik vorzüglich vorbereitet. Zivile Aktionen waren mit denen der militärischen Kräfte gut abgestimmt. Russische Investitionen, Handel und Finanztransaktionen wurden systematisch eingesetzt, um ökonomische und politische Eliten zu beeinflussen. Medien wurden massiv für Desinformation genutzt, insbesondere um pro-russische Positionen zu stärken. Avatare – Akteure mit Scheinidentitäten – diskreditierten über das Internet relevante Personen des öffentlichen Lebens mit kritischen Positionen zu Russland. Verbindungen zu russischem Organisiertem Verbrechen, zu lokalen kriminellen Akteuren und ebenso zu religiösen Einrichtungen wurden mit der Zielsetzung aktiviert, ethnische Spannungen zu verstärken und Kampagnen für die Rechte von Minderheiten zu befeuern. Hinzu kamen massive Cyberangriffe auf ausgewählte Ziele. Militärische Kräfte, ob verdeckt, subversiv oder regulär, hielten sich im Hintergrund und verliehen den entscheidungssuchenden, nicht-militärischen Aktivitäten lediglich den erforderlichen Nachdruck.

Doch Russland ist weder der erste noch der einzige hybride Akteur. Die Entwicklung hybrider Bedrohungen führte von der Hisbollah im Libanon über den IS im Irak, Syrien und in Libyen nach Russland. Längst sind auch Staaten wie Iran, Nordkorea oder China bemerkenswerte hybride Akteure.

Immerhin hat Russland als erster Nationalstaat das Thema gründlich studiert, in funktionsfähige Konzepte umgesetzt, diese in Simulationen und großangelegten Übungen verifiziert und schließlich im Einsatz erprobt. Warum? General Waleri Wassiljewitsch Gerassimow, Generalstabschef der russischen Streitkräfte, brachte es bereits 2013 öffentlich auf den Punkt: *„… ein funktionierender Staat kann sich binnen Monaten und sogar Tagen in ein Gebiet erbitterter bewaffneter Auseinandersetzungen verwandeln, Opfer einer externen Intervention werden und in einem Strudel von Chaos, humanitären Katastrophen und Bürgerkrieg versinken ... ."* Damals haben wir allerdings noch nicht genau genug hingehört.

Worauf müssen wir uns einstellen?

Im Lichte der bisherigen Erfahrungen mit hybriden Akteuren zeichnen sich eine Reihe von *Charakteristika* ab:

- *Staatliche und gesellschaftliche Ordnung und Zusammenhalt sind das primäre Angriffsziel.* Deren Bekämpfung und der gezielte Einsatz hybrider Akteure an den Schnittstellen traditioneller Verantwortungsbereiche werden Verwundbarkeiten zunächst geschaffen und dann gezielt angegriffen. Die daraus resultierende Ambiguität erschwert eine schnelle und entschlossene Reaktion des Angriffsopfers bzw. der internationalen Gemeinschaft. Durch schnelles, überraschendes Handeln schafft der Angreifer Tatsachen.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

- *Der Schwerpunkt der Aggression liegt in zivilen Wirkungsfeldern.* Die Konfliktentscheidung wird über eine planvolle Orchestrierung unterschiedlicher Mittel und Methoden primär politisch und zivil gesucht. Die militärische Komponente, darunter verdeckt operierende Spezialkräfte, Subversion oder reguläre Streitkräfte, verleiht den politischen und zivilen Aktivitäten lediglich den erforderlichen Nachdruck.
- *Die Kombination und Verschränkung unterschiedlicher Kategorien und Mittel lässt neue Formen der Kriegführung entstehen*. Hybride Kriegführung kombiniert höchst kreativ irreguläre, subversive wie auch propagandistische Mittel und Methoden mit konventionellen Mitteln der Konfliktaustragung. Großangelegte Desinformationskampagnen und die Nutzung der sozialen Medien zur Beherrschung des politischen Diskurses oder zur Radikalisierung, Rekrutierung und Steuerung von Stellvertreter-akteuren werden als Vehikel für hybride Bedrohungen genutzt.
- *Hybride Aggression und deren Angriffsziele sind nur schwer zu erkennen.* Der Aggressor zielt auf die subversive Unterminierung eines anderen Staates und verschleiert seine Aktivitäten, um gegen ihn gerichtete Entscheidungsprozesse zu behindern. Die einzelnen Angriffselemente erscheinen nach außen hin als nur vage zusammenhängend. Tatsächlich sind sie Bausteine eines sorgfältig angelegten Planes, dessen aggressive Zielsetzungen erst in der Gesamtschau der Elemente erkennbar werden.

Offene pluralistische und demokratische Gesellschaften bieten hybriden Bedrohungen, die nur eingeschränkt vorhersehbar und schwer zuzuordnen sind, vielfache Angriffsflächen. Noch vor Kurzem konzentrierten sich Gegenmaßnahmen von Europäischer Union und NATO im Kontext hybrider Kriegführung auf militärische Maßnahmen. Doch wenn die Schwelle zum Krieg überschritten wird, ist die militärische Verteidigung möglicherweise bereits zu spät. Ein Angriff mit hybriden Mittel kann seine strategischen Ziele lange bevor militärische Mittel eingesetzt werden erreicht haben. Die Herausforderung lautet deshalb, Schadensereignisse zu absorbieren, ohne dass die Funktionsfähigkeit von Staat, Wirtschaft und Gesellschaft nachhaltig beeinträchtigt wird. Hierzu sind Strukturen erforderlich, die widerstandsfähig gegenüber bekannten und anpassungsfähig gegenüber unvorhersehbaren Herausforderungen sind.

Standhalten

Europäische Union und NATO entwickeln derzeit flexible Ansätze, die vor hybriden Angriffen abschrecken bzw. diesen mit einem breiten Portfolio an Instrumenten begegnen können. Zugleich soll die Fähigkeit besser ausgeprägt werden, hybrider Gewalt und Ambiguität standzuhalten und sich von erfolgreichen Angriffen ggf. schnell zu erholen, kritische Dienstleistungen und Infrastrukturen einsatzfähig zu halten bzw. deren Einsatzfähigkeit zügig wiederherzustellen.

Die entsprechenden Hausaufgaben für die politischen, zivilen Eliten in Europäischer Union und Atlantischem Bündnis sind beachtlich. Das Ausgangsfundament ist nicht besonders belastbar. Neben Haushaltsproblemen, Banken- und Finanzkrisen, Identitätsproblemen im europäischen Integrationsprojekt und Brexit ist es insbesondere das fragwürdige Krisenmanagement der vergangenen Jahre, das den Wachstumsbedarf politischer und ziviler Eliten bei der Bewältigung anspruchsvoller außen- und sicherheitspolitischer Herausforderungen beleuchtet.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Die Ergebnisse der außen- und sicherheitspolitischen Beiträge von NATO und EU-Mitgliedstaaten im vergangenen Jahrzehnt zum Krisenmanagement in der europäischen Nachbarschaft sind ernüchternd bis verstörend. Wie soll man zerfallende Staaten mit Millionen von Flüchtlingen und Zuwandern, die sowohl dem Terror der Gewalt wie auch dem wirtschaftlichen Elend in den Heimatländern entkommen wollen und diese zugleich im Gepäck mitbringen anders bewerten? Leider zeigt auch der Umgang mit der wachsenden Terrorgefahr im Inland: praktisch alle Instrumente, die der Staat zur Wahrnehmung seiner Schutzverantwortung einsetzen kann, sind nicht gut aufgestellt, sondern häufig Opfer des schleichenden Auszehrungsprozesses der vergangenen Jahre – unterbesetzt, mangelhaft ausgerüstet und unterfinanziert.

Unsere Eliten müssen dazulernen. Hier hilft auch der Blick zurück. Bereits im Kalten Krieg war Resilienz darauf ausgelegt, schwerwiegende Störungen kritischer Versorgungsleistungen zu antizipieren und abzufedern. Mit der Übungsreihe CIMEX wurde die Zusammenarbeit aller Verantwortlichen im Katastrophenschutz regelmäßig und mit großem Gewinn geübt. Seit dem Ende des Kalten Krieges wurden entsprechende Fähigkeiten allerdings stark vernachlässigt. Sie sind praktisch nicht mehr existent. Man sah den Bedarf nicht mehr und scheute die Kosten. Der Rückgriff auf das Wissen von gestern ist notwendig, allerdings nicht hinreichend. Vor dem Hintergrund moderner Informations- und Kommunikationstechnologien und der Herausbildung hybrider Bedrohungen muss Resilienz heute mehr und anderes leisten als in der Vergangenheit, muss quasi neu erfunden werden. Dabei ist insbesondere der erheblichen Vernetzung ziviler und privatwirtschaftlicher, staatlicher und militärischer Sektoren Rechnung zu tragen.

Wollen deutsche Streitkräfte beispielsweise baltischen Partnern in der Krise beistehen, sind sie maßgeblich auf die Infrastruktur und Dienstleistungen des privaten Sektors angewiesen, um Kräfte, Ausrüstung und Versorgungsgüter schnellst möglichst in weit entfernte Einsatzgebiete zu verlegen. Zeitgleich müssen auch hybride Gefahren in der Heimat antizipiert, identifiziert, abgewehrt und ggf. auch verkraftet werden können.

Ein Blick auf die Logistik offenbart die Achillesferse der gegenwärtig erheblichen Abhängigkeit von „just-in-time" Ansätzen. Jegliche größere Störung ist nicht nur für staatliche Organe außerordentlich problematisch, sondern mehr noch für die Bevölkerung. Vergleichbare Abhängigkeiten bestehen bei Wasser oder auch Strom. Beispielsweise funktioniert die Wasserversorgung im kommunalen Verbund nur bei zuverlässiger Stromversorgung reibungslos. Ein erfolgreicher hybrider Angriff auf Stromversorgung, Telekommunikation, Verkehr oder auch das Finanzsystem bringt damit immer zeitgleich ein ganzes Spektrum öffentlicher und privater Dienstleistungen zum Erliegen. Dies kann sehr leicht zu sozialen Unruhen führen, zumal wenn diese von Kampagnen in sozialen Medien befeuert werden.

Ein verschärfendes Problem ist die außerordentlich schwierige Identifizierung und Lokalisierung eines etwaigen Verursachers. In Zeiten globaler Vernetzung kann jeder von überall aus angreifen. Angegriffene wissen nicht wo und von wem der Angriff erfolgt. Die resultierende Ambiguität macht eine adäquate Reaktion schwierig und beansprucht insbesondere Gesellschaften und multinationalen Organisationen, die nach dem Konsensprinzip entscheiden. „Cyber-Angriffe" haben in diesem Kontext eine hervorgehobene, noch immer rapide wachsende Bedeutung. Das Spektrum der Akteure reicht vom privaten Hacker über Kriminelle und Terroristen bis hin zu staatlichen Akteuren. Diese beobachten, experimentieren, intervenieren, stehlen, erpressen, stören und zerstören. In wenigen Bereichen fallen innere und äußere Sicherheit so eng zusammen wie im Cyber-Raum.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Innovation nutzen und Schritt halten

Resilienz zu schaffen ist zugleich Weg und Ziel. Es geht um die Einstellung, um die Motivation der Schlüsselakteure bis hin zum einzelnen Staatsbürger. Es geht um den Prozess, der iterativ, inklusiv, integriert, anpassungsfähig und flexibel ausgestaltet werden muss und dabei im Auge behält, dass er eine freiheitliche, demokratische Grundordnung und deren Werte schützt. Es geht auch um ganz konkrete, messbare Fähigkeiten. Resilienz neuen Zuschnitts soll mittels Innovation einen Mehrwert zu bewährten Vorhaben und Prozessen generieren, die dann nachhaltig geübt und kontinuierlich weiterentwickelt werden müssen. Schlüssel zum Erfolg ist die fortgesetzte Einbindung neuer Informationen und neuen Wissens als Grundlage für die aktuelle Neubewertung und Repriorisierung bisheriger Aktivitäten.

Technologische Umwälzungen lassen darauf schließen, dass sich das Portfolio hybrider Gefahren zügig erweitern wird. Resilienz muss damit Schritt halten. Computer werden immer schneller und allgegenwärtiger. Hinzu kommen fundamentale Durchbrüche u.a. in Robotik, Nano- und Biotechnologie, künstlicher Intelligenz und Sensorik. Maschinen werden von Tag zu Tag kleiner und zugleich leistungsstärker. Sie verbinden sich symbiotisch mit dem Leben der Menschen. In der sich zunehmend ausprägenden Wissensgesellschaft proliferiert Wissen nicht nur rechtmäßig, sondern sehr häufig wie auch durch systematischen Diebstahl von geistigem Eigentum. Kommunikationstechnologien befeuern diese Entwicklung. Das enorme Potenzial von Big Data spielt dabei eine wichtige Rolle.

Vor diesem Hintergrund sind Investitionen in Resilienz alles andere als triviale Aufgabenstellungen. Der hybriden Komplexität und Ambiguität muss mit einer ressortübergreifenden und transsektoralen Perspektive begegnet werden. Von Anfang an ist ein entschieden innovativer Ansatz erforderlich, der auf bestehende Ansätze aufsetzt und neuen Schwung entfacht. Eine besondere Chance bietet sich darin, Staat und Gesellschaft, Streitkräfte und den privaten Sektor über einen vernetzten Simulations- und Experimentalverbund neuer Technologien, innovativer Partnerschaften und kreativen Denkens in ihrer Resilienz zu bestärken.

In den USA hat man diesbezüglich z.B. aus den Naturkatastrophen der letzten Jahre gelernt. So haben dort die Hurrikane „Katrina“ und „Sandy“ tausende Menschenleben gekostet und darüber hinaus 3-stellige Milliardensummen verschlungen, um nur die gröbsten Schäden zu beseitigen. Heute gibt es Resilienz-Förderprogramme in Milliardenhöhe. Städte wie New York leisten sich einen „*Chief Resilience Officer*“, der querschnittlich darauf achtet, dass städtische Planung immer auch Resilienz Erfordernisse im Auge behält. Wettbewerbe wie „100 Resilient Cities“ befeuern zudem die verbesserte internationale Ausprägung von Resilienz. Denn das Wohlergehen der Nachbarn dient nicht zuletzt auch der eigenen Prosperität.

***

Anmerkungen: Der Beitrag gibt die persönliche Auffassung des Autors wieder und erschien erstmalig in *Denkwürdigkeiten*, Journal der Politisch-Militärischen Gesellschaft, Nr. 103, Januar 2017.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Über den Autor dieses Beitrags

Oberst a.D. und Diplom-Kaufmann Ralph D. Thiele ist Vorsitzender der Politisch-Militärischen Gesellschaft e.V. (pmg), Berlin und CEO von StratByrd Consulting. In seiner militärischen Laufbahn war Herr Thiele in bedeutenden nationalen und internationalen, sicherheits- und militärpolitischen, planerischen und akademischen Verwendungen eingesetzt, darunter im Planungsstab des Verteidigungsministers, im Private Office des NATO-Oberbefehlshabers, als Chef des Stabes am NATO Defense College, als Kommandeur des Zentrums für Transformation und als Direktor Lehre an der Führungsakademie der Bundeswehr.

Eine Vielzahl von Publikationen, regelmäßige Vorträge in Europa, Amerika und Asien sowie eine intensive Forschungstätigkeit im Kontext deutscher, österreichischer und europäischer Sicherheitsforschung unterstreichen sein ausgeprägtes Kompetenzspektrum.

Ralph D. Thiele ist Mitglied im Beirat Deutscher Arbeitgeber Verband e.V., Wiesbaden und im Defence Science Board, das von Gerald Klug, Verteidigungsminister der Republik Österreich, geleitet wird.

Ralph D. Thiele gehört auch dem ISPSW Rednermanagement Team an. Weitere Informationen finden Sie auf der ISPSW Website unter http://www.ispsw.com/autoren-und-rednermanagement/

Ralph D. Thiele

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de