

# Denkwürdigkeiten



Journal der  
Politisch-  
Militärischen  
Gesellschaft

Nr. 104  
April  
2017

Herausgegeben vom Vorstand  
der Politisch-Militärischen Gesell-  
schaft e.V. (pmg) in Berlin

ISSN 1436-3070

## LEADOFF

### Liebe Mitglieder,

alternative Fakten gibt es offensichtlich nicht nur in den USA. Auch der deutsche Außenminister betont, dass die 2% Verteidigungsausgaben vom Bruttosozialprodukt Verpflichtung, die von der Bundesregierung erst kürzlich beim Warschauer Gipfel der NATO erneuert wurde, nicht so ernst gemeint ist und er hier ordentlichen Interpretationsspielraum sieht. Der Beitrag von Generalleutnant a.D. Dr. Olshausen beleuchtet Konsequenzen für den Zusammenhalt des Bündnisses. Die Neuvermessung Europas in der Welt ist längst unterwegs. Der Brexit hat die Koordinaten verändert. Zusätzlich forciert die Neuausrichtung der amerikanischen Politik ein deutlich fokussierteres, engagierteres Europa mit erheblich verbesserter Entscheidungsfindung und Handlungsagilität. Deutsche Politik wird vor diesem Hintergrund künftig weitaus mehr an ihren Taten als an ihren Worten gemessen werden.

*Ralph Thiele, Vorstandsvorsitzender*

## IMPRESSUM

### Denkwürdigkeiten

Journal der  
Politisch-Militärischen  
Gesellschaft e.V.

Herausgeber  
Der Vorstand der pmg

Redaktion  
Ralph Thiele (V.i.S.d.P.)  
E-Mail: info@pmg-ev.com  
Webseite: www.pmg-ev.com

Die **Denkwürdigkeiten** erscheinen mehrfach jährlich nach den Veranstaltungen der pmg.



## In dieser Ausgabe

### 1 NATO in Gefahr!

Dr. Klaus Olshausen

### 2 Cyber-Angriffe gegen politische Infrastrukturen - Strategische Implikationen

Dr. Sven Herpig

### 4 Optimistisch Wege finden – Resilienz und Europäische Sicherheit

Ralph D. Thiele

### 9 Der Terrorismus hat auf Dauer (k)eine Chance

Friedrich Christian Haas

### 13 Smearing Gorka may mark return of US yellow journalism

Dr. Christina Lin

### 15 Demographic War Index 2017

Prof. Dr. Gunnar Heinsohn

## THEMEN

### NATO in Gefahr!

#### Europäische Staaten suchen Ausflüchte von ihren Zusagen

Seit den Wahlkampfzeiten im Jahr 2016 in den USA mit den Aussagen von Kandidat Trump und später seinen Antworten in Interviews bis in die Tage vor der Amtseinführung im Januar 2017 (die NATO ist obsolet, leistet zu wenig im Kampf gegen ISIS) schien es „conventional wisdom“, dass es Trump ist, der die Nordatlantische Allianz in ihren Grundfesten gefährdet.

Das Argument war, dass der Beistand für jedes Mitglied der Allianz im Falle eines Angriffs ohne Vorbedingung eine Verpflichtung aller sei – natürlich einschließlich der USA. Und jede ausgesprochene oder denkbare Einschränkung dieser Verpflichtung untergrabe das Fundament dieses Bündnisses.

Die Aussagen von Vizepräsident Mike Pence und Verteidigungsminister James Mattis bei der Münchner Sicherheitskonferenz unterstrichen und bestätigten die unverbrüchliche Zustimmung auch von Präsident Trump und seiner Administration zur NATO als dem wichtigsten Bündnis für die USA und in der Welt.

Allerdings erinnerten beide, Pence und Mattis, die europäischen Verbündeten nachdrücklich an ihre Seite der Verpflichtung, nämlich die wiederholt – nicht erst seit September 2014 – gemachten Zusagen, ihre Ressourcen für die Sicherheits- und Verteidigungspolitik drastisch zu erhöhen. Erst vor acht Monaten in Warschau bestätigten sie die „NATO guideline to spend a minimum of 2 per cent of their Gross Domestic Product on defence“. Dies bedeutet, dass große, wirtschaftlich starke Bündnispartner mehr beitragen als wirtschaftlich schwächere. Darin liegt der Hauptgrund für diese Richtlinie und diese schließt viel mehr ein als die ständig als Ablehnungsgrund in den Vordergrund gerückte Rüstung.

### Deutsche Reaktionen

Wenn man die Reaktionen einiger, gerade auch deutscher Politiker – auch Mitglieder der Regierung – und Kommentatoren liest, reibt man sich die Augen. Der neue deutsche Außenminister ist sich offensichtlich der Bedeutung des Artikels 3 des Washingtoner Vertrags von 1949 nicht bewusst. Er weiß nicht, oder will nicht zugeben, dass die wichtigen Punkte des Warschauer Gipfels zur künftigen Ausgestaltung der Sicherheit und Verteidigung der NATO-Staaten zur Prävention und Abwehr von bewaffneten Angriffen, einschließlich vieler hybrider Gefahren und Cyberangriffe, von der deutschen Bundesregierung gebil-

ligt worden sind – ohne Kautelen oder dem in einigen Regionen sprichwörtlichen „Abschwören“.

Seine ersten Reaktionen auf die Hinweise und das Drängen der neuen US Administration (wie schon vieler vor ihr), nun endlich die faire Lastenteilung Wirklichkeit werden zu lassen, konkretisieren nicht etwa, was für die Gesamtstreitkräfte und die Resilienz des Landes jetzt zügig auch von Deutschland getan werden muss, sondern heben hervor, dass Diplomatie und Entwicklungshilfe für die Sicherheit Deutschlands bedeutender seien als die Vorbereitung der Gefahrenabwehr durch Streitkräfte aller Allianzmitglieder.

Dieses mit dem höheren moralischen Anspruch des Nichtmilitärischen verknüpft mit kaum verbrämtem Wegducken von den selbst zugesagten Verpflichtungen vorgetragene Bekenntnis, das er zuletzt beim Besuch des niederländischen Außenministers noch zugespitzt hat, gefährdet das Vertrauen in die Verlässlichkeit deutscher Zusagen. Bei dieser Gelegenheit hat Minister Gabriel sich nicht versagt hinzuzufügen, dass (wohl gerade aufgrund der deutschen Geschichte) unsere niederländischen Nachbarn „eher beunruhigt“ wären, wenn Deutschland eine („zu starke“) gut ausgebildete, nach NATO Erfordernissen ausgerüstete und personell hoch qualifizierte Bundeswehr für die Aufgaben im Bündnis und der Europäischen Union zur Verfügung stellt. Ja, geht's noch?

Das Totschlag-Argument von „65 Milliarden Euro für Rüstung“ (purer Populismus übrigens mal von anderer Seite) und die Hinweise auf Diplomatie, Entwicklungshilfe, zivile Missionen für die Sicherheit, lösen keine der umfassenden Aufgaben, die sich seit Jahren für alle europäischen NATO- und EU-Nationen in der Sicherheits- und Verteidigungspolitik stellen und weiter der Erfüllung harren.

Wer die Verlässlichkeit der US Administration in Sachen Bündnis in Zweifel zieht, wer zugleich zu den Forderungen nach (endlich) fairer Lastenteilung solche Aussagen macht und wer damit den

festgestellten Mangel an Fähigkeiten nicht überwinden will, der gefährdet einen erfolgreiche Verteidigung nach Artikel 5 des NATO-Vertrags. Denn er mag, wenn es „zum Schwur käme“, vielleicht den Willen zu kollektiver Verteidigung haben, aber nicht die Mittel.

*Dr. Klaus Olshausen*

Generalleutnant a.D. Dr. Klaus Olshausen war von 2006 bis 2013 Präsident der Clausewitz-Gesellschaft. Zuvor war er Deutscher Militärischer Vertreter im Militärausschuss der NATO, bei der WEU und EU, HQ NATO, Brüssel. Der Beitrag gibt die persönliche Auffassung des Autors wieder. Der Beitrag erschien erst im Behördenspiegel, Februar 2017 sowie in ISPSW Strategy Series: Focus on Defense and International Security, Issue No. 474, March 2017. [www.ispsw.com/](http://www.ispsw.com/)

### THEMEN

## Cyber-Angriffe gegen politische Infrastrukturen - Strategische Implikationen

Wenn man in Deutschland von Cyber-Angriffen, Verteidigungs- und Sicherheitspolitik spricht, wird man vermutlich das Jahr 2015 zukünftig als Meilenstein betrachten müssen. In diesem Jahr wurde der Bundestag, die Legislative Deutschlands, Ziel und Opfer einer Cyber-Operation ausländischer Kräfte. Folgt man der öffentlichen Stellungnahme des Präsidenten des Bundesamts für Verfassungsschutz Dr. Hans-Georg Maaßen, so konnte dieser Angriff attribuiert werden. Russland soll für den Cyber-Angriff auf einen Teil der deutschen politischen Infrastruktur verantwortlich gewesen sein. Hieraus haben sich für die Cybersicherheits- und -verteidigungspolitik einige elementare Fragestellungen ergeben diese – betrachtet man die Nachwirkungen des Cyber-Angriffs auf das Democratic National Committee in den Vereinigten Staaten – bis heute unbeantwortet geblieben sind.

### Wir wissen nicht, welcher Schaden angerichtet wurde

Was beziffert werden kann, sind die Mannstunden und die finanzi-

ellen Ressourcen, die für die technische Reaktion für den Vorfall aufgebracht werden mussten. Schwieriger wird es dabei zu ermessen, welcher Informationsnachteil der Legislative (und Deutschland) durch den Angriff entstanden ist. Das liegt vor allem daran, dass eine sinnvolle Berechnung vermutlich daran scheitert, dass man nicht ermessen kann inwiefern der Angreifer einen Informationsvorsprung erringen konnte. Bei einer strategischen – vielleicht sogar spieltheoretischen<sup>1</sup> – Betrachtung des Einflusses von Cyber-Operationen ist eine beidseitige Einschätzung des Gewinns/ Verlusts notwendig um das Gesamtergebn zu ermitteln. Vielleicht besaßen die Angreifer bereits alle Informationen, die sie durch den Angriff erlangen konnten durch andere klandestine Aktivitäten – wäre dann ein Schaden entstanden? Schwer zu beziffern sein wird auch die Verunsicherung in der Bevölkerung (und den Politikern selbst), die durch den Angriff ausgelöst wurde und welche Auswirkungen und Nachwehen das mit sich gebracht hat.

### **Wir wissen nicht, wie wir reagieren sollen**

Die einzig bekannte Reaktion auf den Angriff gegen den Bundestag war ein „naming and shaming“ des vermeintlichen Angreifers durch den Präsidenten des BfV. Es ist jedoch unklar, ob es sich hierbei wirklich um eine gewollte politische Reaktion oder lediglich das reguläre Verhalten von Dr. Maaßen bei Cyber-Themen handelte. Angenommen es handelte sich hierbei um eine politische Reaktion so ist interessant, dass die Aussage nicht von der Kanzlerin oder einem Minister kam, sondern „lediglich“ dem Leiter einer Oberen Bundesbehörde – derjenigen Behörde die den Vorfall im Bundestag nicht untersuchen durfte. Aber auch auf amerikanischer Seite wirkte die politische Reaktion nicht minder planlos. Dort ordnete der damalige Präsident Obama erst nach einem dreiviertel Jahr, nachdem die Präsidentschaftswahl dessen Beeinflussung

vermutlich Ziel des Angriffs war gelaufen war, entsprechende Maßnahmen an<sup>2</sup>. Diese politische Reaktion war jedoch, unter anderem mit der Ausweisung von fast drei Dutzend Diplomaten und dem Zugangsverbot für russische Regierungsmitarbeiter zu bestimmten Institutionen, sehr viel intensiver als die deutsche Reaktion. Es stellt sich unweigerlich die Frage, wie auf Cyber-Angriffe reagiert werden sollte. Das beinhaltet unter anderem auch deren Auswirkungen zu bemessen und abzuwägen welche (außen-)politischen Mittel eine Eskalation nur weiter vorantreiben würden („Eskalationsspirale“), der Vorstellung sind hier keine Grenzen gesetzt, denn von nuklearer Vergeltung bis zum „Zurückcybern“ hatte der politische Diskurs bereits alles im Petto.

### **Wir wissen nicht, wer reagieren soll**

Im Fall der Cyber-Operation gegen den Bundestag war unklar, wer in die Reaktion des Vorfalls eingebunden werden sollte. Es gab anfänglich eine generelle Ablehnung gegenüber der Einbindung der Exekutive in Bearbeitung dieses Vorfalls. Über die Einbindung des Militärs, welches gegebenenfalls zukünftig beim Einsatz zum Schutz kritischer Infrastrukturen gegen Cyber-Angriffe zum Einsatz kommen soll wurde nicht einmal ein Wort verloren. Man einigte sich am Ende auf die Einbindung des Bundesamts für Sicherheit in der Informationstechnik, einer Oberen Bundesbehörde im Ressort des Bundesministeriums des Innern. Natürlich gibt es in Deutschland die Gewaltenteilung, weshalb man auch die Zurückhaltung bei der Frage wer jetzt helfen soll verstehen kann. Denn: wer hier hilft hat potenziell Zugriff auf alle Daten der Bundestagsverwaltung und der -abgeordneten (wie auch die Angreifer). Jedoch muss man sich die Frage stellen, ob es nicht sinnvoller sei, wenn das BSI, welches Sicherheitsmaßnahmen für die Regie-

rungsnetze<sup>3</sup> bereitstellt, diesen Schutz auch für andere politische Infrastrukturen wie den Bundestag oder die politischen Parteien zumindest anbietet. Fakt ist: diese Behörde mit über 600 Experten hat in dem Bereich mehr als 25 Jahre Erfahrung. Möglicherweise würde ein solches Angebot mit einer organisatorischen Umstellung, der Herauslösung des BSI aus dem BMI und damit einer Aufstellung ähnlich wie der der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) einhergehen. Dies ist eine Frage, die man sich vor dem Hintergrund der in der Cyber-Sicherheitsstrategie 2016 angekündigten Schaffung von Mobile Incident Response Teams (MIRTs) im BSI und deren Einsatzbestimmungen notwendigerweise stellen muss. Bei all diesen Erwägungen sollte es im Cyber-Raum keine Rolle spielen, ob es sich um einen zivilen oder militärischen Angriff handelt. Hier sollte „schützen“ wer die beste Befähigung hat und das ist derzeit das BSI. Eine Kooperation, auch mit privaten Akteuren ist natürlich nicht ausgeschlossen und hat sich bereits in der Vergangenheit bewährt.

### **Wir wissen nicht, wann wir reagieren sollen**

Selbst wenn klar ist, welcher Schaden angerichtet wurde, welcher Akteur reagieren soll und wie er reagieren soll ist immer noch unklar wann. Damit ist nicht der Zeitpunkt („when“) gemeint, sondern ob eine politische Reaktion stattfinden soll („if“). Es gibt einen langen, komplexen Diskurs darüber, wie gut eine technische und politische Attribution von Cyber-Angriffen sein kann. Dieser fängt bei kyrillischen Schriftzeichen und Bildern brennender amerikanischer Flaggen im Code an und hört bei einer elaborierten geopolitischen Lageeinschätzung auf – jedoch nicht ohne vorher „False Flag Operations“ und „stellt Dir vor Du bist im gegnerischen Netz drin, dann weißt du, dass sie es waren darfst es aber keinem sagen, weil sie dann wissen, dass du in ihrem Netz bist“-Gedankenspiele zu erwähnen. Die Fortführung des Dis-

<sup>1</sup> Hergig, Sven (2016), Anti-War and the Cyber Triangle: Strategic Implications of Cyber Operations and Cyber Security for the State, ePubli GmbH, 09.01.2016

<sup>2</sup> President of the United States (2016), Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, Executive Order 13757 of December 28, 2016, Federal Register, Vol. 82, No. 1, 03.01.2017

<sup>3</sup> Bundesamt für Sicherheit in der Informationstechnik (2010), BSI-Jahresbericht 2010, Bonn

kurses ist wichtig und sollte sowohl von Technikern als auch Politikwissenschaftlern fortgeführt werden, da die Resultate für die gerade aufkommende Debatte zur Cyber-Rüstungsbeschränkung nicht minder relevant sind. Mindestens genauso wichtig ist jedoch auch die Frage „wieviel Attribution ist genug Attribution?“ – vor allem im Verbund mit der Bewertung des eingetretenen Schadens. Wenn ich mir relativ sicher bin woher der Angriff kam aber kaum Schaden angerichtet wurde verhalte ich mich als Staat vermutlich anders als wenn ich mir relativ sicher bin woher der Angriff kam aber ein immenser Schaden angerichtet wurde. Der innenpolitische Druck mag dazu führen (außen-)politisch zu agieren.

### Wir wissen, was wir nicht wissen

Die Erkenntnis darüber an welchen Bereichen wir noch arbeiten müssen ist der erste Schritt zur besseren Vorbereitung auf zukünftige Cyber-Operationen gegen unsere politischen Infrastrukturen – und die werden ohne Frage kommen. Es muss sich weiter damit beschäftigt werden, wie

- die Organisationsstruktur zur Reaktion (aber auch Prävention und Detektion) auf Cyber-Angriffe gegen politische Infrastrukturen aussehen soll;
- die Bewertung der Auswirkungen und die Attribution von Cyber-Angriffen verbessert werden kann;
- und eine sinnvolle und verhältnismäßige Anpassung von (außen-)politischen Reaktionen auf Cyber-Angriffe aussehen kann.

Um die Herausforderungen richtig zu verstehen und Antworten zu finden die effektiv und sinnvoll sind, bietet sich im Cyber-Diskurs oft ein *tabula rasa* Ansatz an. Es ist hierzu notwendig sowohl den Cyber-Raum als sozio-politisch-technisches Konstrukt, als auch die entsprechenden geopolitischen Zusammenhänge zu verstehen. Besonders bedacht sollte mit Analogien umgegangen werden, da diese im Zusammenhang mit „Cyber-Themen“ häufig unzureichend die Komplexität widerspiegeln und dadurch zu falschen

– und teilweise gefährlichen – (Policy-)Schlussfolgerungen führen können.

Dr. Sven Herpig

Dr. Sven Herpig ist Leiter des Transatlantischen Cyber Forums und bringt dort die Experten von beiden Seiten des Atlantiks zu allen Facetten der Innen-, Cyber- und Verteidigungspolitik im Cyber-Raum zusammen. Der Beitrag gibt die persönliche Auffassung des Autors wieder.

## THEMEN

### Optimistisch Wege finden – Resilienz & Europäische Sicherheit

#### 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.“ 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 Sprengätzen 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 Deckmantel der konventionellen militärischen Fähigkeiten Russlands und seines nuklearen Arsenal* 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.

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

... dann kommt der Cyber-Krieg zu Euch. Jetzt ist er da. Cyber-Krieg 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 Infrastruktu-

ren 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 Dammbreach 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.

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. Täglich 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 Cyberkarrierewege 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.

#### „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 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:

- 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.

#### 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. 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.“ 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 ins-

besondere 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 Richtung gedacht. Allerdings entwickelt sich dieser Ansatz noch sehr mühsam. 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.

### 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 größten 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“ befeuern zudem die verbesserte internationale Ausprägung von Resilienz. Denn das Wohlergehen der Nachbarn dient nicht zuletzt auch der eigenen Prosperität.

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, demo-



kratische 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.

### 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 aufgebene Wehrpflicht wieder ein. Finnland, das die Wehrpflicht nie aufgeben 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 die Türkei noch in der Wertegemeinschaft NATO macht 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.

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. Vorgiebig wollen es auch die Europäer selbst. Sie haben wiederholt zugesagt 2 Prozent 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 Prozent Zusage wahr machen. 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 Papier-tiger. 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 technologischem 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 wirtschaftlichem 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 zurecht fest: *„Die Bereitstellung dringend benötigter Satellitenkapazität für das AGS-Programm unterstreicht Luxemburgs Solidarität mit den NATO Verbündeten ... Luxemburgs freiwilliger Beitrag verursacht keine Kosten für das Bündnis und repräsentiert eine bemerkenswerte neue Alternative, dem Bündnis Fähigkeiten bereitzustellen.“*

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.

Ralph D. Thiele

Ralph Thiele ist Vorsitzender der Politisch-Militärischen Gesellschaft (pmg) und geschäftsführender Inhaber von StratByrd Consulting. Der Beitrag gibt die persönliche Auffassung des Autors wieder. Es handelt sich um die Antrittsrede des Autors als neugewählter Präsident von EuroDefense (Deutschland) am 16.03.2017 in Bonn.

## THEMEN

### Der Terrorismus hat auf Dauer (k)eine Chance

Nach dem Innenminister Thomas de Maizière bestätigte, dass es sich bei dem in die Menschenmenge auf dem Weihnachtsmarkt am Breitscheidplatz gefahrenen LKW um einen Terroranschlag handle, wurde vielen klar, dass der Terror nun endgültig und „mit voller Wucht“ in Deutschland angekommen ist. So zitierte der Focus eine Berliner Medizinstudentin. „Berlin war meine sichere Insel“<sup>4</sup> schrieb sie auf Facebook

<sup>4</sup> „Berlin war meine sichere Insel“ - der traurige Facebook-Post einer jungen Berlinerin. In: Focus Online 20.12.16 [zum Artikel <http://urlby.de/w0u23a9> zum Post

und brachte damit zum Ausdruck, was viele Deutsche immer noch gehofft hatten, trotz der Serie von Anschlägen in 2016, die sich bei den Ermittlungen als von islamistischen Gruppen wie dem IS oder Al Qaida motiviert bzw. gelenkt heraus stellten. Aus Sicht der Sicherheitsbehörden ist dabei „nur“ eingetreten, was man seit Jahren befürchtet bzw. erwartet hatte: Dass eines Tages weder präventive Ermittlungen – wie im Fall der Sauerlandgruppe 2007 oder beim geplanten Anschlag auf den Berliner Flughafen 2016 –, noch unprofessionelles Vorgehen der Terroristen – wie bei den Kofferbomben am 31. Juli 2006 – einen erfolgreichen Anschlag verhindern würden.

Während noch die Ermittlungen hunderter Beamter im BKA und anderen Behörden zum genauen Hergang des Anschlags auf Hochtoren laufen, stellt sich die Frage, welche Lehren hieraus gezogen werden können; denn dieser Anschlag war sicherlich nicht der Schlusspunkt, vielleicht nur ein vorläufiger Höhepunkt. Ein Blick nach Frankreich zeigt uns das, wenn wir uns nur die drei Anschläge mit den höchsten Opferzahlen in Paris im Januar 2015 (Charly Hebdo, jüdischer Supermarkt), im November 2015 (Stade de France, Bataclan) und im Juli 2016 in Nizza (Promenade des Anglais) vergegenwärtigen. Um mit Altkanzler Helmut Schmidt zu sprechen, es geht um „Terroristen, die noch nicht am Ende ihrer kriminellen Energie sind“<sup>5</sup>, nicht in Deutschland und nicht in Europa. Dafür sprechen einerseits die prinzipiellen Strategien seitens der beiden diesbezüglich führenden wie rivalisierenden islamistischen Gruppen Al Qaida und Islamischer Staat (IS). Andererseits zeigen die territorialen Rückschläge und der gegebenenfalls mittelfristige Niedergang des vom IS ausgerufenen Kalifats bereits ähnliche Wirkungen, wie das Ende des Krieges

<https://www.facebook.com/Nemi.El.H/posts/1363720976995271>].

<sup>5</sup> Deutscher Herbst: Helmut Schmidt: Fernsehansprache 1977 [YouTube <https://www.youtube.com/watch?v=aMxJ0Kn1r6o>] vgl. Schmidt-Rede wird Viral-Hit "Der Terrorismus hat auf Dauer keine Chance". In: Berliner Zeitung 22.12.2016 [<http://www.berliner-zeitung.de/25361826>].

gegen die Rote Armee 1989 in Afghanistan: zahlreiche in asymmetrischer Kriegsführung erfahrene Kämpfer kehren mehr oder minder motiviert in ihre Heimatländer zurück – und mit ihnen auch die Fähigkeiten zu größeren und wirksameren Terroranschlägen. Die Rückkehrer aus Afghanistan bildeten seinerzeit zum einen in ihren Heimatländern die Aufbauorganisation für neue Terrorgruppen: so in Algerien, Indien (Kaschmir), Indonesien, Jemen, Russland, Somalia, Usbekistan und auf den Philippinen. Hinzu kamen solche, die anderen Konflikten weiterkämpften, wie u.a. Mudschahedin-Brigaden auf Seiten der Bosnischen Muslime im Bosnienkrieg, deren Zahl auf circa 6.000 Kämpfer aus Afghanistan, Albanien, Tschetschenien, Ägypten, Iran, Jordanien, Libanon, Pakistan, Saudi-Arabien, Sudan, Türkei und Jemen geschätzt wird. Ein Teil verblieb nach 1995 in Bosnien. Auch in Tschetschenien kämpften diese Veteranen – und durch sie neu angeworbene radikalisierte Muslime wie Konvertiten. Hier wurden auch deutsche Islamisten erstmals Aktenkundig. Der russische Generalstab vermeldete im November 2003, dass unter getöteten Kämpfern neben drei Türken auch der Deutsche Thomas Fischer (\* 1978) aus Ulm sei – und dass er bereits der dritte getötete Deutsche auf Seiten der Tschetschenischen Terroristen gewesen sei. Zuvor waren schon in Kaschmir zwei Niederländer marokkanischer Abstammung bei Kämpfen getötet worden. Parallel dazu zieht sich die Serie erfolgreicher wie vereitelter Anschläge von Al Qaida seit 1993, kulminierend am 11. September in den USA, aber auch damit keinesfalls endend. Es lohnt sich, sich die Dimension der Anschläge und auch der vereitelten nochmals vor Augen zu führen, da viele schon wieder in Vergessenheit geraten sind.<sup>6</sup> Aus diesen Milieus nationaler Terrorgruppen

heraus rekrutierten sich die Attentäter für weltweiten Anschläge und ab 2004 zusehends im Irak – auch wieder verstärkt als Untergrundkämpfer gegen die US-Besatzer und kurdische wie schiitische Bevölkerungsgruppen beziehungsweise deren Sicherheitskräfte. In dieser Zeit und insbesondere mit der Formierung des Islamischen Staats und seiner Ausrufung des Kalifats, zog es auch immer mehr deutsche Islamisten als Kämpfer und Selbstmordattentäter nach Syrien und in den Irak.

Somit wird Deutschland jetzt erstmals eine Rückkehrerwelle erleben, wie sie andere Staaten bereits nach 1989 durch Rückkehrer aus Afghanistan mit den oben ausgeführten Konsequenzen hinter sich haben. Dies sollte die deutschen Sicherheitsbehörden daher auch nicht völlig unerwartet treffen, die Frage ist nur die Quantität und Qualität der Rückkehrer und potentiellen Terroristen, wie solche aus anderen Ländern, die in mögliche terroristischen Operationen eingebunden werden könnten. Hier haben die laufenden Diskussionen um den Attentäter vom Breitscheidplatz bereits gezeigt, dass die Sicherheitsbehörden an Grenzen kommen, was allein die Beobachtung sogenannter Gefährder betrifft. Erschwert wird dies noch durch die zum Teil völlige intransparente Identität der Mehrzahl der seit 2015 nach Deutschland gekommener Migranten und Flüchtlinge. Mangels Ausweispapieren und der Möglichkeit, diese unter anderem in Syrien mit dortigen Behörden abgleichen zu können, ist oft keine belastbare Überprüfung durch die ohnehin oft am Limit arbeitenden Behörden möglich. Ein Umstand, den sich auch der Berlin Attentäter vom Breitscheidplatz mit mehreren Identitäten zunutze machen konnte.

Im Kern heißt das aber, dass man sich im Bereich innerer Sicherheit auf einen Personenkreis einstellen muss, der über militärische Fähigkeiten und Erfahrungen der asymmetrischen Kriegsführung verfügt. Zu diesen Fähigkeiten gehört unter anderem der Bau und Einsatz improvisierter Sprengsätze (englisch IED). Fachleuten ist es zudem kein Geheimnis, dass

der illegale Erwerb auch von Kriegswaffen in Deutschland kein größeres Problem darstellt, von der Handgranate bis zum Schnellfeuergewehr. Hier wirken noch die geplünderten Depots der Balkankriege nach, vor allem auch 1997 in Albanien, die über die offenen Grenzen bequem gehandelt werden können. Damit ist aber schon eine weitere Schnittstelle beschrieben, die zur organisierten Kriminalität. Fast alle radikalisierten Attentäter der letzten Anschläge, hatten Berührungspunkte zu kriminellen Strukturen oder entstammten bereits vor ihrer Radikalisierung kriminellen Milieus. Beschaffungskriminalität, Waffenbesitz, gefälschte Pässe, Untertauschen und sich unter dem Radar der Sicherheitsbehörden zu bewegen und zu kommunizieren, mussten viele nicht erst beim IS lernen. Und sie können Netzwerke der organisierten Kriminalität für terroristische Zwecke nutzen.

Sind unsere Behörden darauf eingestellt? Verfügen sie über die adäquaten Fähigkeiten, Instrumente und Mittel sowie das entsprechend qualifizierte Personal in ausreichender Anzahl? Völlig neu, dürfte auch dieses Szenario nicht sein. Weder Al Qaida noch der IS haben den Terrorismus erfunden. Wenn einem der Durchblick fehlt, kann einem ein Rückblick helfen. Die letzte Phase massiven Terrors erlebte Deutschland vor ziemlich genau 40 Jahren, im sogenannten heißen Herbst 1977, durch die Anschläge, Entführungen und Morde der Roten Armee Fraktion (RAF). Ein kurzer Blick auf die Geschichte und Struktur der RAF zeigt, dass auch hier Beziehungen zur organisierten Kriminalität und arabischen-muslimischen Befreiungsbewegungen bestanden. Ja nicht wenige der deutschen Terroristen bekamen im Laufe der Zeit eine paramilitärische Ausbildung im Nahen Osten zur asymmetrischen Kriegsführung von Guerillas. Darüber hinaus agierten diese Gruppen in Deutschland, unter anderem beim Terroranschlag auf die Olympia-Mannschaft Israels 1972 in München oder leisteten den deutschen Terroristen Unterstützung, wie mit der Entführung der Lufthansamaschine Landshut 1977. Neue Erkenntnisse zum

<sup>6</sup> Vgl. Liste der Anschläge im Artikel <https://de.wikipedia.org/wiki/Al-Qaida> [4] R.R. Baxter: A Sceptical Look at the Concept of Terrorism, Akron Law Review 7 (1974), 380. [als PDF <http://urlby.de/73gZ41D>] Vgl. auch Vgl. auch Gen Golder / Georg Williams What is 'Terrorism'? Problems of Legal Definition, University of NSW Law Journal, Vol. 27, No. 2, pp. 270-295, 2004 [als PDF <http://urlby.de/Gny2GW4>].

Mord am Deutsche Bank Chef Alfred Herrhausen deuten darauf hin, dass hier ein panzerbrechender improvisierter Sprengsatz (IED), ggf. iranischen Ursprungs, verwendet wurde, der später noch im Irak vielen Fahrzeugen der US-Truppen zum tödlichen Verhängnis werden sollte. Daher musste Deutschland seinerzeit Antworten auf eine völlig neue Form und Qualität von Gewalt finden, wie den Aufbau der GSG 9, die Verstärkung des BKA, ... . Es gibt nicht wenige aktive Polizeibeamte, die noch aktiv die späten 1980er Jahre miterlebt haben. Deren Ausbildung war noch deutlich von den Erfahrungen der RAF Zeit geprägt. Sie verfügen noch über Fähigkeiten, die später sukzessive aus der Ausbildung herausfielen oder nicht mehr Schwerpunkte waren. Hier sind gegebenenfalls Anknüpfungspunkte ebenso wie bei Beamten, die in den letzten Jahren in Auslandsverwendungen der EU oder der UN Erfahrungen in Krisen- und Konfliktgebieten gewonnen haben, in denen islamistischen oder andere Terrorgruppen aktiv sind. Aus eigener Erfahrung und vielen Gesprächen mit Polizeibeamten während und nach solchen Auslandseinsätzen, scheint hier viel Wissen brach zu liegen, das wieder daheim nicht abgefragt wurde, geschweige denn zu sinnvollen Anschlussverwendungen geführt hätte, um dieses in den Dienstbetrieb einfließen zu lassen.

Dies führt mich noch zu einem abschließenden rechtlichen Aspekt des Terrorismus. Was ist eigentlich Terrorismus und ein Terrorist? In einer Abhandlung über den Begriff „Terrorismus“ aus juristischer Sicht hinterfragte schon 1974 der Richter am Internationalen Gerichtshof Richard Baxter kritisch die durch das Ad Hoc Komitee der UNO 1973 eingeführt Definition von Terrorismus. Im damaligen Kontext von Entkolonialisierung, Befreiungsbewegungen und daraus resultierenden Kriegen hing es vom Blickwinkel des Betrachters ab, wer ein patriotischer Soldat, eine Krimineller, ein Befreiungskämpfer oder gar ein Terrorist war. Baxter kommt als Jurist angesichts dieses Dilemmas zu dem Schluss: „Wir haben allen

Grund zu bedauern, dass uns überhaupt ein Rechtsbegriff ‚Terrorismus‘ auferlegt wurde. Der Begriff ist unpräzise; er ist mehrdeutig; und vor allem dient er keinem praktischen juristischen Zweck.“[4] Walter Laqueur formulierte dieses Dilemma 1977 ähnlich: „In letzter Zeit wird der Begriff Terrorismus ... in so vielen verschiedenen Bedeutungen benutzt, dass er fast völlig seinen Sinn verloren hat.“<sup>7</sup>

Die oben aufgeführten Ursprünge des Terrorismus bzw. Terroristen, der 2016 auch Deutschland mit mehreren Anschlägen mit voller Wucht getroffen hat, zeigen deutlich die oft fließenden Grenzen. Die afghanischen Mudschaheddin, unterstützt vor allen von den USA via Pakistan, waren nach landläufiger westlicher Auffassung Guerillas, Freiheitskämpfer, die sich gegen eine brutale sowjetische Besatzungsmacht zur Wehr setzten. Dabei wurden sie auch von ausländischen Kämpfern unterstützt, die später zu den Gründern von Al Qaida gehörten. Einige gingen in den 1990er Jahren nach Bosnien, wo sie eingegliedert in die bosnisch-muslimische Armee im Unabhängigkeitskrieg mitkämpften; zum Teil wieder mit aktiver westlicher Unterstützung. Von der jeweiligen Gegenseite, wurden sie aber gerne als Terroristen bezeichnet. In der Ukraine erleben wir diese auch: Der Freiheitskämpfer der einen Seite ist der Terrorist oder Kriminelle aus Sicht der anderen Seite. Und das Selbstverständnis der PLO und andere palästinensischer Gruppen war und ist das eines legitimen Kampfes um Freiheit und Unabhängigkeit. Bei diesen wiederum gingen Mitglieder der RAF in den 1970er Jahren in die Schule oder tauchten bei ihnen zeitweise unter und unterstützten sich. In Syrien beansprucht aktuelle wohl jede Gruppe für eine gerechte Sache zu kämpfen.

Der Journalist Franz Würdemann versuchte 1977 auf dem Höhepunkt des RAF Terrorismus kurz

<sup>7</sup> Walter Laqueur in: Terrorismus in der demokratischen Gesellschaft, Protokoll der 59. Tagung des Bergedorfer Gesprächskreises, hrsg. vom: Bergedorfer Gesprächskreis, Hamburg 1978.

und knapp folgende Definition: „Der Guerillero will den Raum, der Terrorist will dagegen das Denken besetzen.“<sup>8</sup> Daran schloss sich Andreas Elter an und führte in seinem Aufsatz „Die RAF und die Medien“ 11 Kriterien einer Terroristischen Vereinigung auf, vor allem in Abgrenzung zu Guerillas, als die sich Terroristen immer wieder selber bezeichnet haben, so die RAF als „Stadtguerilla“<sup>9</sup>. Würdemann und Elter haben mit ihren Ansätzen viel für sich.

Allein im Ringen um die richtige Antwort auf den Terrorismus von Al Qaida und des IS, hat sich das Paradox ergeben, dass wir vielfach mit dem ehemaligen US-Präsidenten George W. Busch vom „Krieg“ gegen den „Terror“ sprechen. Hier wurde immer wieder berechtigt eingewendet, dass ein Krieg gegen Terroristen nicht zu gewinnen sei, da sich dieser schlicht den Möglichkeiten und Fähigkeiten des Zugriffs durch einen militärischen Gegner entziehe. Terroristen führten eben keinen Krieg, sondern gehen in der Zivilbevölkerung auf und verüben aus dieser Deckung heraus ihre Anschläge. Und wie Würdemann sagt, sie wollen kein Territorium besetzen, sondern das Denken durch Unsicherheit, Angst und Schrecken.

Aber stimmt das? War das Endziel der RAF „nur“ Angst und Schrecken zu verbreiten? Wohl nicht. Die RAF strebte eine revolutionäre Veränderung Deutschlands hin zum Sozialismus an, wengleich über den Weg einer Revolution unter Einsatz von Gewalt gegen die herrschende Klasse. Einer der linken Wortführer der Studentebewegung Jürgen Habermas, nicht weniger gesellschaftlichen Wandel anstrebend, warf der Gründergeneration der RAF vor, die Lage und Stimmung im Lande völlig falsch eingeschätzt zu haben. Der Wandel lasse sich derzeit nicht durch Gewalt initiieren, sondern müsse gewaltfrei erfol-

<sup>8</sup> Franz Würdemann; Terrorismus. Motive, Täter, Strategien. Piper-Verlag München/Zürich 1977.

<sup>9</sup> Andreas Elter: Die RAF und die Medien. Ein Fallbeispiel für terroristische Kommunikation. In: Wolfgang Kraushaar (Hrsg.): Die RAF und der linke Terrorismus, Hamburger Edition HIS Verlag, Hamburg 2007.

gen, u.a. durch Infiltration und Instrumentalisierung des Bildungssystems – Umerziehung statt blutiger Umsturz. Letztlich war die Strategie der RAF eben doch auf einen politischen Machtwechsel und Machtübernahme in einem Territorium ausgerichtet.

Ähnliches lässt sich – wenn auch unter ganz anderen Vorzeichen – bei den Ideologen vor Vordenkern von Al Qaida und dem IS beobachten, wobei beiden Gruppen auf Gewalt setzten, um letztlich den Gegner zu besiegen und für den Islam alter Territorien von Ungläubigen zu befreien und das „Haus des Islam“, seinen Machtbereich, territorial auszubreiten. Was Al Qaida und IS dabei trennt, ist der Versuch des IS, bereits jetzt ein Territorium, das Kalifat, zu erobern, zu sichern und von dort weiter auszubreiten. Al Qaidas Führung sieht dafür derzeit noch keine sichere Grundlage und setzt weiter auf eine sukzessive Zermürbung des Gegners, ohne ihm eine Angriffsfläche zu bieten, die ein zu haltendes Territorium immer bietet.

Der Terrorismus ist daher nicht als Selbstzweck sondern Teil einer mittel- und langfristigen Strategie zu verstehen, ein Instrument, das zu einer bestimmten Zeit in einem bestimmten Kontext seine Berechtigung hat. In diesem Falle einem total überlegenen konventionellen Gegner möglichst wenig Angriffsfläche zu bieten und zugleich mit einer Vielzahl von Anschlägen zu ermüden und so langfristig zu besiegen. Eine Variation davon ist auch der Guerillakrieg, wenn zum Beispiel einheimische Kämpfer die Vorteile von Ortskenntnissen und Unterstützung der eigenen Bevölkerung nutzen können wie im Irak. Aber auch da setzten Guerillas auf asymmetrische Kriegsführung und nicht auf typisches konventionelles Beherrschen eines Raumes oder Territoriums. Die Bevölkerung dient als Rückzugsraum, man errichtet keine formelle nach außen sicht- und angreifbaren Verwaltungsstrukturen. Der IS hat das versucht und wird damit ggf. scheitern.

Was heißt das nun für Terrorabwehr und Terrorprävention in

Deutschland nach dem Anschlag vom 19. Dezember 2016 am Breitscheidplatz? Worauf müssen sich Bevölkerung und der Staat mit seinen Sicherheitskräften einstellen? Wie können sie effektiv und effizient reagieren?

Eine Lehre spätestens seit der Niederlage der Sowjetunion in Afghanistan ist, dass sich derartige Guerillabewegungen mit der Option des Terrorismus nicht mit konventionellen Mitteln beherrschen geschweige denn besiegen lassen. Russland hat als eine der Lehren aus dem Debakel der Niederlage in Afghanistan unter anderem massiv seine eigenen Fähigkeiten zur asymmetrischen Kriegsführung und Bekämpfung von Terrorismus ausgeweitet. Welche Fähigkeiten man dabei entwickelt hat, zeigten 2014 die Operationen zur handstreichartigen Besetzung und Annektierung der Krim die vor allem hoch professionell agierende Spezialkräfte durchgeführt haben. Ob Russland hier ein Vorbild sein kann, ist eher in Frage zu stellen. Unser Handeln muss immer auch mit unseren Grundwerten und rechtsstaatlichen Regeln konform sein. Aber das schließt keinen asymmetrischen Ansatz aus. Im Kern haben wir diesen bereits mit den vorhandenen deutschen Spezialkräften in Polizei und Militär. Dabei ist zu beachten, dass Terroristen wie Guerillas fast immer ihre Anschläge sorgfältig planen und eine umfangreiche Aufklärung betreiben. Wer genauer nachdenkt, erkennt hier auch eine Parallele zu Spezialkräften, die jeden Einsatz, wo immer möglich, sorgfältig aufgrund einer umfangreichen Voraufklärung durchführen; oft geschieht das durch eigene Aufklärungskräfte ergänzt durch nachrichtendienstliche Erkenntnisse.

In der Quintessenz heißt das, die wenigsten Terroranschläge werden spontan aus dem Blauen heraus erfolgen. Das Vorgehen von Terroristen orientiert sich – auch schon aus ihre Biographie und Ausbildung durch Guerillas – an den Prinzipien einer asymmetrischen Kriegsführung. Motivation des Handelns und folglich die Zielauswahl sind eine andere, die es zu verstehen gilt. Das prinzipi-

elle Vorgehen ist so durchaus berechen- und nachvollziehbar. Während militärischen Spezialkräfte kritische Infrastruktur des Gegners lahmlegen oder Führungskräfte ausschalten oder gefangen nehmen, suchen Terroristen gemäß ihrer Logik Objekte mit hohem Symbolwert im Wertesystem ihrer Gegner und versuchen, eine möglichst große Zahl an Personen am selben Ort zu schädigen. Eine andere Taktik kann sein, durch gezielte Angriffe auf Sicherheitskräfte, vor allem die Messerangriffe der letzten Jahre, diejenigen zum Ziel zu machen, die eigentlich – z.B. eine Streife am Bahnhof – für ein Gefühl der Sicherheit sorgen sollen. Zugleich wollen sie diese Sicherheitskräfte extrem verunsichern. Eine ähnliche Wirkung erzielen in Spezialkräften Scharfschützen.

Abschließend würde das heißen, dass die Antwort nicht in einem massiven Aufgebot von konventionellen Sicherheitskräften auf der Straße liegen kann. In Frankreich häuft sich die Kritik, dass die hier eingesetzten Kräfte schnell überdehnt werden, andere Aufgaben liegen bleiben und man dadurch keinen Anschlag wirklich verhindern kann. Es ist zu fragen, welche Fähigkeiten und Instrumente wie diesbezügliches Personal wir benötigen, die asymmetrisch denken und handeln können. Zugleich braucht dies eine hoch professionelle Gegenaufklärung. Aufklärung muss dabei ggf. auch neu gedacht werden. Neuere angewandte Verhaltensforschung hinsichtlich der Tätererkennung schon in der Frühphase der Aufklärung von Terrorzielen oder unmittelbar vor der Tat haben es oft noch nicht in unsere staatlichen Sicherheitskräfte oder privaten Sicherheitsdienste geschafft; auch nicht der Erfahrungswert, dass Frauen hier besser beobachten und zuverlässiger Täter identifizieren. Spiegelt sich das in der Zusammensetzung des Personals wider? Insbesondere in England, bedingt durch die Terrorerfahrung mit der IRA und in Israel, gibt es hier schon einige beachtenswerte best practice und Erfahrungswerte. Sicher auch in der Diskussion um zu viel oder zu wenig Videoüberwachung, Einsatz von Pol-



lern, und vieles andere mehr. Einige Unternehmen, deren Objekte einem erhöhten Terrorrisiko unterliegen, lassen sich regelmäßig durch ehemalige Angehörige von Spezialeinheiten ausspähen und Penetrationstests durchführen, um so Erkenntnisse über Lücken im System für einen asymmetrisch vorgehenden Terroristen zu identifizieren.

Last but not least – wie im Personenschutz viel mit dem Verhalten der Schutzperson steht und fällt, ist das ebenso mit der Bevölkerung beim Thema Terrorismus. An dem Punkt hat Wördemann dann doch recht: Sie wollen das Denken der Menschen besetzen, lähmen, steuern, dahin wo es ihnen nützt. Deutschland hat über fast zwei Jahrzehnte keine einschlägige Terrorerfahrung gemacht, schon gar nicht mit Anschlägen, die sich gegen die breite Masse richten. Dafür war die erste Reaktion auf den Anschlag in Berlin gut – wenngleich die Nacharbeit über politischen Schuldzuweisungen weniger glücklich verläuft. Die Kunst, sich nicht vom Terror Angst, Unsicherheit und ein vom Terroristen erwünschtes Verhalten aufdrängen zu lassen, will gelernt sein. Wobei das nie ein resignierendes, „Man kann ja doch nichts machen. Wir müssen mit dem Terror leben lernen.“ sein darf, sondern das Gegenteil: Teil der Überwindung und des Besiegens von Terror ist Haltung im Umgang damit. Dabei helfen kann vielleicht das neue Büchlein von Florian Peil.<sup>10</sup> Wer Terrorismus verstehen lernt, der verliert auch Angst davor und weiß wie er damit souveräner umgehen kann, damit Terroristen nicht ihr Denken besetzen können. Das heißt, um auf Helmut Schmidts Fernsehrede 1977 zurückzukommen, es gilt, „trotz unseres Zornes, einen kühlen Kopf behalten“ und nüchtern festzustellen, „dass es eine absolute Sicherheit nicht gibt.“ Zwar wollen Terroristen „den demokratischen Staat und das Vertrauen der Bürger in unseren Staat aushöhlen“, aber der „Terrorismus hat auf Dauer keine Chance. Denn gegen den Terrorismus steht nicht nur der Wille der staatlichen Organe,

sondern der Wille des ganzen Volkes“<sup>11</sup> Und es braucht Verantwortungsträger, Krisenmanager, die in solchen Augenblicken das glaubwürdig und unaufgeregt sagen können.

*Friedrich Christian Haas*

Friedrich Christian Haas, MA, Jahrgang 1968, nach seiner Tätigkeit als Zeitsoldat im Objektschutz der Luftwaffe studierte er Internationale Beziehungen in Köln und Simferopol (Krim, Ukraine) und absolvierte Lehrgänge in Verhandlungsführung (Harvard Program on Negotiation) sowie Change-Management (SYMA). Als Berater deutscher Kommandeure in Auslandseinsätzen befasste er sich zunehmend mit Terrorismus und gewaltbereiten traumatisierten Einzeltätern. Als Geschäftsführender Gesellschaft der AKE | SKABE GmbH berät er Kunden v.a. wie Risiken wie Krieg, Terrorismus, u.a. Gefahren für Unternehmensstandorte im In- und Ausland sowie von Mitarbeitern auf Reisen gemeistert werden können.

Der Beitrag gibt die persönliche Auffassung des Autors wieder.

Erstmals erschienen unter:

[www.veko-online.de/titel/der-terrorismus-hat-auf-dauer-k-eine-chance.html](http://www.veko-online.de/titel/der-terrorismus-hat-auf-dauer-k-eine-chance.html)

## THEMEN

### Smearing Gorka may mark return of US yellow journalism

The recent media onslaught and accusations of Nazi links against US President Donald Trump's counterterrorism adviser, Dr Sebastian Gorka, seems to highlight the alarming decay of US media and the return of yellow journalism.

According to the State Department's history website, „yellow journalism was a style of newspaper reporting that emphasized sensationalism over facts. During its heyday in the late 19th century it was one of many factors that helped push the United States and Spain into war in Cuba and the Philippines, leading to the acquisition of overseas territory by the United States.“ The website acknowledged that the dramatic style of yellow journalism contributed to „creating public support for the Spanish-American War, a war

that would ultimately expand the global reach of the United States“.

With the current hysteria in the Beltway regarding the „Russia threat“, and opposition to the Trump administration's proposal of working with Moscow to counter ISIS and the trans-regional Salafi jihadist movement, one wonders if this is a repeat of history goading the „indispensable nation“ into another war.

Interestingly, the Council on American-Islamic Relations (CAIR), a controversial organization that moderate Sunni ally the United Arab Emirates has listed as a terrorist organization for its ties with the Muslim Brotherhood, has allied with some of these media outlets in their attempts to oust Seb Gorka. This is eerily similar to how they had coalesced to oust Michael Flynn – another Trump adviser who understood the expediency of working with Russia to counter Salafi terrorism in Syria and help stabilize the Middle East. However, it seems CAIR has a stake in overthrowing the Syrian government and installing a Muslim Brotherhood-type replacement, similar to what happened with Egypt and Mohamed Morsi.

In 2012, CAIR leader Yaser Tabbara was the spokesman for the Syrian „opposition“ that was already infested with al-Qaeda and Salafi extremists, and worked closely with the Barack Obama administration to topple the Syrian government. However, the entry of Russia into the Syrian conflict in 2015 complicated the regime-change agenda, and in December 2016 when CAIR's Los Angeles director Hussam Ayloush revealed his disdain for Russia and celebrated the deaths of 92 Russians in a jet crash en route to Syria – consisting mainly of 60 musicians, with some journalists and doctors – he received a swift rebuke and condemnation. Perhaps we are witnessing a resurgence of the regime-change interventionists and yellow journalism.

### Regime change in Syria – again?

Already there has been an unhealthy uptick of news stories mis-

<sup>10</sup> Florian Peil: Terrorismus - wie wir uns schützen können. Murmann Verlag 2016.

<sup>11</sup> Deutscher Herbst: Helmut Schmidt: Fernsehansprache 1977 [YouTube [www.youtube.com/watch?v=aMxJ0Kn1r6o](http://www.youtube.com/watch?v=aMxJ0Kn1r6o)].

representing facts to mislead the American public and undermine the current administration's policies. These new policies include reversing the Obama administration's regime-change operations in Libya and Syria that further empower ISIS and al-Qaeda, and not supporting the North Atlantic Treaty Organization (Nato) as an instrument to provoke Russia unnecessarily or for „warmongering“, in the words of German Foreign Minister Frank-Walter Steinmeier. For example, in addition to US news coverage, Netflix and most recently HBO have shown films documented by the al-Qaeda-linked White Helmets to demonize the Syrian government as a human-rights abuser that needs to be toppled, similar to the 2003 campaign to overthrow the Iraqi government over the false existence of weapons of mass destruction.

Then there was the media blitz that President Trump snubbed German Chancellor Angela Merkel by refusing to shake her hand during her state visit, despite the fact he did shake her hand. Is the insinuation that perhaps because she supports Nato more than he does, and since he is supposedly a supporter of Russian President Vladimir Putin, he thus won't shake her hand?

Now Senator Rand Paul is the latest casualty in this Beltway anti-Russia hysteria, with fellow Senator John McCain accusing him of working for Putin simply by voting against admitting Montenegro to Nato, thereby putting additional burdens upon the shoulders of American soldiers and taxpayers to extract more blood and treasure.

Never mind that Senator Paul explained the folly of expanding „the monetary and military obligations

of the United States given the burden of our \$20-trillion debt“, with US troops already fighting endlessly in regime-change target countries of Iraq, Syria, Libya, Yemen, Afghanistan (and drone strikes in Pakistan), pledging to defend East Asian allies in addition to the 28 countries in Nato, and maintenance of some 800 military bases in more than 70 countries.

A house divided against itself cannot stand, and this unhealthy partisan environment only serves to paralyze US leadership and effectiveness in the international community. The current anti-Russia and anti-China hysteria is also unhelpful given they both of those countries have legitimate security interests in Syria and the Middle East, especially after years of US support for the Syrian „opposition“ that includes anti-Chinese militants.

Now it may be prudent to have a paradigm shift away from a zero-sum cold-war lens, to one of how in a multipolar/multi-partner world, Russia, China and the rising rest can supplement Western efforts to address the global pandemic of ISIS and Islamic extremism. Otherwise, with various al-Qaeda groups from China, Russia, and Central and Southeast Asia having merged with ISIS in Syrian jihad, should the US and Russia stumble into a military conflict, ISIS may actually come out the winner.

### **Three dogs and a bone**

Chinese strategist Liu Mingfu noted in the 20th century that Britain fought and won a war against Germany, but was so weakened and brought to its knees that it ceded its hegemonic position to the United States. Two dogs fought over a bone, and a third ran away with it – the US. Now if Washington and Moscow end up

fighting over a bone in the Middle East rather than coalescing to counter the global threat of terrorism, the third dog that runs away with the bone may be ISIS, with a clear path then to realize its global caliphate.

As for the stories bearing false witness against Gorka, many who know him are already stepping forward to testify on his character and the truth, including this author. I first knew Dr Gorka in 2011 as a fellow in the National Security Fellows Program, which he directed at the Foundation for Defense of Democracies (FDD), known for its research in support of Israel, US national security and counterterrorism. There he tried to instill in the fellows – selected mainly from the US defense and intelligence sectors – a sense of urgency to combat fascism and racism in all forms, and he has consistently written and spoken out against them since then.

It is thus both comical and tragic that his detractors would paint him as an anti-Semite or Nazi sympathizer and, sadly, help usher the US into a disturbing new era of yellow journalism.

---

*Dr. Christina Lin*

Dr. Christina Lin is a Fellow at the Center for Transatlantic Relations at SAIS-Johns Hopkins University, focusing on China-Middle East/Mediterranean relations. She was recently a Visiting Academic Fellow at the Mercator Institute for China Studies (MERICS) in Berlin and a former Transatlantic Academy Fellow at the German Marshall Fund of the United States. Dr. Lin has extensive US government experience working on China security issues, including policy planning at the US Department of Defense, the National Security Council, and US Department of State.

Opinions expressed in this contribution are those of the author.

This paper was first published March 22, 2017 in Asia Times.

### DEMOGRAPHIC WAR INDEX 2017: RANKING BY COUNTRY.

A national war index of between 2.5 and 8.0 indicates that 2,500-8,000 young men aged 15-19 are competing for the jobs and social positions of 1,000 retiring men aged 55-59. The higher the war index, the more likely it is that these young competitors will resort to crime, homicide, gang war, political coup, revolution, civil war, expulsion, genocide and war. Even an index below 2.5 may indicate volatility if combined with a stagnating or shrinking economy. If nations in the blue sectors [590-999 young following 1.000 old] consider war or intervention they act extremely careful because every fallen soldier — statistically his mother's only son or only child — will terminate his family line.

[Data for 2016 from: [https://esa.un.org/unpd/wpp/DataQuery/.](https://esa.un.org/unpd/wpp/DataQuery/)]

COPYRIGHT GUNNAR HEINSOHN; 25-01-2017

Uganda	8.08	Kenya	5.14	Syria	4.02	Samoa	2.75	Antigua&B.	2.00	Fr. Polynesia	1.50	Aruba	1.00	Japan	0.82
Zambia	7.52	S.-Sudan	5.02	Niger	4.01	Maldives	2.67	Saint Lucia	2.00	Sri Lanka	1.46	Barbados	1.00	Portugal	0.82
Lesotho	7.35	Sao Tome	5.00	Jordan	3.95	Fre. Guiana	2.60	Turkey	2.00	Puerto Rico	1.44	Cuba	1.00	Singapore	0.82
Malawi	7.04	Sierra Leone	4.99	Gabon	3.91	Eq. Guinea	2.53	Algeria	1.98	Uruguay	1.44	Curacao	1.00	Croatia	0.81
Zimbabwe	6.81	Guatemala	4.98	Cabo Verde	3.86	Mexiko	2.52	Qatar	1.90	Tunisia	1.43	Iceland	1.00	Lithuania	0.80
Mali	6.61	Madagascar	4.84	Honduras	3.75	Grenada	2.50	Lebanon	1.88	N. Caledonia	1.43	Seychelles	1.00	Canada	0.79
Burkina F.	6.46	Benin	4.80	Cambodia	3.72	Bhutan	2.47	Israel	1.87	Kazakhstan	1.37	US Virgin	1.00	Slovakia	0.78
Chad	6.40	Namibia	4.75	Nepal	3.65	Libya	2.46	Saudi Arabia	1.86	Réunion	1.36	China	0.99	Switzerland	0.77
Afghanistan	5.99	Liberia	4.74	Haiti	3.59	Egypt	2.45	Suriname	1.85	Azerbaijan	1.33	France	0.99	Greece	0.76
Senegal	5.87	Nigeria	4.74	Botswana	3.58	Ecuador	2.41	Colombia	1.84	Chile	1.32	Georgia	0.98	Ukraine	0.76
Angola	5.84	C. African R.	4.72	Micronesia	3.50	Guyana	2.40	Morocco	1.84	Albania	1.31	Thailand	0.98	Austria	0.75
Ethiopa	5.83	Sudan	4.65	Vanuatu	3.50	India	2.38	Brazil	1.81	N. Korea	1.27	United Kingd.	0.96	Bosnia & Herz	0.75
Iraq	5.80	Rep. Congo	4.55	Pakistan	3.39	Peru	2.37	Argentina	1.79	Mauritius	1.20	USA	0.96	Martinique	0.75
Gambia	5.79	Guinea-Bis.	4.45	Bolivia	3.24	Dominican R.	2.35	Fiji	1.77	U. Arab Em.	1.17	Luxembourg	0.95	Poland	0.71
Mozambique	5.77	Guinea	4.42	Djibouti	3.21	Myanmar	2.26	Iran	1.75	Guadeloupe	1.14	Moldova	0.92	Czech R.	0.70
Somalia	5.68	Timor-Leste	4.40	Tajikistan	3.21	Kyrgyzstan	2.25	Oman	1.70	Montenegro	1.10	Taiwan	0.88	Italy	0.70
Swaziland	5.62	C. d'Ivoire	4.37	South Africa	3.19	Turkmenistan	2.25	Kuwait	1.69	New Zealand	1.10	Sweden	0.87	Spain	0.69
Rwanda	5.59	Mayotte	4.33	Belize	3.17	Uzbekistan	2.22	S. Vincent	1.67	Ireland	1.08	Armenia	0.86	Bulgaria	0.68
Palestine	5.46	Comoros	4.30	Nicaragua	3.12	Jamaica	2.19	Brunei	1.64	Serbia	1.08	Malta	0.86	Estonia	0.68
[Gaza >6.00]												Romania	0.86	Russia	0.67
Cameroon	5.42	Burundi	4.21	El Salvador	3.02	Kosovo	2.15	Guam	1.60	Cyprus	1.06	Netherlands	0.85	Belarus	0.66
Eritrea	5.41	Ghana	4.19	Kiribati	3.00	Mongolia	2.15	Costa Rica	1.59	Trinidad & Tob.	1.05	S.-Korea	0.85	Germany	0.65
Yemen	5.41	Mauritania	4.17	Tonga	3.00	Venezuela	2.15	W. Sahara	1.57	Australia	1.03	Finland	0.84	Macao	0.65
D.R. Congo	5.29	Papua N.G.	4.13	Bangla Desh	2.98	Panama	2.06	Vietnam	1.53	Norway	1.02	Hungary	0.84	Slovenia	0.63
Tanzania	5.22	Solomon Is.	4.13	Paraguay	2.87	Indonesia	2.05	Bahamas	1.50	Denmark	1.01	Channel Is.	0.83	Latvia	0.62
Togo	5.21	Laos	4.05	Philippines	2.84	Malaysia	2.04	Bahrein	1.50	Macedonia	1.01	Belgium	0.82	Hong Kong	0.59

### DEMOGRAPHIC WAR INDEX 2017: WORLD MAP

A national war index of between 2.5 and 8.0 indicates that 2,500-8,000 young men aged 15-19 are competing for the jobs and social positions of 1,000 retiring men aged 55-59. The higher the war index, the more likely it is that these young competitors will resort to crime, homicide, gang war, political coup, revolution, civil war, expulsion, genocide and war. Even an index below 2.5 may indicate volatility if it is combined with a stagnating and/or shrinking economy. [Data for 2016 from: [https://esa.un.org/unpd/wpp/DataQuery/.](https://esa.un.org/unpd/wpp/DataQuery/)]

COPYRIGHT GUNNAR HEINSOHN; 25-01-2017

