Herbert Saurugg, MSc, Mjr
herbert@saurugg.net
www.herbert.saurugg.net

Hybride Bedrohungspotenziale im Lichte der Vernetzung und Systemischen Denkens

Seit dem Ende des Kalten Krieges vor 25 Jahren haben sich die Bedrohungsbilder und -szenarien wesentlich verändert. Von einer relativ einfach überschaubaren bipolaren Welt sind wir heute in einer hochkomplexen, sehr dynamischen und zunehmend turbulenteren Zeit angelangt. Die Fachwelt verwendet dafür auch den Begriff VUCA[1] - volatil, unsicher, komplex und ambivalent. Diese Entwicklungen betreffen so gut wie allen Lebensbereiche. Gleichzeitig haben sich unsere altbewährten Denkmuster kaum verändert. Doch reicht das aus, um mit den neuen Herausforderungen zurecht zu kommen?

Ein wesentlicher Treiber für die Veränderungen war die exponentiell ansteigende Verbreitung von Informationstechnologien (IT; Computer, IT-Lösungen und vor allem die technische Vernetzung, im speziellen das Internet), die Basistechnologien des 5. Kondratieff-Zykluses. Diese beschreiben zyklische Wirtschaftsentwicklungen in der Dauer von rund 40-60 Jahren, wo je eine Basistechnologie/-innovation[2] die Entwicklungen bestimmt. Demnach befinden wir uns derzeit im abklingenden 5. bzw. am beginnenden 6. Zyklus, also in einer Phase des Umbruches.

Netzwerkgesellschaft

Parallel dazu hat sich seit den 1950er Jahren die Netzwerkgesellschaft zu entwickeln begonnen. Zuerst sehr langsam. Mit der breiten gesellschaftlichen Durchdringung mit Informationstechnologien Anfang des 21. Jahrhunderts nahm die Geschwindigkeit deutlich zu. Während die Industriegesellschaft durch Standardisierung, Synchronisierung, Zentralisierung (hierarchische Strukturen) oder durch Konzentration (Massenheere, Massenmedien, Massenproduktion, Arbeit in der Fabrik) gekennzeichnet ist, ist die nun sich etablierende Netzwerkgesellschaft durch genau gegenteilige Kennzeichen charakterisiert.[3] Es kommt zu einer Individualisierung (Produkte, Lebensweise), zur Autokoordinierung (über/durch das Internet, ad-hoc Vernetzungen), zur Dezentralisierung (Energiebereitstellung, bzw. verlieren Nationalstaaten ihre Bedeutung) und zur dynamischen Vernetzung statt Konzentration, was wiederum hierarchische Strukturen in Frage stellt. Die Netzwerkgesellschaft etabliert sich neben der Agrar- und Industriegesellschaft als dritte wesentliche Gesellschaftsform. Unabhängig von der jeweiligen religiösen oder wirtschaftlichen Weltanschauung.

Der Transformationsprozess von der Agrar- zur Industriegesellschaft, zwischen ca. 1650 und 1750, ist nicht reibungsfrei verlaufen und hat so manches bis dahin gültige Weltbild über den Haufen geworfen. Ähnliche Turbulenzen zeichnen sich auch heute ab. Dabei wird die bisherige Agrar- und Industriegesellschaft nicht vollständig abgelöst, sondern sie entwickelt sich

1 Englisch: Volatility, uncertainty, complexity and ambiguity.

2 1. Dampfmaschine, Frühmechanisierung, Industrialisierung → Kraft; 2. Eisenbahn → Transport; 3. Elektrotechnik- und Schwermaschinen; Chemie → Verarbeitung; 4. Integrierter Schaltkreis, Kernenergie, Transistor, Automobil → Automatisierung; 5. Informations- und Kommunikations-Technik → Integration, Globalisierung; 6. Wahrscheinlich Psychosoziale Gesundheit, Biotechnologie, Bildung.

3 Vgl. Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0. Masterarbeit: 2013 unter URL: http://www.saurugg.net/wp/wp-content/uploads/2014/10/die_netzwerkgesellschaft_und_krisenmanagement_2.0.pdf [22.10.14].

parallel dazu, was zusätzliche Herausforderungen schafft. Konflikte haben daher häufig mit den damit verbundenen unterschiedlichen Wertemustern und Denkweisen zu tun und weniger mit den häufig vorgeschobenen Motiven, wie etwa bei scheinbaren Religionskriegen.

Bemerkenswert ist, dass sich die abzeichnenden Lösungen und Denkweisen der Netzwerkgesellschaft viel stärker mit der Agrar- als mit der Industriegesellschaft decken, was auch mit der vorherrschenden Energienutzung zu tun hat. Die Industriegesellschaft war durch das fossile Zeitalter geprägt, dass wahrscheinlich noch weitreichende Nachwirkungen haben wird, wie etwa beim sich abzeichnenden Klimawandel. Darüber hinaus ist zu erwarten, dass Lösungen der Netzwerkgesellschaft, beispielsweise dezentrale Energieversorgungssysteme oder Produktionsmethoden, auch zu einer positiven Weiterentwicklung in der Agrargesellschaft, etwa in entlegenen Regionen, beitragen können. Damit könnten auch wichtige sicherheitspolitische Ziele, wie die Stabilisierung vor Ort, gefördert und leichter erreicht werden. Wenn ein würdiges Leben vor Ort möglich ist, sinkt der Migrationsdruck bzw. das Konfliktpotential. Die durch die Industriegesellschaft geschaffene Chancenungleichheit oder Ressourcenprobleme könnten damit wieder reduziert werden. Das Ende des noch vorherrschenden Wachstumsparadigmas zeichnet sich ab. Es ist auf einer Welt mit begrenzten Ressourcen nicht nachhaltig und wirkt selbstzerstörerisch. Die wesentliche Frage dabei ist noch, wie und ob uns eine Abkehr ohne einer „Schöpferischen Zerstörung“[4] gelingen kann.

Aus dieser Perspektive erscheinen so manche Widersprüchlichkeiten und aktuelle Entwicklungen in einem anderen Licht. Etwa die Auflösung der häufig künstlich geschaffenen Nationalstaaten im arabischen Raum, oder, dass es durch eine dezentrale Energieversorgung zu massiven Machtverschiebungen kommt, die von den etablierten und konzentrierten/zentralisierten Machthabern wahrscheinlich nicht ohne weiteres hingenommen werden. Natürlich berücksichtigt das hier dargestellte einfache Ursache-Wirkungsmodell viele Aspekte nicht, die auch noch eine Rolle spielen. Dazu aber noch mehr weiter unten.

Es gibt verschiedene Modelle, die aus der Vergangenheit zyklische Entwicklungen ableiten bzw. beschreiben. Gemein ist ihnen, dass sie eine große Umbruchphase für diese Dekade prognostizieren.[5] Die Anzeichen für größere Umbrüche sind bereits mehr als deutlich, wobei die tatsächliche Tragweite erst im Nachhinein beurteilt werden kann.

Um das Thema hybride Bedrohungen im Lichte dieser Entwicklungen besser beleuchten zu können, ist es noch erforderlich, sich mit einigen Grundlagen auseinanderzusetzen. Eine zentrale Rolle spielen dabei Systeme.

Systeme

Ein System beschreibt die funktionale Zusammensetzung von verschiedenen Systemelementen zu einem Ganzen. Entscheidend dabei sind die Beziehungen zwischen den Systemelementen, das „Wirkungsgefüge“. Denn ohne Beziehungen hat man kein System, sondern nur

4 Ein Begriff aus der Makroökonomie, dessen Kernaussage lautet: Jede ökonomische Entwicklung (im Sinne von nicht bloß quantitativer Entwicklung) baut auf dem Prozess der schöpferischen bzw. kreativen Zerstörung auf. Durch eine Neukombination von Produktionsfaktoren, die sich erfolgreich durchsetzt, werden alte Strukturen verdrängt und schließlich zerstört. Die Zerstörung ist also notwendig – und nicht etwa ein Systemfehler –, damit Neuordnung stattfinden kann. Quelle: https://de.wikipedia.org/wiki/Schöpferische_Zerstörung [26.10.14].

5 Vgl. Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0. Masterarbeit: 2013 unter URL: http://www.saurugg.net/wp/wp-content/uploads/2014/10/die_netzwerkgesellschaft_und_krisenmanagement_2.0.pdf [22.10.14].

eine Ansammlung oder einen Haufen.[6] Entscheidend ist, dass ein System mehr ist, als die Summe der Einzelelemente. Was nicht weiter spektakulär klingt, hat es dennoch in sich. Unzählige Beispiele zeugen davon, wo diese einfache Weisheit unzureichend berücksichtigt wurde und es daher zu weitreichenden negativen Konsequenzen kam. Ob das im Umweltbereich (Wildbachverbauungen, Umweltverschmutzung), bei der Entwicklungshilfe (Brunnenbau) oder auch beim Finanzcrash 2007/2008 mit zahlreichen Folgekrisen war, immer wurde diese einfach klingende Aussage unzureichend berücksichtigt.

Auch wenn man alle chemischen Elemente des menschlichen Körpers kennt und zur Verfügung hat, ergibt das noch keinen Menschen. Ein Orchester ist viel mehr als die Summe von perfekten Einzelmusikern. Immer spielen die „unsichtbaren Fäden" zwischen den Einzelelementen eine Rolle, die erst einen Mehrwert schaffen.

Was konkret ein System ist, hängt von der jeweiligen Betrachtung und Detaillierung ab. Ob man etwa ein Molekül, eine Zelle, ein Organ, den Menschen, oder sein Sozialsystem betrachtet. Ein System kann auch eine inhaltliche, eine zeitliche und/oder eine soziale Grenze zu seiner Umwelt aufweisen, die von den Systemauswirkungen betroffen sein mag, aber keinen Einfluss auf das Wirkungsgefüge hat.[7] Daher darf ein System nicht als etwas absolutes verstanden werden.

Grundsätzlich wird zwischen einfachen und komplexen Systemen unterschieden. Einfache Systeme (Maschinen) stellen kein großes Problem dar, was ihre Steuerung, Regulierung und Lenkung – kurz, ihre Kontrolle – betrifft. Hier haben wir eine Erfolgsgeschichte hinter uns. Komplexe technische Systeme sind jedoch ein relativ neues Phänomen, mit dem wir erst umzugehen lernen müssen.[8] Zeitgleich sind wir aber ständig von komplexen Systemen umgeben, da die Natur nur aus offenen, dynamischen und damit komplexen Systemen besteht. Daher könnten wir auch von der Systemgestaltung in der Natur sehr viel lernen.

Komplexe Systeme

Komplexität ist ein häufig verwendeter Begriff, ohne das er eindeutig definiert wäre. Wir verbinden damit meist intuitiv undurchsichtige, komplizierte, vielschichtige oder unerklärlich Situationen oder Phänomene. Unsere Welt ist komplexer geworden, alles „dreht" sich schneller. Das „Hamsterrad" dient häufig als Metapher, immer schneller, aber ohne jemals an das Ziel gelangen zu können. Selten sind uns aber die dahinterliegenden Zusammenhänge bewusst.

Komplexe Systeme bestehen aus einer großen Anzahl von Elementen, die miteinander verbunden sind, die aber auch mit ihrer Umwelt interagieren und wo es laufend zu Rückkopplungen kommt. Es gibt auch technische Systeme (Maschinen) mit einer großen Anzahl von Elementen. Sie funktionieren aber nur in einer determinierten Umgebung und sie können in ihre Einzelteile zerlegt und wieder zusammengebaut werden. Das sind dann komplizierte Systeme, wie etwa mechanische Uhrwerke oder Druckmaschinen. Sie werden auch als tote Systeme bezeichnet. Komplexe Systeme hingegen können nicht einfach zerlegt und analy-

6 Vgl. Ossimitz, Günther/Lapp, Christian. Systeme: Denken und Handeln; Das Metanoia-Prinzip: Eine Einführung in systemisches Denken und Handeln. Berlin: Franzbecker, 2006

7 Vgl. Krizanits, Joana. Einführung in die Methoden der systemischen Organisationsberatung. Heidelberg: Carl-Auer Verlag, 2013

8 Vgl. Malik, Fredmund: Komplexität – was ist das?/ Modewort oder mehr? Kybernetisches Führungswissen Control of High Variety-Systems. In: Internet unter URL: http://www.kybernetik.ch/dwn/Komplexitaet.pdf [24.10.14].

siert und dann wieder zusammengebaut werden. Sie werden daher auch als lebendige Systeme bezeichnet. Daher führt die Vernetzung in einer nicht determinierbaren Umgebung zu komplexen Systemen, die ein völlig anderes Systemverhalten aufweisen, als unsere bisherigen einfachen bzw. komplizierten Systeme (Maschinen).

In komplexen Systemen kommt es zu laufenden Rückkopplungen, es entstehen Eigendynamiken. Einfache Ursache-Wirkungszusammenhänge gehen verloren, die Steuerbarkeit (Management) sinkt bzw. wird unmöglich. Es kommt zu langen Ursache-Wirkungsketten. Eingriffe wirken sich zeitverzögert aus und sind irreversible. Es entsteht die Gefahr einer Übersteuerung. Kleine Ursachen können zu großen Wirkungen führen und umgekehrt. Viel Aufwand mit wenig Ergebnis. Es kommt zu indirekten Wirkungen, die kaum abschätzbar sind und daher durch unsere etablierten Risikobewertungsmethoden nicht erfasst werden. Eine fehlende Reichweitenbegrenzung ermöglicht Domino- und Kaskadeneffekte, die umso verheerender ausfallen können, je größer das vernetzte System ist. Die Lösung eines Problems schafft neue Probleme (Aktionismus). Es kommt zu exponentiellen Entwicklungen und zur Erhöhung der Dynamik, mit denen wir nur sehr schlecht umgehen können, etwa mit dem Zinseszins.

Klingt vielleicht theoretisch. Bei näherer Betrachtung finden wir jedoch wieder unzählige Beispiele aus dem täglichen Leben. Ob das die Ohnmacht bei einer Vielzahl von anstehenden Problemen ist (Bildungs-, Gesundheits-, Pensionssystem), die zeitverzögerten negativen Auswirkungen des Internets mit den steigenden Herausforderungen aus dem Cyberspace (Cyber-Angriffe, Sicherheitsschwachstellen), ein Terroranschlag der zwei Kriege nach sich zieht (9/11), die immer wieder praktizierte Anlassgesetzgebung oder die unlösbaren Entwicklungen im Finanzsystem, immer spielt die unterschätzte Komplexität und Nicht-Steuerbarkeit eine Rolle. Ganz abgesehen davon, dass alle Kriege in ihrer Dynamik und Tragweite unterschätzt wurden.

Emergenz

Hinzu kommt, dass mit dem Grad der Vernetzung auch die Emergenz in einem System steigt. Unter Emergenz wird die spontane Herausbildung von neuen Eigenschaften oder Strukturen infolge des Zusammenspiels der Elemente in einem System verstanden. Die Eigenschaften der Elemente lassen dabei keine Rückschlüsse auf die emergenten Eigenschaften des Systems zu, was wiederum dazu führt, dass es zu einer spontanen Selbstorganisation und zu einer Nichtvorhersagbarkeit der Entwicklungen kommt.

Berücksichtigt man diesen Aspekt in aktuellen Entwicklungen, erscheinen diese wohl in einem neuen Licht. So wird etwa begreifbarer, wie faktisch aus dem Nichts eine Organisation wie der Islamische Staat (IS) unrühmliche Weltbekanntheit erlangen konnte. Durch die heutigen Möglichkeiten der technischen Vernetzung kann eine spontane und weitreichende Selbstorganisation erfolgen. In diesem negativen Fall führte das innerhalb sehr kurzer Zeit zu einer Schreckensherrschaft in einer sehr großen Region. Es ist jedoch nicht davon auszugehen, dass diese nachhaltig sein wird, da das Wachstum zu explosiv erfolgte. Dennoch wurden damit erhebliche Schäden und menschliches Leid verursacht. Verstärkt wurde das Ganze durch die heutigen Propagandamöglichkeiten, die wir durch das Internet bereit stellen. Daran ist aber weniger das Transportmedium schuld, als viel mehr, wie wir uns dadurch manipulieren lassen.

Die Nichtvorhersagbarkeit könnte aber auch dazu führen, dass nun die Gegenreaktionen auf den Islamischen Staat heftiger werden, was sich bereits abzeichnet, was wohl Seitens dieser Gruppierungen nicht intendiert ist. Aber auch hier sind die Folgewirkungen nicht abschätzbar. Die steigende Sorge vor möglichen Anschlägen in anderen Ländern ist daher mehr als begründet.[9] Ein wesentliches Problem dabei ist, dass viele Reaktionen auf Aktionismus und Symptombehandlung zurückzuführen sind.

Symptombehandlung

Eine wesentliche Änderung in der Bedrohungsbetrachtung wurde durch die Terroranschläge vom 11. September 2001 ausgelöst (9/11). Keine Sicherheitsdebatte kommt seither ohne dem Thema „internationaler Terrorismus" aus.

Ein besonders hoher Aufwand wurde in die Erhöhung der Flugsicherheit investiert, was de facto einer Vorbereitung auf den letzten Krieg gleichkommt, ohne pauschal alle getroffenen Maßnahmen infrage stellen zu wollen. Bei einer systemischen Betrachtung stößt man jedoch rasch auf viel Aktionismus. Ob das beim „Krieg gegen den Terror" generell oder beim Irak- bzw. Afghanistankrieg im speziellen, aber auch bei den inzwischen vielfach installierten technischen Sicherheitslösungen in der Flugsicherheit ist, der Erfolg ist bescheiden, bzw. wurden fast immer nur Symptome behandelt. Die meisten Maßnahmen haben zu keiner wesentlichen Verbesserung der Sicherheitslage insgesamt geführt, sondern zur weiteren Destabilisierungen bzw. zur Erhöhung der Scheinsicherheit, aber auch zu nicht intendierten Nebenwirkungen, wie etwa durch die Einschränkung der Privatsphäre oder indem durch die voranschreitende Überwachung unzählige unschuldige Menschen unter Generalverdacht geraten. Ganz abgesehen davon, dass diese Systeme ein hohes Missbrauchspotential aufweisen.

Terrorismus

Um Terrorismus verstehen und begegnen zu können, muss man zuerst wissen, wie er funktioniert. Kurz und knapp dargestellt wirkt Terrorismus zweimal. Einmal durch die unmittelbaren Auswirkungen bei einem Anschlag. Das zweite Mal durch die beim Opfer hervorgerufenen Reaktionen.[10] Aus verschiedenen Untersuchungen ist bekannt, dass die Sekundärschäden wesentlich höher sind, als die Schäden durch das unmittelbare Ereignis. So geht man heute davon aus, dass die Folgekosten von 9/11 in die Billionen gehen.[11] [12] Damit führt eigentlich nicht das unmittelbare Ereignis, sondern unsere Reaktionen darauf zu den wesentlich größeren Schäden. Und dies nicht nur auf finanzieller Basis. Eine große Anzahl von unschuldigen Menschen verloren in Folge des „Kampfes gegen den Terror" ihr Leben. Neben den unzähligen Soldaten eine viel größere Anzahl an Zivilisten – direkt, aber auch indirekt. Ist deshalb unsere Welt sicherer geworden?

9 Vgl. Sadowski, David/Becker, Jeff: Beyond the „Hybrid" Threat: Asserting the Essential Unity of Warfare. In: Small Wars Journal, 2010, unter URL: http://smallwarsjournal.com/blog/journal/docs-temp/344-sadowski-etal.pdf [24.10.14].

10 Vgl. Vester, Frederic. Die Kunst vernetzt zu denken/Ideen und Werkzeuge für einen neuen Umgang mit Komplexität: Ideen und Werkzeuge für einen neuen Umgang mit Komplexität. Ein Bericht an den Club of Rome. München: Deutscher Taschenbuch Verlag, 2011[8]

11 Vgl. Anti-Terror-Kampf kostet USA eine Billion Dollar unter URL: http://www.welt.de/politik/ausland/article13371713/Anti-Terror-Kampf-kostet-USA-eine-Billion-Dollar.html [23.10.14].

12 Hoffman, Frank G.: 'Hybrid Threats': Neither Omnipotent nor Unbeatable, Orbis (2010). doi:10.1016/j.orbis.2010.04.009.

In den vergangenen Jahren gab es auch ein positives Beispiel, wo nicht gleich überreagiert wurde. Und zwar nach den Anschlägen auf das öffentliche Verkehrssystem in London im Jahr 2005, da man mit dieser Möglichkeit gerechnet und sich darauf vorbereitet hat.[13]

Ein zunehmendes Problem stellen die geänderten Ziele von Terrorgruppen dar. Im 20. Jahrhundert wurden mit Terrorismus noch vorwiegend politische Ziele zu erreichen versucht, wozu man auch Rücksicht auf die gegnerische Bevölkerung nehmen musste. Das hat sich mit 9/11 geändert. Fundamentalistische, vorwiegend islamische Gruppierungen, verfolgen nicht mehr dieses irdische Ziel, womit auch gewisse Hemmschwellen wegfallen. Wir sind daher angehalten, in Zukunft mit höheren Schäden durch Terrorismus zu rechnen. Gleichzeitig ein wichtiger Indikator, uns nicht zu sehr auf mögliche Akteure zu konzentrieren, sondern vielmehr auf unsere Verwundbarkeiten.

Ursachen für Terrorismus

Die derzeitige „Terrorismusbekämpfung" ist weitgehend nur eine Symptombekämpfung. Selten wird versucht, den möglichen Ursachen auf den Grund zu gehen und dort anzusetzen. Der deutsche Risikoforscher Ortwin Renn sieht gerade in der zunehmenden Unzufriedenheit mit ungerechten Vermögens- und Machtverhältnissen eine Ursache, die zu sozialer Unzufriedenheit bis hin zu aggressiven Handlungen, wie sozialem Aufruhr, Fanatismus und Terrorismus führen.[14] Um wirklich einen Beitrag für eine sichere Zukunft zu leisten, müsste hier angesetzt werden. Leider stehen dazu nicht einfache technische Lösungen mit großen Versprechungen zur Verfügung.

Cyber-Bedrohungen

Ähnlich wie beim Terrorismus erfolgt die Auseinandersetzung auch mit den Cyber-Bedrohungen. Während sie lange vernachlässigt wurden, ist auch hier nun sehr viel Aktionismus und Scheinsicherheit zu beobachten, was sich etwa bei Aussagen wie „*Als Kernelemente werden der Verlust der Vertraulichkeit von Informationen, die digitale Spionage und das Einschleusen von Computerviren genannt. Die Cyberkriminalität hat ebenfalls einen steigenden Stellenwert, jedoch mit dem Hintergrund eines Betruges von professionellen Kriminellen und ist weniger als Machtprojektion zu bewerten.*" widerspiegelt.[15] Auch hier orientieren wir uns an der Vergangenheit und am bisher Erlebten.

Die wirkliche Bedrohung für unsere Sicherheit und Gesellschaft ist nicht der Datenverlust, sondern die Gefahr, dass unsere zunehmend mit dem Internet verbundene Kritische Infrastruktur – durch welches Ereignis auch immer – physisch ausfallen könnte, was wiederum zahlreiche Dominoeffekte nach sich ziehen würde. Unsere derzeitige Systemgestaltung und Abhängigkeit lässt ein Versagen nicht zu. Wir haben viele überlebenswichtige Infrastrukturen als „too big to fail" gestaltet, ohne dass wir uns dessen Bewusst wären, noch dass wir dafür einen Plan B hätten, sollte es zu größeren Störungen kommen. Dabei geht die Gefahr nicht nur von Angreifern aus, sondern ist systemimmanent. Am 01.01.2010 versagten etwa in Deutschland rund 30 Millionen EC- und Kreditkarten, da die Mikrochips fehlerhaft programmiert worden waren. Die betroffenen Kunden konnten weder an Geldautomaten Bargeld ab-

13 Saurugg, Herbert: Blackout/Eine nationale Herausforderung bereits vor der Krise. Wien: Seminararbeit, 2012 unter URL: http://www.saurugg.net/wp/wp-content/uploads/2014/10/Blackout-Eine-nationale-Herausforderung-bereits-vor-der-Krise.pdf [23.10.14].

14 Renn, Ortwin: Das Risikoparadox/Warum wir uns vor dem Falschen fürchten. Frankfurt am Main: Fischer Verlag, 2014.

15 Querverweis GULDER Alfred.

heben noch damit bargeldlos bezahlen.[16] Ein solcher Fehler in wichtigen Komponenten in einer hoch vernetzen Infrastruktur hätte wahrscheinlich verheerende Folgen. Wie etwa auch auf der Hackerkonferenz Black Hat 2014 wieder einmal aufgezeigt wurde. Forschern ist es gelungen, einen in Spanien bereits millionenfach ausgerollten intelligenten Stromzähler („Smart Meter") zu kompromittieren und eine Fernabschaltung über das Netzwerk zu initiieren.[17] Ein neues Geschäftsmodell für die Organisierte Kriminalität – wir sind massiv Erpressbar geworden.

Ein anderes Beispiel für unsere „blinden Flecken" zeigt der Bericht „Power Supply Dependencies in the Electronic Communications Sector"[18] von der European Union Agency for Network and Information Security (ENISA) auf. Als Nebenprodukt der Erfassung von Cyber-Vorfällen in der EU stellte sich heraus, dass „power cuts are a dominant cause of severe network and service outages in the EU's electronic communications sector". Die höchsten Schäden werden demnach durch Überlastung, Stromausfälle und durch Softwarefehler verursacht. Wobei natürlich zu berücksichtigen gilt, dass in einem komplexen System eine kleine Ursache verheerende Auswirkungen nach sich ziehen kann. Aber wenn schon nicht einmal einfache Hausaufgaben gemacht wurden, bedeutet das wohl auch, dass die Verwundbarkeit dieser Systeme weit höher ist, als gemeinhin angenommen wird. Auch wenn überraschender Weise noch keine größeren Zwischenfälle passiert sind. Wir befinden uns hier wahrscheinlich in einer gefährlichen „Truthahn-Illusion"[19].

Aktuelle Cyber-Sicherheitskonzepte berücksichtigen diese Faktoren kaum. Ganz abgesehen davon, dass Cyber-Defence in einem vernetzten System keine zweite Verteidigungslinie darstellt, wie das gerne gesehen wird.

„Blinde Flecken"

Unser genereller Fokus auf die Bekämpfung von möglichen Akteuren führt dazu, dass wir viele Dinge übersehen, die eigentlich weit gravierender sind. Terrorismus kann nur wirken, wenn wir es zulassen. Einerseits durch unsere Reaktionen und andererseits, indem wir ihm entsprechende Verwundbarkeiten anbieten. Während in den letzten Jahren für die Erhöhung der Flugsicherheit viele Milliarden Euro aufgewendet wurden, haben wir gleichzeitig zugelassen, dass unsere Infrastrukturen immer verwundbarer geworden sind.

Durch die technische Vernetzung haben wir meist unbewusst hochkomplexe und wechselseitig abhängige Systeme mit möglicherweise verheerenden systemischen Risiken geschaffen. Dementsprechend sind wir auch in keinster Weise auf daraus resultierende strategische Schockereignisse („Schwarzer Schwan")[20] vorbereitet. Egal, ob das die europäische Stromver-

16 Vgl. Wikipedia EMV (Kartenzahlungsverkehr) unter URL: http://de.wikipedia.org/wiki/EMV_(Kartenzahlungsverkehr)#2010-Bug

17 Vgl. Intelligenter Stromzähler: Gehackte Smart Meter machen Lichter aus unter URL: http://www.golem.de/news/intelligente-stromzaehler-gehackte-smart-meter-machen-lichter-aus-1410-109923.html [24.10.14].

18 Unter URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies.

19 Ein Truthahn, der Tag für Tag von seinem Besitzer gefüttert wird, nimmt aufgrund seiner täglich positiven Erfahrung an, dass die Wahrscheinlichkeit, dass etwas Gravierendes passiert, von Tag zu Tag kleiner wird. Gleichzeitig steigt sein Vertrauen mit jeder positiven Erfahrung (Fütterung). Am Tag vor Thanksgiving (bei dem traditionell die Truthähne geschlachtet werden) erlebt der Truthahn allerdings eine fatale Überraschung.

20 Ein Ereignis mit den drei Attributen Seltenheit, massive Auswirkungen und Vorhersagbarkeit im Rückblick (allerdings nicht in der Vorausschau). Siehe Taleb, Nassim Nicholas. Der Schwarze Schwan: Die Macht

sorgungsinfrastruktur, die Telekommunikations- und Internetinfrastrukturen oder die Lebensmittelversorgung betrifft, wir bewegen uns in vielen Bereichen auf sehr dünnem Eis. Ein größeres Ereignis in einem Sektor würde weitreichende Dominoeffekte, auch über Systemgrenzen hinaus, auslösen. Eine europäische Großstörung im Stromversorgungssystem („Blackout") hätte verheerende Folgen, nicht nur für die Elektrizitätswirtschaft, sondern für die gesamte Gesellschaft, sind wir doch völlig von der einwandfrei funktionierenden Stromversorgung abhängig.[21] Ein solches Ereignis würde gleichzeitig unser Finanz- und Wirtschaftssystem auf eine gewaltige Belastungsprobe stellen, wenn nicht sogar weitere weitreichende Dominoeffekte auslösen. Dabei ist irrelevant, wodurch und durch wen ein solches Ereignis ausgelöst wird. Ob durch technische Pannen, Naturereignisse oder durch Terrorismus. Daher sollte unser Fokus und unsere Energie weniger auf mögliche Akteure gelegt werden als vielmehr auf die Angriffsflächen, die wir meist unbewusst geschaffen haben. Dabei geht es nicht nur um die Verwundbarkeit unserer Infrastrukturen, sondern auch um die Fähigkeit, als Gesellschaft mit solchen Störungen sinnvoll umzugehen.

Systemische Risiken

Die chaotische und nicht-systemische technische Vernetzung der vergangenen Jahre hat dazu geführt, dass in unserer Gesellschaft und in den Kritischen Infrastrukturen die Anzahl der systemischen Risiken massiv angestiegen ist.[22] Diese sind gekennzeichnet durch:

- einen hohen Vernetzungsgrad (Dynamik, Komplexität, Wechselwirkungen)
- der Gefahr von Dominoeffekten
- einer Nicht-Linearität in den Auswirkungen (keine einfachen Ursache-Wirkungsketten, die durch das standardisierte Risikomanagement erfasst werden) und
- durch eine systematische Unterschätzung durch Verantwortungsträger.

Das hat dazu geführt, dass die Wahrscheinlichkeit von strategischen Schockereignissen, also Ereignissen, die in der Lage sind, unser Zusammenleben nachhaltig – langfristig und erheblich – zu verändern („Game-Changer"), massiv angestiegen ist. Dabei wird hier noch gar nicht direkt auf die richtig großen Themen unserer Zeit eingegangen:[23]

- Bedrohungen durch menschliche Interventionen in das Ökosystem Erde (z.B. Klimawandel, Ressourcenknappheit, Süßwasserkrise, Gefährdung der Artenvielfalt)
- Bedrohungen durch Steuerungsdefizite in der Wirtschaft und Gesellschaft (Umgang mit öffentlichen Gütern, Finanzkrisen, Pandemien).
- Bedrohungen durch soziale Fehlentwicklungen (ungleiche Lebensbedingungen).

Hinzu kommt, dass heute sich ohnmächtig fühlende Menschen oder Gruppierungen mithilfe moderner Technologien große Wirkungen bis hin zu Katastrophen auslösen können (kleine

höchst unwahrscheinlicher Ereignisse. München: dtv, 2013[5]

21 Vgl. European Union Agency for Network and Information Security (ENISA; Hrsg.): Power Supply Dependencies in the Electronic Communications Sector/Survey, analysis and recommendations for resilience against power supply failures. Heraklion: ENISA, 2013 unter URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies [22.10.14].

22 Vgl. Zurich Insurance Company Ltd and Atlantic Council of the United State (Hrsg.): Beyond data breaches: global interconnections of cyber risk. In: Internet unter URL: http://www.atlanticcouncil.org/publications/reports/beyond-data-breaches-global-interconnections-of-cyber-risk [23.10.14].

23 Vgl. Renn, Ortwin: Das Risikoparadox/Warum wir uns vor dem Falschen fürchten. Frankfurt am Main: Fischer Verlag, 2014.

Ursache, große Wirkung). Die Terroranschläge von 9/11 wurden in letzter Konsequenz mit einem einfachen Teppichmesser ausgelöst:

> *„Mit dieser Waffe können zwar Menschen ermordet werden, aber zu einem systemischen Risiko wird sie erst dann, wenn sie mit der Verwundbarkeit moderner vernetzter Technologien verbunden wird. Denn mit Hilfe eines Teppichmessers gelangten die Terroristen in den Besitz von wesentlich wirksameren Waffen wie Flugzeuge, die sie wiederum nutzten, um die Verwundbarkeit komplexer Hochhausstrukturen auszunutzen. Die Kaskade von einfachen Mitteln hin zu globalen Auswirkungen wird durch die beschriebenen Zusammenhänge der technischen Entwicklung, der Virtualisierung und der Zunahme der Verwundbarkeit ermöglicht.*
>
> *Dazu kommt der Potenzierungseffekt* [Dominoeffekte] *durch Globalisierung und Vernetzung, durch den auch Machtmissbrauch, kriminelle Handlungen und Terrorismus eine wesentlich höhere Wirkmächtigkeit besitzen als früher."*[24]

Risikowahrnehmung

Ein wesentlicher Grund für die vielen „blinden Flecken" ist darauf zurückzuführen, dass unsere Risikowahrnehmung vorwiegend auf vergangene Erfahrungen und auf stark gefilterte Informationen aus den Medien passiert. Ersteres ist evolutionär bedingt und hat bisher ausgereicht. Aber auch institutionell aufbereitete Informationen unterliegen meist einer vorgefertigten Deutungshoheit bzw. geben meist nur einem Teilausschnitt der Wirklichkeit wieder.[25] Zudem wird die Öffentlichkeit einem Wechselbad von Dramatisierungen (Medien) und Verharmlosungen (Politik) ausgesetzt. Die Vielzahl an Themen und der ständige Zeitdruck lassen tiefer gehende Betrachtungen meist nicht zu. Zusätzlich wird häufig eine starke Vereinfachung eingefordert („Managementbriefing"). Ganz abgesehen davon, dass unsere Steuerungsmechanismen (Management) nach wie vor auf das industriegesellschaftliche Denken und Handeln bei einfachen und komplizierten Systemen (Maschinen) ausgerichtet sind.

Es gibt eine Vielzahl an falsch und zum Teil irrational wahrgenommen Risiken. Während wir bei einzelnen vermeintlichen Risiken schon fast hysterisch reagieren, wie etwa aktuell bei Ebola[26], nehmen wir andere weit bedrohlichere Risiken so gut wie überhaupt nicht war. Wobei gerade Ebola ein Beispiel für Ambivalenz ist. Während die Gefahr in den betroffenen Gebieten zu lange unterschätzt wurde, wird sie bei uns völlig überschätzt. In Österreich sterben jährlich rund 8.000 Menschen direkt oder indirekt an den Folgen von Alkoholkonsum, oder anders ausgedrückt, etwa 16x so viel wie im Straßenverkehr.[27] In der EU sterben derzeit geschätzte 25.000 Menschen jährlich an Infektionen mit multiresistenten Keimen. Die damit verbundenen Sekundärkosten werden mit jährlich rund 1,5 Milliarden Euro beziffert.[28]

24 Ebenda.

25 Vgl. Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0. Masterarbeit: 2013 unter URL: http://www.saurugg.net/wp/wp-content/uploads/2014/10/die_netzwerkgesellschaft_und_krisenmanagement_2.0.pdf [22.10.14].

26 Vgl. Allgemeine Erkenntnisse aus dem Workshop "Mein Unternehmen auf ein Blackout vorbereiten" unter URL: http://www.ploetzlichblackout.at/2014/10/15/allgemeine-erkenntnisse-aus-dem-workshop-mein-unternehmen-auf-ein-blackout-vorbereiten/ [24.10.14].

27 Alkohol: Fakten und Mythen unter URL: http://www.uni-salzburg.at/index.php?id=50709 [24.10.14].

28 Clostridium-difficile-Infektion, antibiotikaassoziierte Diarrhö/Colitis – Nosokomiale Last unter URL: http://www.medmedia.at/univ-innere-medizin/infektiologie-nosokomiale-last/ [24.10.14].

Im Zusammenhang mit Terrorismus wird auch gerne der globale Finanzmarkt mit der Möglichkeit der einfachen Finanzierung und Kapitalverschiebungen diskutiert.[29] Aufgrund der Finanzkrise 2007/2008 könnte man aber auch zum Schluss kommen, dass ein viel höheres Risiko von den Finanzmärkten selbst ausgeht und die Anzahl der Opfer – indirekt auch Todesopfer – durch den überbordenden Finanzkapitalismus weit höher sind. Doch das sieht man nicht so offensichtlich, bzw. widerspricht unsere derzeitigen Denkmodellen. Wir haben hier kognitive Grenzen.

Ein anderes Beispiel stellt der Risikobericht 2012 der Schweiz dar.[30] Darin geht hervor, dass eine Pandemie und ein Ausfall der Stromversorgung als größtes Risiko für die Schweiz in Bezug auf Schadensausmaß und Eintrittswahrscheinlichkeit darstellt. Gleichzeitig sprechen wir von einem europäischen Verbundsystem, wo alle Länder im gleichen Umfang betroffen wären. Wie auch bei einer Pandemie. Doch kaum ein anderes Land in Europa setzt sich derart intensiv damit auseinander. Ganz abgesehen davon, dass eine Bewältigung nur auf Behördenebene (Krisenmanagement) nicht möglich ist und es einer umfassenden gesellschaftlichen Auseinandersetzung erfordern würde, um mit derartigen strategischen Schockereignissen sinnvoll umgehen zu können.

Hybride Bedrohungspotenziale

Aber was hat das nun alles mit hybriden Bedrohungen zu tun? Sehr viel, obwohl es auf den ersten Blick viele Widersprüchlichkeiten zu geben scheint. Mit der Definition hybrider Bedrohungen wurde versucht, den realen Entwicklungen Rechnung zu tragen.[31] Dabei erfolgte jedoch ein Klassifizierungsversuch in der bisher erfolgreichen Denklogik, etwa indem von „Akteuren“, „Interessendurchsetzung“ oder von einer „strategischen Schwelle“ ausgegangen wird. Diese „Silos“ stehen jedoch im Widerspruch zur Netzwerkgesellschaft und zu den realen Entwicklungen. Dies wird etwa auch bei der „Akteursübersicht Hybride Bedrohung“[32] ersichtlich. Hier wurden bisher klar identifizierbare und übliche „Silos“ gegenübergestellt, das Ganze ist auch übersichtlich darstellbar, entspricht jedoch kaum den Realitäten. Denn zwischen den unterschiedlichen Domänen gibt es vielschichtige Vernetzungen und Querverbindungen („unsichtbare Fäden“) mit zeitlich verzögerten Wirkungen oder Abhängigkeiten. Daher entsprechen die daraus ableitbaren Konsequenzen der bisherigen Logik, die aber für VUCA Entwicklungen nur bedingt bis gar nicht tauglich sind.

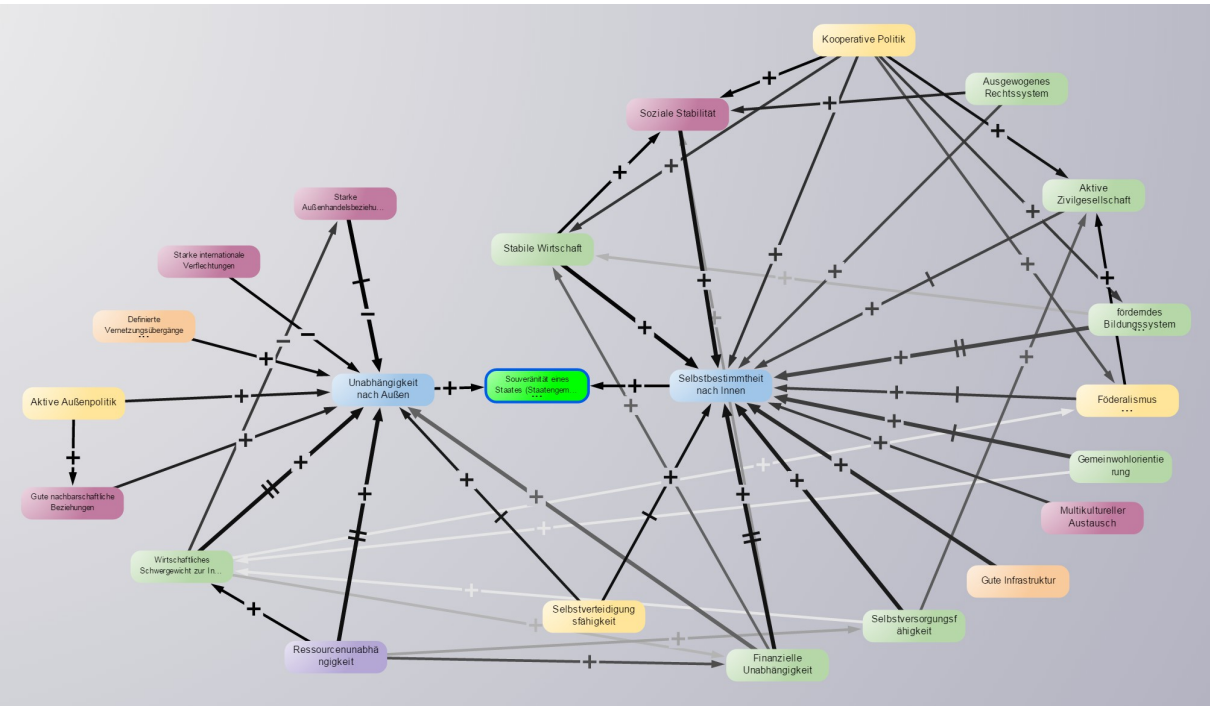
Wenn man jedoch versucht, die Ausgangsfrage „Welche Faktoren sind für die Souveränität eines Staates (Staatengemeinschaft) erforderlich“ in einem Modell darzustellen, wird es sehr rasch unübersichtlich (Abbildung [x]).

29 Querverweise Rastislav Báchor - Zudem erleichtern „globale Finanzmärkte“ Kapitalverschiebungen von Terroristen.

30 Bundesamt für Bevölkerungsschutz (BABS): Katastrophen und Notlagen Schweiz: Risikobericht 2012. In: Internet unter URL: http://www.alexandria.admin.ch/bv001490434.pdf.

31 Querverweis Definition.

32 Verweis oder Bild einfügen.

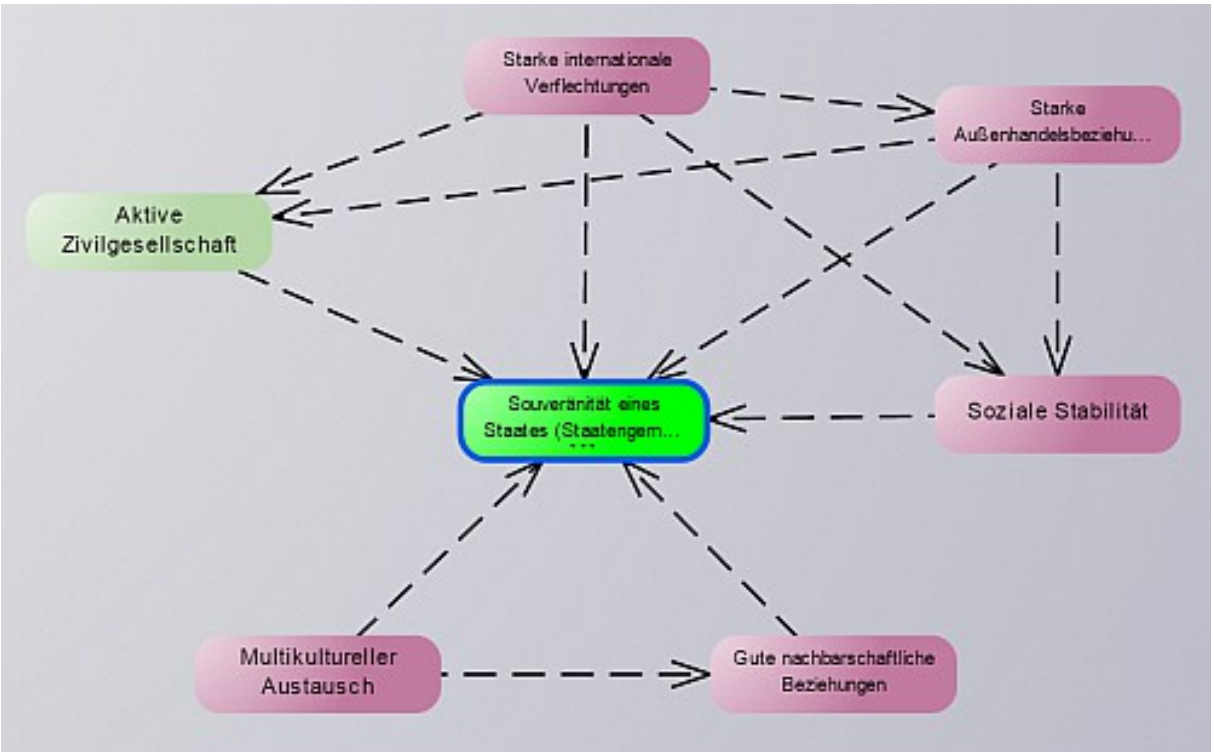


Daran ist jedoch nicht das Modell schuld, sondern unser Wunsch, komplexe Sachverhalte möglichst einfach darzustellen, was zu starken Vereinfachungen führt und sich schön darstellen lässt, aber mit den tatsächlichen Realitäten nur wenig zu tun hat. Eine Vielzahl an gescheiterten Großprojekten sind stumme Zeugen davon.

Aus der Forschung ist bekannt, dass unser Hirn die möglichen Wechselwirkungen zwischen max. 3-4 Faktoren erfassen kann. Alles was darüber hinaus geht, erfordert Hilfsmittel und Visualisierungen. Eine Möglichkeit ist, wie im Modell „Souveränität eines Staates (Staatengemeinschaft)“ (Abbildung [x]) begonnen wurde, die möglichen Wechselwirkungen und Zusammenhänge zu erfassen und darzustellen. Durch weiterführende Analysen können dann zeitverzögerte bzw. sonst nicht erfassbare Wechselwirkungen aufgespürt werden.

Zum anderen bietet Modellieren die Möglichkeit, einzelne Aspekte isoliert zu betrachten und hervorzuheben, ohne jedoch dabei mögliche Wechselwirkungen außer Acht zu lassen (Abbildung [y]). Ein Modell erlaubt es auch, mögliche widersprüchliche Ansichten zu erfassen, die es so gut wie immer geben wird.[33]

33 Vgl. VUCA - volatil, unsicher, komplex und ambivalent.



Aber auch ein Modell ist keine Abbildung der Wirklichkeit, sondern nur ein Versuch, dieser näher zu kommen. Hier bietet sich der Vergleich zwischen Gelände und Karte an. Nicht die Detaildichte führt zu einem besseren Ergebnis, sondern indem die wesentlichen Merkmale des Geländes abgebildet sind. Diese sind natürlich je nach Bedarf unterschiedlich, ob man etwa zu Fuß oder mit dem Flugzeug unterwegs ist. Und so ist es auch mit Modellen, die einen Wirklichkeitsausschnitt wiedergeben sollen. Sie dienen als Kommunikationsinstrument, um eine gemeinsame Sicht zu schaffen. Um die tatsächlichen Abhängigkeiten und Realitäten bei der Souveränität eines Staates (Staatengemeinschaft) erfassen zu können, müssten daher auch Akteure aus den unterschiedlichen „Silos" mitwirken, um zu einem bestmöglichen Abbild der Realität zum Zeitpunkt der Erstellung zu kommen. Und das wir aufgrund der heutigen Dynamiken und Geschwindigkeiten zunehmend schwieriger. Genau genommen bedürfte es eines fortlaufenden Prozesses. Daher wäre, wie bei den Länderanalysen festgestellt wurde, durchaus zu hinterfragen, ob formalisierte (Schweden)[34] bzw. veraltete Strategien (Slowakei)[35] wirklich einen Mehrwert liefern.

Aber wie kann man dann mit hybriden Bedrohungen umgehen?
Indem man die Ausgangsdefinition[36] kritisch hinterfragt und prüft, ob aufgrund der bisherigen Ausführungen diese wirklich zweckmäßig ist, oder ob es nicht vielmehr notwendig ist, eine neue Fragestellung zu definieren. Wenn wir davon ausgehen, dass die Zukunft volatiler, unsicherer, komplexer und ambivalenter (VUCA) wird, dann brauchen wir wohl auch neue Denkmodelle.

Die einzelnen Länderstrategien weisen durchaus erfolgversprechende Ansätze auf. Etwa in Schweden, indem man nicht auf formalisierte Strategien und auf niedergeschriebene Kon-

34 Querverweis Schweden
35 Querverweis Slowakei
36 Querverweise Definition

zepte Wert legt, sondern vielmehr auf eine flexible und der Realität angepassten Kooperationskultur, auch wenn aus der Analyse hervorgeht, dass bei der praktischen Umsetzung noch Verbesserungsbedarf besteht.[37] Bei vielen Strategien stellt sich bei einer näheren Betrachtung heraus, dass es zwischen den formalisierten „Wunschvorstellungen" und der tatsächlichen Umsetzung erhebliche Differenzen gibt. Gerade in Österreich gibt es einige Beispiele dafür.

Auch die Aussage von Michael Miklaucic, Director of Research and Editor of PRISM at the Center for Complex Operations at National Defense University, *„A hybrid threat is more than just the sum total of its constituent parts. Combating such threats does not require new capabilities as much as new partners, new processes and, above all, new thinking"* ist völlig treffend.[38]

Ein anderer Aspekt der in der schwedischen Analyse hervorsticht, ist das Amt für Bevölkerungsschutz und Bereitschaft.[39] Während man etwa auch in Deutschland über ein Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) oder in der Schweiz über ein Bundesamt für Bevölkerungsschutz (BABS) verfügt, gibt es in Österreich keine derartige Einrichtung. Der Katastrophenschutz ist in Österreich Ländersache und dementsprechend heterogen ist dieser auch abgebildet. Nationale oder sogar internationale Krisenlagen oder strategische Schockereignisse sind damit nur unzureichend abgebildet. Die Erfassung von systemischen Risiken ist dadurch ebenfalls nur unzureichend gegeben. Bei einer derartigen Organisationsstruktur ist aber darauf zu achten, dass nicht wieder ein neuer Silo geschaffen wird, sondern ein Vernetzungsinstrument. Denn viele erforderliche Systemelemente sind bereits heute in irgend einer Art und Weise abgebildet. Was fehlt ist die bedarfs- und zielorientierte Vernetzung unter Hintanhaltung des bisherigen „Silodenkens und -verhaltens".[40]

Indirekt wird das auch in der slowakischen Analyse von Rastislav Báchora angesprochen, wo ein Schulterschluss zwischen institutionellen, nichtstaatlichen als auch zivilgesellschaftlichen und kommerziellen Akteuren eingefordert wird.[41] Grundsätzlich wurde dieser Gedanke in Österreich bereits in der Umfassenden Landesverteidigung (ULV) und heute in der Umfassenden Sicherheitsvorsorge (USV) formalisiert. Die Realität blieb aber immer deutlich hinter den vorgefassten Zielvorstellungen.

Durch standardisierte und vereinfachte Prozesse wurden in den vergangenen Jahren große Fortschritte bei Standardeinsätzen gemacht, die auch zu einer sehr hohen Versorgungsquali-

37 Querverweis auf Michael Fredholm: „Es gibt nicht einmal einige Weiß- oder Grünbücher, die mit der nationalen Sicherheit befasst sind. Bedrohungen werden typischerweise nicht mit veröffentlichten Konzepten aber mit ganz pragmatischen Mitteln behandelt, abhängig von der jeweiligen Situation."
„Schwedens sicherheitspolitische Ausrichtung ist von einer ausgesprochen starken Kooperationskultur geprägt."

38 NATO Countering the Hybrid Threat unter URL: http://www.act.nato.int/nato-countering-the-hybrid-threat [23.10.14].

39 Querverweis auf Michael Fredholm: Ein wichtiger Akteur ist das Amt für Bevölkerungsschutz und Bereitschaft (MSB; Swedish Civil Contingencies Agency). Die Aufgabe des MSB besteht darin, die gesellschaftlichen Kapazitäten zu verbessern und die Vorbereitung auf und die Prävention von Notfällen und Krisen zu unterstützen.

40 Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0. Masterarbeit: 2013 unter URL: http://www.saurugg.net/wp/wp-content/uploads/2014/10/die_netzwerkgesellschaft_und_krisenmanagement_2.0.pdf [22.10.14].

41 Die institutionelle Zusammenarbeit bei der Bekämpfung von Bedrohungen schließt sowohl nichtstaatliche als auch zivilgesellschaftliche aber auch kommerzielle Gruppen ein.

tät geführt haben. Eine organisationsübergreifende Zusammenarbeit von Einsatzorganisationen ist zwar mittlerweile State-of-the-Art, aber häufig nur bei konkreten Anlassfällen. Eine gemeinsame Ausbildung bzw. zumindest übergreifende Ausbildungsmodule stecken noch in den Kinderschuhen bzw. sind auf Einzelbereiche beschränkt. Die Interoperabilität zwischen den zivilen und militärischen Einsatzorganisationen wurde zwar verbessert (etwa bei der Führungsorganisation), jedoch gibt es noch ein großes Verbesserungspotential, um auch mit den Auswirkungen von möglichen strategischen Schockereignissen fertig zu werden. Ganz zu schweigen von der Herausforderung bei der Zusammenarbeit mit „ungebundenen Helfern“[42], wie etwa mit den Mitgliedern des Team Österreichs bei Katastrophenlagen.

Ein anderes Beispiel ist die zivilgesellschaftliche Initiative „Plötzlich Blackout!“ - Vorbereitung auf einen europaweiten Stromausfall.[43] Während es bisher in Österreich von institutioneller Seite kein nationales Szenario für einen möglichen plötzlichen, überregionalen und länger andauernden Stromausfall („Blackout“) gibt, thematisiert die Initiative dieses Szenario seit Herbst 2013 und hat bei verschiedenen Veranstaltungen mehrere hundert Organisationen aus allen gesellschaftswichtigen Bereichen (Behörden, Einsatzorganisationen, Unternehmen, Forschung und Zivilgesellschaft) eingebunden und sogar eine internationale Vernetzung geschaffen. Gerade bei neuen Themen ist die Zivilgesellschaft häufig flexibler und schneller. Dieses Potential sollte bei sicherheitspolitischen Themen stärker berücksichtigt werden.

Möglicherweise wird auch der zunehmende finanzielle Druck dazu führen, dass wir in Zukunft mehr auf Synergiemöglichkeiten achten werden. Gerade die österreichische Kultur ist durch den „kleinen Dienstweg“ geprägt. Dort wo formalisierte Strukturen unzureichend sind, bilden sich informelle Wege („unsichtbare Fäden“), die zum Gelingen beitragen. Das Gegenbeispiel ist die Androhung „Dienst nach Vorschrift“ zu versehen. Wir handeln häufig intuitiv nach den Grundsätzen der Netzwerkgesellschaft, uns flexibel und ad-hoc zu vernetzen, um einen Mehrwert zu schaffen. Um diese Eigenschaft werden wir anderorts häufig beneidet. Wir sollten sie daher bewusst als Stärke wahrnehmen, fördern und im Sinne des Ganzen nutzen.

Verwundbarkeiten

Wie sich aus den vorangegangenen Ausführungen ableiten lässt, sollten wir stärker auf Verwundbarkeiten, als auf mögliche Akteure achten. Auch für die möglichen Akteure im Sinne der Definition von hybriden Bedrohungen ist es zunehmend schwieriger bis unmöglich, die eigenen Interessen gegenüber Dritte durchzusetzen. Auch für sie gelten die Gesetzmäßigkeiten von komplexen Systemen. Wobei das nicht ausschließt, dass eine temporäre Beeinflussung möglich ist. Hierzu ist es notwendig, nicht nur in den heute in der Betriebswirtschaftslehre üblichen sehr kurzen Zeithorizonten zu denken, sondern längerfristig. Denn viele *Quick and Dirty*-Lösungen konzentrieren sich nur auf die Symptome und lassen sich sofort umsetzen, während fundamentale Lösungen die Ursache des Problems zu beseitigen versucht. *Quick and Dirty*-Lösungen sind meist schnell angewandt, verschlimmern aber langfristig das eigentliche Problem, während fundamentale Lösungen kurzfristig oft deutliche Nachteile bringen und sich erst langfristig als vorteilhaft herausstellen.[44]

42 Vgl. „Ungebundene Helfer im Katastrophenschutz: Die Sicht der Behörden und Organisationen mit Sicherheitsaufgaben“ unter URL: http://www.kat-leuchtturm.de/assets/content/images/pdfs/593_597_Kircher.pdf [22.10.14].

43 Siehe unter URL: www.ploetzlichblackout.at [22.11.14].

44 Vgl. Ossimitz, Günther/Lapp, Christian. Systeme: Denken und Handeln; Das Metanoia-Prinzip: Eine Einführung in systemisches Denken und Handeln. Berlin: Franzbecker, 2006.

Ein aktuelles Beispiel dafür ist der Konflikt zwischen der EU/Ukraine und Russland. Keine der beiden Seiten kann wirklich abschätzen, welche Folgewirkungen mit den bisherigen Drohgebärden und Sanktionen noch verbunden sein werden. Gleichzeitig sind die Mechanismen dem alten Denken zuzuordnen. Nicht einmal haben Banalitäten in die Katastrophe geführt. Auch hier haben wir zahlreiche „blinde Flecken".

Seit Monaten gibt es Hinweise auf gezielte Cyber-Angriffe auf westliche Energieversorgungsunternehmen, die vermeintlich aus Russland kommen sollen, was bei Cyber-Angriffen nie eindeutig feststellbar ist.[45] Dennoch sollten die Alarmglocken läuten. 2007 hat die Versetzung eines russischen Denkmals zu einem massiven Cyber-Angriff auf Estland geführt. Damals waren „nur" virtuelle Systeme betroffen. Heute könnte dabei unsere Kritischste Infrastruktur angegriffen und möglicherweise zum Ausfall gebracht werden. Dabei sollte davon Abstand genommen werden, eine solche Möglichkeit nur einem Akteur zuzuordnen. Gerade Cyber-Angriffe können äußerst rasch außer Kontrolle geraten und eine unvorhergesehene Eigendynamik entwickeln, wie das eben in komplexen Systemen möglich ist.

In der Schweiz wurde dieses Szenario als Ausgangsszenario für die Sicherheitsverbundsübung 2014 herangezogen,[46] in folge dessen es zu Instabilitäten im Stromversorgungssystem mit einem dadurch ausgelösten Blackout kommt. Als noch schlimmer wird dabei die darauf folgende mehrwöchige Strommangellage beurteilt, da wir weder als Gesellschaft noch unsere Infrastrukturen auf ein solches strategisches Schockereignis vorbereitet sind.[47]

Die belgische Regierung hat im Sommer 2014 einen nationalen Notfallplan erlassen, indem für den kommenden Winter nationale Notabschaltungen in der Stromversorgung vorbereitet wurden. Auslöser sind zwei Atomkraftwerke, die aus massiven Sicherheitsbedenken vom Netz genommen werden mussten und die Sorge, dass die Stromversorgung über den Winter nicht aufrecht erhalten werden kann. Gleichzeitig bleiben in Europa 22 baugleiche Reaktoren mit denselben kritischen Sicherheitsmängeln im Betrieb.[48]

Die OECD hält in ihrer Studie „Future Global Shocks - Geomagnetic Storms" fest:

> *„The lack of valid risk assessments has limited risk mitigation efforts in many critical infrastructure sectors, as it is difficult to demonstrate the utility of investing in either hardening or operational mitigation efforts, especially if these investments reduce time and money spent in preparing for more common risks.*
>
> *Geomagnetic storms can be categorized as a global shock for several reasons: the effects of an extreme storm will be felt on multiple continents; the resulting damage to electric power transmission will require international cooperation to address; and the economic costs of a lengthy power outage will affect economies around the world."*[49]

45 Russian Hackers Threaten Power Companies, Researchers Say unter URL: http://www.bloomberg.com/news/2014-06-30/symantec-warns-energetic-bear-hackers-threaten-energy-firms.html [24.10.14].

46 Vgl. URL: http://www.ploetzlichblackout.at/2014/10/01/svu-14-überwinden-der-krise/ [24.10.14].

47 Vgl. SVU 14 – Newsletter Juni unter URL: http://www.vbs.admin.ch/internet/vbs/de/home/themen/security/svu14/dokumente.parsys.9373.downloadList.82421.DownloadFile.tmp/infosvu14junid.pdf [26.10.14].

48 Vgl. Belgiens Angst vor dem nächsten Winter unter URL: http://www.ploetzlichblackout.at/2014/08/21/belgiens-angst-vor-dem-nächsten-winter/ [24.10.14].

49 OECD/IFP: Futures Project on "Future Global Shocks - Geomagnetic Storms". Im: Internet, 2011, unter URL: http://www.oecd.org/dataoecd/57/25/46891645.pdf [24.10.14].

Es gibt eine beachtliche Bedrohung für unsere Infrastruktursysteme, die von geomagnetischen Sonnenstürmen ausgehen. Auch hier ist wiederum unsere Strominfrastruktur aufgrund des derzeitigen Systemdesigns massiv gefährdet.[50]

Im Zusammenhang mit dem schwellenden Konflikt mit Russland wurde ein europäischer Stresstest bei der Gasversorgung durchgeführt. Die Regulierungsbehörden versuchen zu beruhigen, indem festgehalten wird, dass bei einer Gaslieferungsunterbrechnung aus Russland für mehrere Monate keine Gefahr droht. Gleichzeitig hätte 2012 der damalige Engpass in der Gasversorgung beinahe zum Blackout geführt. Auch hier wissen wir nicht, welche sonstigen Abhängigkeiten und Wechselwirkungen es noch gibt.[51]

Allein diese wenigen Beispiele weisen auf eine massive Verwundbarkeit unserer Kritischen Infrastruktur und damit auch unserer Gesellschaft hin. All diese Aspekte werden aber bisher beim Thema „Schutz Kritischer Infrastrukturen" kaum berücksichtigt. Was 2013 auch durch die EU-Kommission eingestanden wurde:

> *„The review process of the current EPCIP, conducted in close cooperation with the Member States and other stakeholders, revealed that there has not been enough consideration of the links between critical infrastructures in different sectors, nor indeed across national boundaries.*
>
> *(...) The studies indicate that risk assessment methodologies for CIP follow either: 1) a sectoral approach, where each sector is treated separately with its own risk methodologies and risk ranking; or 2) a systems approach, where critical infrastructures are treated as an interconnected network. Most work has been sectoral, but these methodologies show their limits when cross-sectoral issues need to be addressed, so a systems approach will be by the Commission from now on."*[52]

Der Schutz Kritischer Infrastrukturen (SKI) reicht bei weitem nicht mehr aus, sondern wir benötigen ebenso einen „Schutz VOR Kritischer Infrastruktur", einen Plan B, sollte es zu einem größeren Ausfall in dieser kommen.

Mittel- bis langfristig kann mit der derzeitigen Systemgestaltung und den hochgradig vernetzten und wechselseitigen Abhängigkeiten Sicherheit und der Schutz der Bevölkerung nicht gewährleistet werden. Daher hat sich in der Natur „small is beautiful" durchgesetzt, da zu große Strukturen anfälliger gegenüber Störungen sind. Die Natur begrenzt nicht die Interaktionen zwischen den Wesen, sondern nur ihre Größe.[53] Es erscheint daher mehr als notwendig, auch bei unseren komplexen technischen Systemen und Lösungen von der Natur zu lernen, um ein langfristige Lebensfähigkeit sicherzustellen.

50 Vgl. Ein heftiger Sonnensturm hat die Erde im Juli 2012 knapp verfehlt unter URL: http://www.ploetzlichblackout.at/2014/07/26/ein-heftiger-sonnensturm-hat-die-erde-im-juli-2012-knapp-verfehlt/ [24.10.14].

51 Vgl. Druckmittel Gas: Reale Gefahr oder Hysterie? unter URL: http://www.ploetzlichblackout.at/2014/08/29/druckmittel-gas-reale-gefahr-oder-hysterie/ [24.10.14].

52 European Commission: COMMISSION STAFF WORKING DOCUMENT: on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. In Internet unter URL: http://ec.europa.eu/energy/infrastructure/doc/critical/20130828_epcip_commission_staff_working_document.pdf [24.10.14].

53 Vgl. Vester, Frederic. Die Kunst vernetzt zu denken/Ideen und Werkzeuge für einen neuen Umgang mit Komplexität: Ideen und Werkzeuge für einen neuen Umgang mit Komplexität. Ein Bericht an den Club of Rome. München: Deutscher Taschenbuch Verlag, 2011[8]

Systemgestaltung
Die Systemsicherheit jegliches Systems kann mit einfachen Grundregeln – gegenüber jeglicher Störungen – erhöht werden, egal ob eine Störung durch einen Fehler, ein Naturereignis, durch Zufall oder durch einen Aggressor ausgelöst wurde.

Energiebedarfssenkung
Jede evolutionäre Weiterentwicklung erfolgt in der Natur über eine Energiebedarfssenkung. Damit können die externen Abhängigkeiten reduziert und die Lebensfähig eines Systems erhöht werden. Wobei dies nicht nur die klassischen Energieformen betrifft. Auch unser hochgradig synchronisiertes Logistik- und Versorgungssystem für unsere Lebensmittelgrundversorgung weist massive Verwundbarkeiten auf.[54] Ganz zu schweigen vom hohen Energieaufwand, der durch die Transport- und Verarbeitungsprozesse notwendig ist. Zudem ist eine Energieversorgung wie bisher mit einer volatilen Erzeugung nicht möglich. Die Energiewende kann nur gelingen, wenn wir unseren Bedarf durch intelligente Maßnahmen deutlich senken können. Das erfordert einen Kulturwandel und nicht nur technische Lösungen. Damit können aber auch Abhängigkeiten, wie sie im Industriezeitalter notwendig waren, reduziert werden.

Dezentralität
Der zweite Aspekt ist die Dezentralität. Komplexe Systeme lassen sich nicht zentral steuern und organisieren. Sie erfordern dezentrale selbstregulierende Rückkopplungsprozesse. Dezentrale Systeme sind zugleich robuster und resistenter gegenüber Störungen. Dabei spielt die Selbstorganisationsfähigkeit eine wesentliche Rolle, die grundsätzlich systemimmanent vorhanden ist. Dezentralität bedeutet jedoch nicht eine Isolierung oder Abkapselung, ganz im Gegenteil. Dezentralität bedeutet die Bildung von lebensfähigen Strukturen, die durchaus mit anderen Strukturen wieder ein gemeinsames Größeres bilden können (Zellenstruktur). Jedoch nicht durch eine chaotische Vernetzung. Viele Strukturen waren bereits vor der technischen Vernetzung vorhanden. Sie müssen nicht neu erfunden werden. Mit den heutigen Möglichkeiten kann jedoch ein zusätzlicher Mehrwert geschaffen werden, ohne dabei das gesamte System aufs Spiel zu setzen.

Fehlerfreundlichkeit
Ein weiterer Aspekt ist die Fehlerfreundlichkeit bzw. Fehlertoleranz in einem Systemen. Wir haben unsere technischen System weitgehend optimiert und versuchen so weit als möglich Fehler auszuschließen. Was vor allem beim Faktor „Mensch“ regelmäßig scheitert. Aber anstatt dass wir die Technik an die Menschen anpassen, versuchen wir es weiterhin umgekehrt. Mit wenig Erfolgsaussicht. In der Natur werden Störungen nicht ausgeschaltet, sondern in den Verlauf eingebunden. Dazu sind Freiräume, Puffer, Redundanzen, Variationen, Vielfalt, Flexibilität und eine Wandlungs- und Anpassungsfähigkeit erforderlich. Besonders wichtig sind Barrieren, um eine Reichweitenbegrenzung bei Störungen sicherstellen zu können.

Das europäische Stromversorgungssystem verfügt heute nur über unzureichende Barrieren, die eine Ausbreitung einer Störung verhindern könnten. Dadurch kann sich innerhalb weniger Sekunden eine Großstörung über den gesamten Kontinent ausbreiten.

54 Querverweis Kees - It is clear that any disruption in the supply of raw materials and goods to Europe would have devastating economic effects on countries including the Netherlands. Securing supply routes, protecting vital infrastructure and promoting stability in states or regions can reduce these risks

Das Internet verfügt zwar über unzählige Subnetze, aber es fehlt an der Vielfalt bei den Systemelementen. Dadurch kann sich etwa Schadsoftware sehr rasch ausbreiten. Zudem sind beide Systeme „too big to fail". Die Fehlerfreundlichkeit eines Systems ist Voraussetzung, damit auch Unsicherheiten und Turbulenzen bewältigt werden können. Und sie beschränkt sich nicht nur auf technische Systeme.

Wir haben in den letzten Jahren versucht, durch immer höhere Aufwände jegliche Unsicherheiten zu minimieren oder sogar auszuschalten. Wir haben uns zu einer Art „Vollkaskogesellschaft" entwickelt, die immer weniger in der Lage ist, auch mit Turbulenzen oder Ausfällen von wichtigen Infrastrukturen umzugehen. Auch hier sind daher neue Denkansätze erforderlich.

Resilienz

Um die Sicherheit für die Gesellschaft zu erhöhen, ist neben der Berücksichtigung der genannten Aspekte ebenso die Resilienz der Menschen entscheidend. Dieser Begriff ist im deutschsprachigen Raum noch nicht sehr geläufig, gewinnt aber zunehmend an Bedeutung. Er beschreibt die Fähigkeit eines Systems, mit Störungen sinnvoll umzugehen. Er wird auch häufig einfach mit Widerstandsfähigkeit übersetzt, was aber zu kurz greift. Es geht nicht nur um Robustheit, sondern auch um Anpassungs- und Erholungsfähigkeit sowie um Agilität. Dies inkludiert die Fähigkeit, gestärkt aus Störungen herauszugehen. Resiliente Systeme können nach einer Störungen in den ursprünglichen Zustande zurückkehren, oder auf eine verbesserte transformierte Ebene gelangen.[55] Der Begriff „Resilienz" wird in der Psychologie verwendet, um Menschen zu beschreiben, die trotz widriger Umstände gestärkt aus Krisen hervorgehen, während andere daran zerbrechen.

Was heißt das nun konkret? Viele Menschen sind gewohnt, dass immer irgendjemand zuständig ist und zur Hilfe eilen kann („Vollkaskogesellschaft"). Bei strategischen Schockereignissen sind jedoch die Ressourcen begrenzt. Nur wenn eine gewissen Eigenvorsorge und Eigenverantwortung übernommen wird, lassen sich solche Ereignisse sinnvoll als Gesellschaft meistern. Darüber hinaus führt eine Risikomündigkeit und Selbstwirksamkeit automatisch zu mehr Resilienz. Auswirkungen von etwa hybriden Bedrohungen werden dadurch begrenzt. Das Gesamtsystem Gesellschaft wird resilienter.

Zusammenfassung

Die vorliegende systemische Betrachtung kommt zum Schluss, dass aktuelle sicherheitspolitische Einschätzungen, wie sie etwa auch in der europäischen Sicherheitsstrategie niedergeschrieben wurden, bei weitem nicht ausreichen, um die aktuelle Bedrohungslage zu beschreiben:

> *„Bei einer Summierung dieser verschiedenen Elemente – extrem gewaltbereite Terroristen, Verfügbarkeit von Massenvernichtungswaffen, Organisierte Kriminalität, Schwächung staatlicher Systeme und Privatisierung der Gewalt – ist es durchaus vorstellbar, dass Europa einer sehr ernsten Bedrohung ausgesetzt sein könnte."*[56]

55 Querverweis Kees - Homan Reducing that vulnerability — and therefore increasing our resilience — requires explicit attention.

56 Europäische Gemeinschaften: Europäische Sicherheitsstrategie: Ein sicheres Europa in einer besseren Welt. In: Internet unter URL: http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568DEC.pdf.

Eine systemische Betrachtung und vernetztes Denken erscheinen daher unverzichtbar, um mit den aktuellen und zukünftigen Herausforderungen sinnvoll und erfolgreich umgehen zu können. Sicherheit ist immer relativ und subjektiv. Wir haben es aber selber in der Hand, wie wir Betrachtungen und Mitteln einsetzen. Sicherheit bedeutet nicht die Ausschaltung von Unsicherheit, sondern einen vernünftigen Umgang damit. Denn Sicherheit und Weiterentwicklung ist ohne Unsicherheit nicht möglich. Beide Pole bedingen einander.[57]

Wie sich aus der Betrachtung auch ergeben hat, sollten wir von den bisher häufig isolierten „Silo"-Betrachtungen abrücken, da diese nicht den vernetzten Realitäten entsprechen und bestenfalls Scheinsicherheiten schaffen. Die veränderten Rahmenbedingungen führen nicht nur dazu, dass die Welt immer undurchsichtiger und unsteuerbarer wird, sondern auch dazu, dass eine Fremdsteuerung schwieriger bis unmöglich wird. Es geht daher weniger um die Erfassung von möglichen Akteuren und konkreten Bedrohungen, als vielmehr um eine aktive und robuste Systemgestaltung, die mit jeglichen Störungen, egal ob durch Angreifer, Fehler, Naturereignisse, oder was auch immer, ausgelöst wurden, umzugehen.

Um mit den sich daraus ergebenden Ambivalenzen besser umgehen zu können, ist ein „Sowohl-als-auch-Denken" erforderlich. Unser abendländisches „Entweder-oder-Denken" begrenzt die Möglichkeiten und behindert Lösungen. Die alte Weisheit des chinesischen Militärstrategen, Sunzi, wonach der Krieg und der Kampf möglichst vermieden werden sollte hat auch heute noch seine volle Gültigkeit. Wir sollten daher so wenig Angriffsflächen wie nur möglich bieten.

Daher ist es notwendig, dass wir die bisherigen „Silos" aufbrechen und eine kooperative Vernetzung und Zusammenarbeit zwischen Politik, Wirtschaft, Zivilgesellschaft und Wissenschaft sicherzustellen. Nur so wird es uns auch gelingen, systemische Risiken effektiv und effizient zu begrenzen und gleichzeitig den ökologischen, wirtschaftlichen und sozialen Nebenwirkungen der möglichen risikobegrenzenden Maßnahmen genügend Aufmerksamkeit zu schenken.[58] Wesentliche Kennzeichen der Netzwerkgesellschaft sind Transparenz, Partizipation und Kollaboration und die Bildung von ad-hoc Netzwerken. Nicht der Wettkampf, sondern die Kooperation steht im Vordergrund. Dabei darf nicht erwartet werden, dass sich alle Menschen aktiv einbringen. Wenn es jedoch gelingt, die jeweils „klügsten Köpfe" für das jeweilige Thema zusammenzubringen, dann werden wir auch wieder Lösungen entwickeln, die eine solche Bezeichnung verdienen und auch von der Gemeinschaft getragen werden.

Daraus lassen sich einige Aspekte für die österreichische Sicherheitspolitik und für das Österreichische Bundesheer im speziellen ableiten:

- Die Wehrpflicht sollte dazu genutzt werden, junge Menschen in der Selbstwirksamkeit und Selbsthilfefähigkeit auszubilden. Dies würde einen großen gesellschaftlichen Mehrwert schaffen und zur Erhöhung der gesamtgesellschaftlichen Resilienz beitragen.
- Das Selbstverständnis des Österreichischen Bundesheeres sollte sich stärker an den neuen Herausforderungen orientieren. Das Österreichische Bundesheer wird weder die Mittel noch das Verständnis für ein Massenheer der Industriegesellschaft erhal-

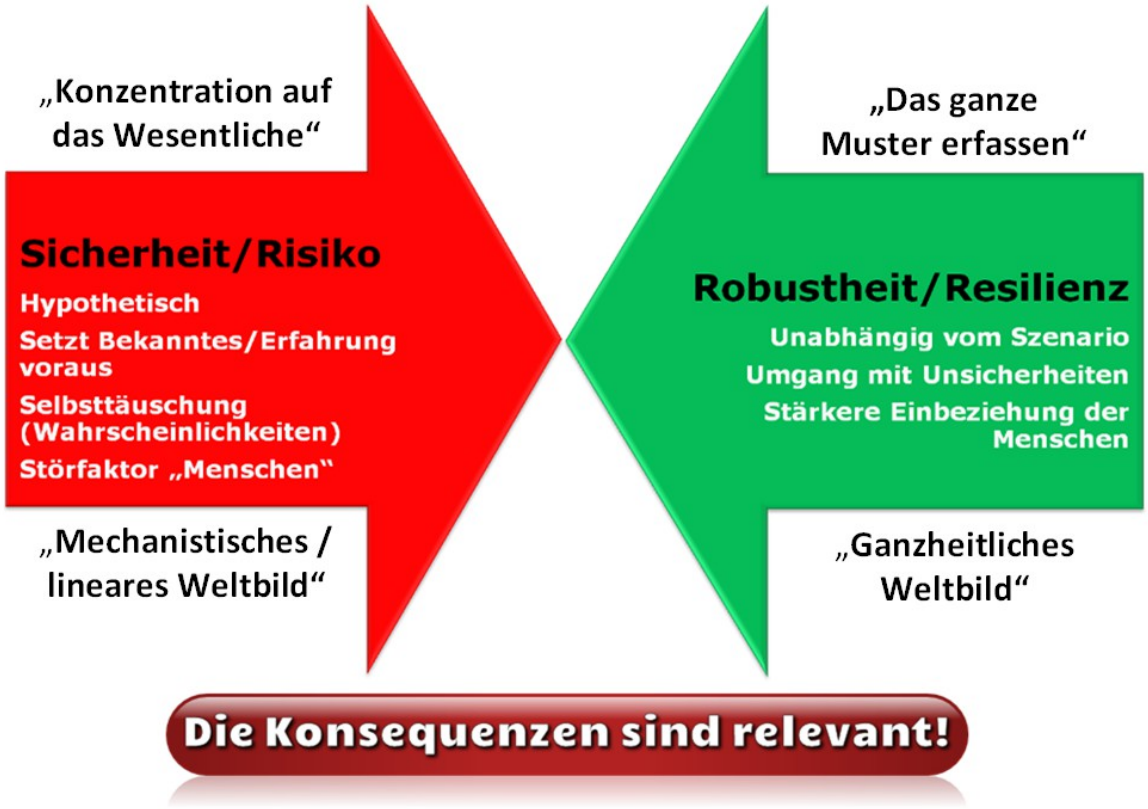
57 Vgl. Völkl, Kurt/Wallner, Heinz Peter. Das innere Spiel: Wie Entscheidung und Veränderung spielerisch gelingen. Göttingen: BusinessVillage GmbH, 2013

58 Vgl. Renn, Ortwin: Das Risikoparadox/Warum wir uns vor dem Falschen fürchten. Frankfurt am Main: Fischer Verlag, 2014.

ten. Die Armee der Netzwerkgesellschaft ist kleinteilig, flexibel und anpassungsfähig. Das bedingt vor allem flexibler Strukturen, die das ermöglichen. Das bedeutet aber auch, dass nicht die Fokussierung auf die Kernaufgaben (militärische Landesverteidigung), sondern eine Flexibilisierung notwendig ist, um auf möglichst viele Szenarien zum Wohle der Bevölkerung reagieren zu können. Unabhängig davon, wodurch diese ausgelöst wurden und ob sie im klassischen Sinn eine militärische Aufgabe darstellen.[59]

- Es ist eine Durchlässigkeit zwischen den unterschiedlichen Sicherheitsdomänen und einer besseren Kooperation erforderlich. Das Österreichische Bundesheer stellt eine gesamtstaatliche strategische Reserve dar, die gesellschaftlich unverzichtbar ist. Dabei geht es nicht nur um militärische Fähigkeiten, sondern um Fähigkeiten und Ressourcen, die sonst nicht vorgehalten werden (können). Dies könnte etwa auch bedeuten, dass Soldaten bei einem strategischen Schockereignis auf lokaler Ebene die Führung und Selbstorganisation übernehmen bzw. unterstützen. Dies erfordert ein Umdenken und eine Anpassung der Organisationskultur.
- Der Schutz Kritischer Infrastruktur muss neu ausgerichtet werden. Hoch vernetzte Objekte und Infrastrukturen können nicht mittels Objektschutz geschützt werden. Vielmehr ist zu erwarten, dass Soldaten nach einem möglichen Anschlag nicht zur Absicherung/zum Objektschutz, sondern zum Aufräumen erforderlich sein werden. Andere Maßnahmen, wie etwa die Erhöhung der IT-Sicherheit, stellen nur einen kleinen Teilbereich der heutigen Erfordernisse dar.
- Strategische Schocks können nicht verhindert werden. Wir können zwar die begünstigenden systemischen Risiken minimieren, was dennoch keinen vollständigen Schutz bietet. Wir müssen uns daher so ausrichten und aufstellen, dass wir derartige Ereignisse möglichst rasch überwinden und wieder zu einer neuen Realität zurückfinden können. Ein sinnvoller Umgang mit Unsicherheiten und Ungewissheiten ist dabei essentiell. Dies erfordert jedoch auch einen gesellschaftlichen Diskurs.
- Eine gesamtstaatliche Sicht ist erforderlich. Ein nationales Kompetenzzentrum für den Bevölkerungsschutz erscheint dringen geboten. Einerseits um die vielschichtigen Problemlagen und systemischen Risiken erfassen zu können und andererseits, um eine nationale oder sogar internationale Koordinierung und Sicht zu gewährleisten. Dabei darf aber kein neuer „Silo“ entstehen. Vielmehr ist die Vernetzung der bereits vorhandenen Einzelelemente in den Vordergrund zu stellen. Die Krisenbewältigung selbst muss auch weiterhin auf lokaler/regionaler Ebene und bei Bedarf auch autonom und durch Selbstorganisation erfolgen können.
- Versprechungen von technischen Lösungen sollten nicht unreflektiert akzeptiert werden. Mit vielen vermeintlichen Lösungen werde nur noch größere Probleme geschaffen.

59 Vgl. Eisregen in Slowenien mit nachfolgendem großflächigen Stromausfall Anfang 2014. Siehe unter URL: http://www.bundesheer.at/truppendienst/ausgaben/ausgabe.php?folge=340 [26.10.14].


„Konzentration auf das Wesentliche“
Sicherheit/Risiko
Hypothetisch
Setzt Bekanntes/Erfahrung voraus
Selbsttäuschung (Wahrscheinlichkeiten)
Störfaktor „Menschen“
„Mechanistisches / lineares Weltbild“
„Das ganze Muster erfassen“
Robustheit/Resilienz
Unabhängig vom Szenario
Umgang mit Unsicherheiten
Stärkere Einbeziehung der Menschen
„Ganzheitliches Weltbild“
Die Konsequenzen sind relevant!