Optimistisch Wege finden – Resilienz und Europäische Sicherheit

Ralph D. Thiele

März 2017

Zusammenfassung

Resilienz ist angesichts hybrider Bedrohungslagen für Innere und Äußere Sicherheit gleichermaßen ein Schlüsselthema. Cyberrisiken spielen dabei eine herausgehobene Rolle und führen Spionage, Informationsmanipulation, Terrorakte und Sabotage in eine neue Dimension. Leistungsfähige staatliche Strukturen sind wichtig für die Herausbildung von Resilienz. Eine mangelhafte Reaktionsfähigkeit von Gerichten, Polizei und Streitkräften hingegen beunruhigt die Menschen und führt zu Prozessen und Strukturen „erweiterter Unsicherheit". Ebenso wie deren Mitgliedstaaten sind bislang weder die Europäische Union noch die NATO hinreichend auf hybride Herausforderungen vorbereitet. Dies wollen beide Organisationen ändern. Dabei muss Resilienz mit der Dynamik von Innovation Schritt halten. Neue, optimistische Ansätze werden dringend gebraucht.

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

1. Zu gefährlich für Krieg

„*Diese Welt ist zu gefährlich für Krieg*" sagte General John R. Galvin, der frühere Oberbefehlshaber der NATO in Europa, 1990 in seiner Londoner Rede. Er wiederholte diesen Topos in seiner Biographie „*Fighting the Cold War*" vor zwei Jahren nicht ohne den Hinweis, dass die Welt inzwischen noch gefährlicher geworden ist – eine Einschätzung, die NATO Generalsekretär Stoltenberg in seinem im März 2017 veröffentlichten Jahresbericht voll teilt.

Unter dem Druck von Globalisierung, Urbanisierung und Klimawandel entsteht eine neue Weltordnung mit neuen Schlüsselakteuren. Krisen entwickeln sich zum Dauerphänomen. Stress und Schock sind Weggefährten des Alltags. Kriegstraumata und Flüchtlinge, Terror- und Cyberangriffe, Naturkatastrophen und sozialer Aufruhr, finanzielle und wirtschaftliche Krisen gehören zum mittlerweile vertrauten Vokabular der Berichterstattung in den Medien.

Viele dieser Phänomene verbinden sich zu hybriden Bedrohungen – eine Wortschöpfung des 21. Jahrhunderts, die Kriegsführung unterhalb der Schwelle des Einsatzes militärischer Gewalt adressiert. Charakteristisch hierfür sind „*irreguläre Kampfweisen*" von staatlichen und nichtstaatlichen Akteuren, unter Beimischung von terroristischen und kriminellen sowie Aktionen in digitalen und sozialen Medien. Sie zielen auf die Funktionsfähigkeit und den Zusammenhalt von Staaten und Gesellschaften. Kein Wunder, dass bei vielen Menschen ein Gefühl von Unsicherheit und Zukunftsangst grassiert.

Die Sorgen der Menschen sind nicht unbegründet. Verfassungsschutzpräsident Maaßen zeigte sich vor wenigen Wochen auf dem 20. Europäischen Polizeikongress in Berlin über die Lageentwicklung in der Inneren Sicherheit besorgt. Er forderte: *„Wir brauchen eine Resilienz-Fähigkeit, die Fähigkeit auf Terroranschläge, auf Veränderungen im Cyber-Raum, auf Desinformationskampagnen und auf extremistische Gewaltausbrüche... reagieren zu können ... Und wir müssen in der Lage sein, schnell zum Normalzustand zurückkehren zu können."*[1] Maaßen geht von zunehmend schwierigen Rahmenbedingungen aus. Mit der Flüchtlingskrise sei die Bundesrepublik mittlerweile Bestandteil eines Dramas, das man zuvor noch aus sicherer Distanz beobachten konnte. Heute sind Menschen mitten unter uns, die professionell mit Sprengsätzen und Kalaschnikows umgehen können und wissen, wie man tötet.

Hybride Herausforderungen prägen auch die äußere Sicherheit. 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. Keiner hat es kommen sehen. Keiner hat wirklich überzeugende Antworten. Die russischen hybriden Ansätze machen den westlichen Staaten und Gesellschaften politisch, militärisch und sogar gesellschaftlich sichtbar zu schaffen – trotz der eigenen scheinbar überwältigenden wirtschaftlichen und technologischen Überlegenheit. Der kürzlich ernannte neue Chef des Nationalen Sicherheitsrates in den USA, Generalleutnant H. R. McMaster, urteilte in seiner Buchbesprechung von General Galvins Biographie: „*Vladimir Putins unkonventionelle, hybride Kriegsführung unter dem*

[1] Dr. Hans Georg Maaßen. Behördenspiegel vom 22.2.2017. http://www.behoerden-spiegel.de/icc/Internet/sub/2a6/2a610a27-8836-6a51-bb8f-107607b988f2,,,aaaaaaaa-aaaa-aaaa-bbbb-000000000003&uMen=2b620c03-4c4e-5411-c9b9-a612700266cb.htm

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

Deckmantel der konventionellen militärischen Fähigkeiten Russlands und seines nuklearen Arsenals zielt darauf ab, die Nachkriegs -Sicherheitsordnung in Europa zum Einsturz zu bringen." Vor diesem Hintergrund ist „*Resilienz*" gefragt – die Fähigkeit, Rückschläge einzustecken, wieder aufzustehen und weiterzumachen.

2. Stell Dir vor es ist Cyber-Krieg und keiner geht hin ...

... dann kommt der Cyber-Krieg zu Euch. Jetzt ist er da. Cyberkrieg ist Alltag, so die mehrheitliche Überzeugung der Teilnehmer am jüngsten Weltwirtschaftsforum in Davos. Cyber ist ein Hauptthema in hybriden Bedrohungslagen – Spionage, Informationsmanipulation, Cyber-Terrorakte, groß angelegte Sabotage-Attacken zum Beispiel auf kritische Infrastrukturen wie Banken, Kommunikationsinfrastrukturen oder die Netze der Energieversorger. Mittlerweile sind auch politische Infrastrukturen durch Ausforschung und Desinformationskampagnen bedroht. Der Bundesverfassungsschutz rechnet bis zu den Bundestagswahlen am 24. September mit einem massiven Anstieg diesbezüglicher Aktivitäten. Die über Cyberattacken gewonnenen Informationen können dazu genutzt werden, Politiker zu diskreditieren oder zu erpressen.

Private Hacker, Kriminelle, Terroristen und staatliche Akteure beobachten, experimentieren, intervenieren, stehlen, erpressen, fälschen, stören und zerstören. Sie sind schwer zu lokalisieren und identifizieren. In Zeiten globaler Vernetzung kann der Aggressor von überall aus angreifen. Angegriffene wissen in aller Regel nicht, wo und von wem der Angriff erfolgt. Die damit verbundene Ambiguität macht eine adäquate Reaktion problematisch, insbesondere in demokratischen Gemeinwesen und ihren nationalen und multinationalen Organisationen.

Grundsätzlich ist jegliche größere Störung der kritischen Infrastrukturen nicht nur für staatliche Organe außerordentlich problematisch, sondern zugleich auch für die Bevölkerung. So funktioniert beispielsweise die Wasserversorgung im kommunalen Verbund nur bei zuverlässiger Stromversorgung. Ein erfolgreicher hybrider Angriff auf Stromversorgung, Telekommunikation, Verkehr oder auch das Finanzsystem bringt immer zeitgleich ein ganzes Spektrum öffentlicher und privater Dienstleistungen zum Erliegen. Die Konsequenzen sind durchaus nicht nur virtuell. Ohne Strom bei Kälte oder Hitze sterben Menschen. Ohne funktionsfähige Banken und öffentliche Dienstleistungen ist der Weg zu sozialen Unruhen nicht weit, insbesondere wenn diese von Kampagnen in sozialen Medien zusätzlich befeuert werden.

Diese Entwicklung kam nicht überraschend. Sie hat dennoch viele überrascht. Bereits die russischen Cyberangriffe auf Estland im Jahr 2007 beleuchteten die besondere Qualität von Cyberangriffen, als Websites von Regierung, Parteien, Firmen, Banken, Handynetzbetreibern und Zeitungen zum Zusammenbruch gebracht wurden. Ein Jahr später flankierten die Cyberattacken auf Georgien den russischen Einmarsch in Südossetien. Die Nationalbank sah sich gezwungen anzuordnen, dass die Geldinstitute ihren elektronischen Bankverkehr für zehn Tage einstellen.

Dennoch kam erst richtige Bewegung ins Cyberthema, als die USA im Jahr 2012 feststellten, dass jemand – vermutlich Russen – für ein paar Sekunden in den USA den Strom abgestellt hatte und dass jemand anderes – vermutlich Asiaten – sich lange unbemerkt bei den Geheimnissen amerikanischer Rüstungsindustrie bedient hatte. Als dann auch noch Snowden die Ziele, Wege und Mittel amerikanischer Cyberspionage enthüllte, war der Dammbruch perfekt. Plötzlich war Geld da für Cybersicherheit – in den USA und in Japan, in Großbritannien und den Vereinigten Arabischen Emiraten, um nur einige Staaten zu nennen.

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

In Deutschland brauchte alles ein bisschen länger. Die Snowden-Offenbarungen spülten in Deutschland zunächst das Handy der Kanzlerin in den Mittelpunkt des Interesses. Öffentlichkeit und Politik konzentrierten sich auf amerikanische Bedrohungen. Das Kanzleramt überlegte, die Nutzung von U.S. Informationstechnologie zu begrenzen. Inzwischen ist ein reichhaltiges Biotop an Cyber-Kompetenzzentren in der Entstehung. Auch wenn heute deren Kapazitäten, Prozesse und Strukturen noch etwas unaufgeräumt wirken, leider auch die neue Teilstreitkraft der Bundeswehr für den Cyber- und Informationsraum, ist inzwischen Cyber auch hier in Deutschland ein wichtiges Thema mit der Perspektive rasch zunehmender Kompetenz.

Tatsächlich ist Dringlichkeit angesagt. Nicht nur die kriminellen Angriffe auf Privatleute und Unternehmen – z.B. Krankenhäuser – sowie der Diebstahl geistigen Eigentums nehmen rasant zu. Tagtäglich finden auch Cyberangriffe auf die Bundeswehr statt. Zum Teil werden diese Angriffe mit hohem Aufwand geplant, vorbereitet und durchgeführt. Im Jahr 2015 dauerte es im Schnitt selbst bei schwerwiegenden Attacken 205 Tage, bis Cyberangriffe überhaupt erkannt wurden. Die Lösung der daraus resultierenden Probleme dauerte dann durchschnittlich noch einmal 32 Tage.

Zwei Schlüsseldokumente setzen derzeit den Kurs. Das Weißbuch 2016 steht für die Absicht der Bundesregierung

- gesamtstaatliche Fähigkeiten auszubauen und mit Wissenschaft, Industrie und Partnern zu vernetzen;
- die Sicherheitsarchitektur des IT-Systems der Bundeswehr zu konsolidieren und resilienter zu machen;
- Waffensysteme und Gefechtsstände sowie Lieferketten in der Rüstung zu härten;
- Spitzenpersonal durch Schaffung attraktiver Cyberkarrierepfade zu rekrutieren;
- fragmentierte Zuständigkeiten und Strukturen für einen robusten Fähigkeitsaufbau zusammenführen sowie zentrale Ansprechpartner für andere Ressorts und multinationale Partner zu schaffen.

Die Cybersicherheitsstrategie für Deutschland 2016 beschreibt

- eine deutlich stärkere Rolle der Bundeswehr in der gesamtstaatlichen Sicherheitsvorsorge;
- den Schutz Kritischer Infrastrukturen als ressortgemeinsame Aufgabe;
- den Auf- und Ausbau eines Cyber-Clusters bei der Münchner Universität der Bundeswehr;
- die Weiterentwicklung des Nationalen Cyber Abwehrzentrums;
- die Nutzung der Bundeswehr Incident Response Teams als Teil der gesamtstaatlichen Sicherheitsvorsorge im Kontext von Amtshilfe;
- die Intensivierung der Zusammenarbeit nationaler CERT Strukturen;
- den Aufbau einer Cyber-Reserve.

3. „Angst essen Seele auf“

„*Angst essen Seele auf*“ lautet der Titel des berühmten Films von Rainer Maria Faßbinder aus dem Jahr 1974. Um die Seele von Staat und Gesellschaft, Führungspersönlichkeiten und jedem einzelnen Bürger geht es bei der hybriden Kriegführung. Offene pluralistische und demokratische Gesellschaften bieten hybriden Bedrohungen, die nur eingeschränkt vorhersehbar und schwer zuzuordnen sind, vielfache Angriffsflächen. Hybride

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

Bedrohungen verstärken den bereits grassierenden Vertrauensverlust in die Handlungsfähigkeit staatlicher Institutionen.

"*Resilienzforschung*" setzt sich mit der Frage auseinander, was Menschen und Gesellschaften in existenziellen Krisensituationen Halt gibt. Denn während manche der Betroffenen von traumatischen Erlebnissen aus der Bahn geworfen werden, verarbeiten andere dieselbe Notlage vergleichsweise souverän. Was macht Menschen und Gesellschaften resilient? Forschungsergebnisse zeigen, dass Menschen und Gesellschaften grundsätzlich über zwei Mechanismen ihre Ängste und Unsicherheiten verarbeiten[2]:

- Über die Rückversicherung bei staatlichen Institutionen und als
- individuelle Anpassungs- und Lernfähigkeit.

Leistungsfähige staatliche Strukturen sind somit ein wichtiger Teil der Lösung zur verstärkten Herausbildung von Resilienz. Umgekehrt wird deutlich, wenn staatliche Handlungsfähigkeit hinter dem Sicherheits- und Gestaltungsbedürfnis der Menschen zurückbleibt, leidet die Resilienz. Eine mangelhafte sicherheitspolitische Reaktionsfähigkeit von Gerichten, Polizei und Streitkräften beunruhigt die Menschen. Es kommt zu sogenannten Prozessen und Strukturen „*erweiterter Unsicherheit*".

Ein Realitätscheck in Deutschland zeigt, dass inzwischen 60 Prozent der Deutschen kein oder ein nur geringes Vertrauen in die Problemlösungsfähigkeit des Staates haben. Dieser Vertrauensverlust gegenüber Staat und Politik führt zu einem Rückzug ins Private, zu Politikverdrossenheit, zu einem Anwachsen der stillen Masse, zu Populismus, außerparlamentarischer Opposition und Radikalisierung. In dieser Lage wirken soziale Medien als Angstbeschleuniger. Dies verdeutlicht z.B. das Münchener Attentat im Juli 2016, bei dem soziale Medien Unsicherheit und öffentliche Hysterie befeuerten.

Dies lässt sich natürlich auch absichtsvoll nutzen, zumal mittlerweile sogenannte Fake News – alternative Wahrheiten – häufig größere Aufmerksamkeit erfahren als seriöse Nachrichten. Ziel-Algorithmen in den sozialen Medien und computergesteuerte Twitter-Meldungen können durchaus die Meinungsbildung manipulieren. Derart wird ein Tsunami anonym verdichteten Wählerwillens von Enttäuschung, Vertrauensverlust und Wut aktivierbar, der dann unkontrollierbarer auf die Medien und politischen Institutionen zuläuft und den Zusammenhalt der Gesellschaft untergräbt.

Resilienz soll und kann hier helfen, der demokratiegefährdenden Dynamik erweiterter Unsicherheit das Momentum zu entziehen. Dabei ist der Weg das Ziel, denn wer Resilienz will, bekennt sich implizit zu einer Prozesshaftigkeit und akzeptiert Ungewissheit als ein zentrales sicherheitspolitisches Element. Wo es keine absolute Sicherheit gibt, wird Resilienz zum Rückgrat einer systemischen Sicherung von Freiheit durch permanentes Risikomanagement. Ziel ist die leistungsfähige Selbststeuerung von Gesellschaften, Organisationen und Individuen in der konstruktiven Auseinandersetzung mit Risiken. Resilienz baut auf einen „dynamischen Prozess", der sich in der Herausforderung bewährt. Resilienz kann und soll in und mit der Krise wachsen. Derart entstehen in Krisen auch Rettungswege, die wir vorher nicht kennen.

[2] Jan Pospisil. Resilienz: Die Neukonfiguration von Sicherheitspolitik im Zeitalter von Risiko

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

4. Standhalten

Bislang sind weder die Europäische Union noch die NATO hinreichend auf hybride Herausforderungen vorbereitet. Dies wollen beide Organisationen ändern. Sie wollen hybriden Herausforderungen durch verbesserte Resilienz begegnen.[3] Noch vor Kurzem konzentrierten sich im Kontext hybrider Kriegführung die Gegenmaßnahmen von Europäischer Union und NATO auf militärische Maßnahmen. Doch in der hybriden Auseinandersetzung ist die militärische Verteidigung möglicherweise bereits zu spät, wenn die Schwelle zum Krieg überschritten wird. Ein Angriff mit hybriden Mitteln kann seine strategischen Ziele erreicht haben lange bevor militärische Mittel eingesetzt werden. 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.

In NATO und Europäischer Union ist man nicht nur über Desinformationskampagnen besorgt, sondern auch, dass ganze Stromnetze und Bankensysteme lahmgelegt werden. Man will hybriden Bedrohungen, Krisenmanagement und Resilienz Hand in Hand begegnen. Während in erster Linie die Nationalstaaten gefordert sind, wollen beide Organisationen enger zusammenrücken und flexible Ansätze entwickeln, die in Ergänzung nationalstaatlicher Maßnahmen vor hybriden Angriffen abschrecken bzw. diesen mit einem breiten Portfolio an Instrumenten begegnen können. Derart 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.

Gipfeltreffen der Organisationen Mitte 2016 mündeten 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*."[4] Diese 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. Für Mitte 2017 sind die ersten Deliveries angekündigt.

Bereits im Kalten Krieg galt es, 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. Der Rückgriff auf das Wissen von gestern ist hilfreich, 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. Hier ist insbesondere der erheblichen Vernetzung ziviler und privatwirtschaftlicher, staatlicher und militärischer Sektoren Rechnung zu tragen.

Die mit großer Medienbegleitung auf den Weg gebrachte gemeinsame Übung von Polizei und Bundeswehr – GETEX – zur Abwehr terroristischer Lagen war von Verteidigungsministerin von der Leyen als ein Schritt in diese

---

Österreichische Zeitschrift für Politikwissenschaft. Wien 2013. S. 25-42.

[3] European Commission. Press release. Security: EU strengthens response to hybrid threats. http://europa.eu/rapid/press-release_IP-16-1227_en.htm

[4] NATO. Joint press conference by NATO Secretary General Jens Stoltenberg with the EU High Representative for Foreign Affairs, Federica Mogherini. Brussels 6 December 2016. http://www.nato.int/cps/en/natohq/opinions_138729.htm

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

Richtung gedacht. Allerdings entwickelt sich dieser Ansatz noch sehr mühsam.[5] Nicht wirklich von der Notwendigkeit überzeugt, haben die Länderinnenminister die Übung zu einer Stabsrahmenübung geschrumpft und juristische Grenzbereiche gemieden. So begründete das Gemeinsame Szenario von Polizei und Bundeswehr eine Art verstärkter Amtshilfe – die Unterstützung der Polizeikräfte bei Objektschutz, Verkehrsregelung, Evakuierung und Identifizierung/Dekontamination chemischer Waffen. Dies ist noch nicht der erforderliche Aufbruch zu neuen Ufern.

5. Disruptive Innovation

Technologische Umwälzungen lassen darauf schließen, dass sich das Portfolio hybrider Gefahren zügig erweitern wird. Resilienz muss mit der Dynamik von Innovation Schritt halten. Hierzu zählen fundamentale Durchbrüche u.a. in Robotik, Nano- und Biotechnologie, künstlicher Intelligenz und Sensorik. Computer werden immer schneller und allgegenwärtiger. 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.

Ein schlagendes Beispiel sind die jüngsten Wikileaks, bei denen Tausende von Dateien online gestellt wurden, die Einblick geben, mit welchen Instrumenten die CIA arbeitet, um sich im Cyberraum umfassend Informationen zu verschaffen. Die Dateien beschreiben detailliert den Zugang zu iPhones und Android-Smartphones, zu Computern, die mit dem Microsoft-Betriebssystem arbeiten. Sie erläutern, wie mit dem Internet verbundene Fernseher von Samsung für geheime Gesprächsmitschnitte genutzt werden können. Generationen von privaten, kriminellen und staatlichen Cyberkriegern werden Wikileaks dafür dankbar sein. Viele Bürger werden darunter leiden.

Investitionen in Resilienz sind dringend und anspruchsvoll. Der hybriden Komplexität und Ambiguität muss mit einer ressortübergreifenden und transsektoralen Perspektive begegnet werden. Von Anfang an ist ein innovativer Ansatz erforderlich, der auf bestehenden Ansätzen 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 dreistellige Milliardensummen verschlungen, um nur die gröbsten Schäden zu beseitigen. Heute gibt es Resilienz-Förderprogramme in Milliardenhöhe. Städte wie New York haben die Funktion eines „*Chief Resilience Officers*“ eingerichtet, der querschnittlich darauf achtet, dass städtische Planung immer auch Resilienzerfordernisse im Auge behält. Wettbewerbe wie „100 Resilient Cities“[6] befeuern zudem die verbesserte internationale Ausprägung von Resilienz. Denn das Wohlergehen der Nachbarn dient nicht zuletzt auch der eigenen Prosperität.

[5] Thomas Wiegold. Anti-Terror-Übung GETEX: Was ist eigentlich das Neue? Augengeradeaus 07. März 2017. http://augengeradeaus.net/2017/03/anti-terror-uebung-getex-was-ist-eigentlich-das-neue/
[6] Rockefeller Foundation. 100 Resilient Cities. http://www.100resilientcities.org/#/-_/

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

Resilienz zu schaffen ist zugleich Weg und Ziel. Es geht um die Einstellung, um die Motivation der Schlüsselakteure bis hin zu jedem 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.

Das hat natürlich Konsequenzen für die Aus- und Weiterbildung von Führungskräften und Leistungsträgern. Belastbares Wissen und Können in Wissenschaft und Technologie, Weiterbildung über die gesamte Laufbahn hinweg und enge Interaktion mit der Privatwirtschaft, um die eigene Urteilsfähigkeit über relevante Innovationen zu stärken – all das muss mit Personalentwicklungsmodellen und Compliance-Vorgaben passend gemacht werden.

6. Auf Messers Schneide?

Der März 2017 ist ein ungemütlicher Monat für Europa. Wohin man auch schaut, alte Gewissheiten drohen in einem Krisensturm unterzugehen. Die Briten haben in diesen Tagen ihren Abschied aus der Europäischen Union definitiv eingeleitet. Ein zweites Referendum zur schottischen Unabhängigkeit wird folgen. Die Nordiren könnten sich versucht fühlen, sich der Republik Irland anzuschließen. Geert Wilders lehrt nicht nur vielen Niederländern das Fürchten, auch wenn er vor dem Hintergrund einer großen Wahlbeteiligung bei den jüngsten Wahlen in den Niederlanden noch einmal in die Schranken gewiesen werden konnte. Marine Le Pen erweist sich ihm in Frankreich durchaus ebenbürtig, wenn nicht sogar überlegen.

Nordeuropa ist in Sorge vor einem zunehmend aggressiven Russland. So führen die Schweden die erst 2010 aufgegebene Wehrpflicht wieder ein. Finnland, das die Wehrpflicht nie aufgegeben hatte, bereitet sich in militärischen Übungen darauf vor, hybride Aggressionen abzuwehren. In den Baltischen Staaten steht die NATO inmitten ihrer größten Verlegung seit dem Kalten Krieg. Deutschland übernimmt im Kontext des Rahmennationen-Konzeptes Zug um Zug mehr Führungsaufgaben in und um Europa.

Die Europäische Währungskrise kommt aus ihrem volatilen Status seit einem Jahrzehnt nicht heraus. Das könnte sich demnächst weiter verschärfen. Die nächsten Wahlen in Italien könnten diese Verschärfung einleiten. Kein Wunder, dass europäische Krisengipfel ein Stück europäischer Normalität geworden sind. Präsident Putin kann sich für die europäische Unentschlossenheit, den sichtbaren Mangel an Führungsfähigkeit nur bedanken und beutet die sich bietenden Chancen für eine eigene größere geopolitische Rolle nach Kräften aus.

Die Ereignisse der vergangenen Wochen haben in den USA bereits bestehende Unsicherheiten und Ungewissheiten eher vergrößert. An dieser Stelle kommt der Name „Trump“ ins Spiel. Auch wenn die deutschen Medien schlechte Nachrichten über ihn bevorzugen und ich persönlich Trump-skeptisch bleibe, er macht und will nicht nur Unsinn. Er macht vor allem vieles von dem, was die Menschen in seinem Land von Ihrem Präsidenten erwarten und erhoffen. Die Mehrzahl der amerikanischen Steuerzahler macht sich Sorgen um ihre Arbeitsplätze und ihr Einkommen, Terrorismus und Kriminalität. Sie wollen nicht ungeniert von mexikanischen Banden in ihren kalifornischen Häusern überfallen werden. Sie sind es leid, dass ihre Söhne und Töchter auf regionalen Kriegsschauplätzen fern der Heimat in Europa und Asien verwundet werden oder sterben. Sie fragen sich, was

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 Türkei noch in der Wertegemeinschaft NATO macht[7] und sie sind es müde, Alliierte zu finanzieren, die sich selbst nur wenig Sorgen um die eigene Sicherheit machen. Europa soll militärisch endlich erwachsen werden.[8]

Dass im ersten Monat von Trumps Amtsführung in den USA 235.000 neue Arbeitsplätze entstanden sind, werden ihm seine Wähler danken. Ob sie ihm langfristig danken, dass er faktisch die globale Führungsrolle der USA untergräbt, wird man sehen. Die schon bei Barack Obama entstandenen Zweifel sind unter Trump explosionsartig gewachsen. In den vergangenen Jahrzehnten waren amerikanische Politik und Gestaltungsmacht der Garant deutscher und europäischer Prosperität und Sicherheit. Deutschland und die Europäische Union profitierten vom im Wesentlichen US-finanzierten Schutzschirm der NATO. Geht nun das amerikanische Jahrhundert zu Ende?

Wenn man die Ergebnisse der Münchner Sicherheitskonferenz 2017 zusammenfasst, lässt sich konstatieren: Wir Deutschen und Europäer müssen uns darauf einstellen, dass die USA künftig eine kleinere Rolle in der Verteidigung Europas und seiner Nachbarschaft spielen werden. Das Nordatlantische Bündnis zeigt Risse. Europa soll die Risse kitten – durch ein deutlich verstärktes Engagement. So will es Trump. Vorgeblich wollen es auch die Europäer selbst. Sie haben wiederholt zugesagt 2% ihres Sozialproduktes für Verteidigung auszugeben. Große, wirtschaftlich starke Bündnispartner sollen mehr beitragen als wirtschaftlich schwächere. Kaum ein Staat nimmt die Zusagen ernst. Es gibt Stimmen in kleineren Staaten, aber selbst in England und Frankreich, die sich Sorgen um eine deutsche militärische Übermacht machen, sollte Deutschland seine 2% Zusage wahrmachen. Zudem haben 70 Jahre Trittbrett fahren die europäischen Akteure sozialisiert. Werden sie das Steuer herumreißen können?

Neue Ansätze werden dringend gebraucht. Denn es gibt keine Garantie, dass zusätzliche europäische Verteidigungsausgaben auch wirklichen Bedarf adressieren werden. Absehbar werden etliche Akteure der Versuchung erliegen, den ausgetrampelten bisherigen Pfaden kultureller, geografischer und national bewährter Präferenzen weiter zu folgen. Vor diesem Hintergrund ist es überlegenswert, in einem Spektrum realistischer Einsatzoptionen insbesondere die Mängel zu identifizieren, die bei moderaten Investitionen besonders große kurz- und mittelfristige Fähigkeitsgewinne versprechen. Für diese Investitionen sollten auch frisches, zusätzliches Geld bereitgestellt werden, keine Papiertiger. Was spricht dagegen, dass unterschiedliche Nationen unterschiedliche Schwerpunkte setzen und dabei auf bereits existierende eigene technologische Fähigkeiten und auch eigenen wirtschaftlichen Nutzen fokussieren?

Luxemburg verfolgt beispielsweise einen Ansatz, bei dem Mehrausgaben für Verteidigung, mit verfügbarem technologischen Know-how, wirtschaftlichem Nutzen für die Allgemeinheit und operativem Nutzen für die NATO verbunden werden. Luxemburg beschafft den Militärsatelliten „GovSat“ und stellt im Rahmen des NATO-Programms „Alliance Ground Surveillance“ (AGS) kostenfrei Satellitenkommunikationskapazitäten und Services bereit. Aus diesem Ansatz – ein Land stellt Fähigkeiten bereit, die es technologisch meistert und die sich mit eigenem wirtschaftlichen Nutzen verbinden – ließe sich eine dramatisch wirksamere Beschaffungspolitik in Europäischer Union und NATO gestalten als mit den herkömmlichen Konzepten. Der luxemburgische Premier- und Verteidigungsminister Etienne Schneider stellt jedenfalls völlig zu recht fest: „*Die Bereitstellung dringend benötigter Satellitenkapazität für das AGS-Programm unterstreicht Luxemburgs Solidarität mit den NATO*

[7] Stanley Weiss. It's Time to Kick Erdogan's Turkey Out of NATO. Huffington Post. http://www.huffingtonpost.com/stanley-weiss/its-time-to-kick-erdogans_b_9300670.html
[8] Stephen M. Walt. It's Time for Europe's Militaries to Grow Up. Foreign Policy. February 23, 2017. http://foreignpolicy.com/2017/02/23/its-time-for-europes-militaries-to-grow-up-trump-nato/

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

Verbündeten ... Luxemburgs freiwilliger Beitrag verursacht keine Kosten für das Bündnis und repräsentiert eine bemerkenswerte neue Alternative, dem Bündnis Fähigkeiten bereitzustellen."[9]

Bei aller Skepsis gegenüber europäischen Institutionen – sie haben allen Krisen trotzend bislang eine Reihe bemerkenswerter „Deliveries" zu verantworten. Sie haben entscheidende Beiträge geleistet, mehr als sechs Jahrzehnte Frieden in Freiheit zu bewahren und den europäischen Bürgern einen gediegenen Wohlstand zu sichern. Das ist weitaus mehr, als die Masse der Menschheit in diesem Zeitraum erfahren hat. Leider ist Europa in den letzten Jahren auch unfreundlicher geworden, insbesondere gegenüber Flüchtlingen und Migranten. Man kann also nur spekulieren wie es weitergeht.

Wünschen müsste man sich, dass mehr optimistische Entwürfe entwickelt werden. Dies ist genau ein Feld, zu dem EuroDefense beitragen will und kann. EuroDefense Deutschland ist entstanden, um die Gemeinsame Sicherheits- und Verteidigungspolitik zu erklären, zu vermitteln und zu unterstützen. Diese Aufgabe ist auch heute wichtig. *„Jeder muss tun, als ob etwas an ihm läge, als ob sein Reden und Handeln von Bedeutung wäre."* So lautete 1899 die Aufforderung des großen deutschen Historikers Theodor Mommsen zum Bürgersinn. Ich finde, das passt auch gut zu Europa und zu EuroDefense. Wir sollten mit diesem Ansatz europäische Zukunft schreiben.

***

Anmerkungen: Der Beitrag gibt die persönliche Auffassung des Autors wieder. Es handelt sich um die Antrittsrede des Autors als neugewählter Präsident von EuroDefense (Deutschland) e.V. am 16.03.2017 in Bonn.

[9] NATO. NCIA. https://www.ncia.nato.int/NewsRoom/Pages/161122_KU_Band_Satellite.aspx

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, Präsident von EuroDefense (Deutschland) 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 Beirat der Zeitschrift für Außen- und Sicherheitspolitik, Köln.

Er 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