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

Eine systemische Betrachtung sicherheitspolitisch relevanter Entwicklungen

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 - volatil, unsicher, komplex und ambivalent (Englisch: volatility, uncertainty, complexity and ambiguity). Diese Entwicklungen betreffen so gut wie alle Lebensbereiche. Gleichzeitig haben sich unsere altbewährten Denkmuster kaum verändert. Doch reicht das aus, um mit den neuen Herausforderungen zu Recht zu kommen?

Die vorliegende systemische Betrachtung wird mit einem Blick über den Tellerrand aktuelle und zukünftig erwartbare sicherheitspolitische Herausforderungen aus einem etwas anderen Blickwinkel beleuchten.

Ein wesentlicher Treiber für die Veränderungen nach dem Ende des Kalten Krieges war die exponentiell ansteigende Verbreitung von Informations- und Kommunikationstechnologien (IKT), der Basistechnologie des 5. Kondratieff-Zykluses, ab den 1990er Jahren. Mit den Kondratieff-Zyklen werden zyklische Wirtschaftsentwicklungen in der Dauer von rund 40-60 Jahren, wo je eine Basistechnologie/-innovation[1] die Entwicklungen bestimmt hat, beschrieben. Demnach befinden wir uns aktuell im abklingenden 5. bzw. am beginnenden 6. Zyklus, also in einer Umbruchphase. [Bild: Kondratieff-Zyklen]

Eine solche Umbruchphase wird auch von verschiedenen anderen Autoren und mit unterschiedlichen Blinkwinkeln für diese Dekade erwartet, welche sich mit der Transformation von der Industrie- zur Netzwerkgesellschaft zusammenfassen lässt. Ausschlaggebend dafür ist die zunehmende technische Vernetzung auf Basis der Informations- und Kommunikationstechnik. Eine steigende Vernetzung in einem System führt zu mehr Dynamik und Komplexität. [Bild: Vernetzung]

Systeme

Ein System beschreibt die funktionale Zusammensetzung von verschiedenen Systemelementen zu einem Ganzen. Entscheidend dabei sind die Beziehungen zwischen den Systemelementen, das „Wirkungsgefüge" bzw. die „unsichtbaren Fäden". Ein System ist daher mehr als die Summe der Einzelelemente. Was unspektakulär klingt, hat dennoch weitreichende Folgen, wie unzählige Beispiele bezeugen. Ob das beim Ausbruch des Ersten Weltkrieges (es ging zu Beginn eigentlich nur um Serbien), im Umweltbereich (Wildbachverbauungen, Umweltverschmutzung), bei der Entwicklungshilfe (Brunnenbau), bei Großprojekten wie dem Berliner Flughafen oder auch beim Finanzcrash 2007/2008 war, immer wurden die „unsicht-

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

baren Fäden“ zu anderen Systemen bzw. Umwelten unzureichend berücksichtigt bzw. unterschätzt. [Bild: Vermurung]

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. Daher darf ein System nicht als etwas Absolutes oder Starres verstanden werden.

Zudem wird zwischen einfachen, komplizierten und komplexen Systemen unterschieden. Einfache und komplizierte Systeme (etwa Maschinen) sind relativ einfach steuer-, manage-, und kontrollierbar. Komplizierte Systeme mögen unübersichtlich bzw. undurchschaubar erscheinen. Sie verfügen aber über einen standardisierten „Bauplan“ und lassen sich in ihre Einzelteile zerlegen und anschließend wieder zusammensetzen, ohne dass sich dadurch die Funktionalität oder das Systemverhalten ändert. Ganz im Gegensatz zu komplexen Systemen.

Komplexe Systeme

Steigt die Vernetzung in einem System bzw. mit der Umwelt, so entstehen komplexe Systeme mit einem differenzierten Systemverhalten. In komplexen Systemen kommt es zu laufenden Rückkopplungen, die den weiteren Prozessverlauf beeinflussen bzw. verändern. Es entstehen Eigendynamiken. Einfache Ursache-Wirkungszusammenhänge gehen verloren, die Steuerbarkeit (Management) sinkt bzw. wird unmöglich. Es kommt zu langen Ursache-Wirkungsketten. Eingriffe wirken sich häufig erst zeitverzögert aus und sind irreversible (zum Beispiel Klimawandel). 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 (Nebenfolgen), die im Vorhinein kaum abschätzbar sind und daher durch unsere etablierten Risikobewertungsmethoden nicht erfasst werden (können). Eine fehlende Reichweitenbegrenzung ermöglicht Domino- und Kaskadeneffekte, die umso verheerender ausfallen können, je größer das vernetzte System ist. Die Lösung eines Problems schafft leicht neue Probleme (Gefahr von Aktionismus). Es kommt zu exponentiellen Entwicklungen und zur Erhöhung der Dynamik, mit denen wir nur sehr schlecht umgehen können. [Bild: Dominoeffekt]

Das alles mag auf den ersten Blick wenig Praxisbezug aufweisen. Bei einer näheren Betrachtung finden sich jedoch unzählige Beispiele aus dem täglichen Leben, wo genau diese Aspekte eine ganz zentrale Rolle spiel(t)en. Hinzu kommt, dass wir erst seit sehr kurzer Zeit mit komplexen technischen Systemen konfrontiert sind und es noch wenig Erfahrungswissen gibt. Beispiele wie, die zeitverzögerten negativen Auswirkungen durch das Internet (Cyber-Angriffe, Sicherheitsschwachstellen), ein Terroranschlag der zwei Kriege zur Folge hatte (9/11) oder ein fehlgeleitetes Finanzsystem, immer spielt die unterschätzte Komplexität und Nicht-Steuerbarkeit eine Rolle. Zeitgleich sind wir permanent von komplexen Systemen umgeben, da die Natur nur aus offenen, dynamischen und damit komplexen Systemen besteht.

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 Sys-

tems zu, was wiederum dazu führt, dass es zu einer spontanen Selbstorganisation und zu einer Nichtvorhersagbarkeit der Entwicklungen kommt. Berücksichtigt man diese Aspekte bei der Betrachtung von aktuellen Entwicklungen, so erscheinen diese in einem neuen Licht.

Islamischer Staat

So wird etwa begreifbarer, wie faktisch aus dem Nichts eine Organisation wie der Islamische Staat (IS) unrühmliche Weltbekanntheit erlangen konnte. Nur durch die Möglichkeiten der technischen Vernetzung konnte eine spontane und weitreichende Selbstorganisation erfolgen. In diesem negativen Fall führte das innerhalb kürzester Zeit zu einer weiträumigen Destabilisierung und Schreckensherrschaft. Verstärkt wurde das Ganze durch die Desinformations- und Propagandamöglichkeiten, die durch das Internet bereit gestellt werden. Daran ist aber weniger das Transportmedium schuld, als viel mehr, wie wir uns selbst dadurch manipulieren (lassen). [Bild: Computer/Internet]

Die Gegenreaktionen – insbesondere die Luftschläge – zeigen bisher wenig Wirkung. Ganz abgesehen davon, dass die Folgewirkungen kaum abschätzbar sind. Die steigende Sorge vor möglichen Anschlägen in anderen Ländern ist daher mehr als begründet, werden diese doch mit einer Zersplitterung deutlich wahrscheinlicher. Nichts zu tun, wäre aber genauso falsch, womit sich hier die Widersprüchlichkeit (VUC-Ambivalenz) widerspiegelt.

Terrorismus

Um Terrorismus begegnen zu können, muss man zuerst seine Funktionsweise verstehen, wenngleich es keinen homogenen Terrorismus gibt. Kurz und knapp dargestellt wirkt Terrorismus im Wesentlichen zweimal. Einmal durch die unmittelbaren Auswirkungen etwa eines Anschlages und das zweite Mal, durch die beim Opfer hervorgerufenen Reaktionen. Aus verschiedenen Untersuchungen ist etwa bekannt, dass in der Regel 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. Damit führt eigentlich nicht das unmittelbare Ereignis, sondern die Reaktionen darauf zu den wesentlich größeren Schäden und dies nicht nur auf finanzieller Basis oder so offensichtlich, wie nach 9/11. Eine große Anzahl von unschuldigen Menschen verlor in Folge des „Kampfes gegen den Terror“ ihr Leben. Neben den unzähligen Soldaten eine noch viel größere Anzahl von Zivilisten – direkt, aber auch indirekt. Zudem haben wir erhebliche Freiheitseinschränkungen oder eine sehr weitgehende Überwachung in Kauf genommen, um vermeintlich die Sicherheit zu erhöhen, was aber eher einen Trugschluss darstellt, wie sich im weiteren Verlauf noch zeigen wird. [Bild: 9/11]

In den vergangenen Jahren gab es jedoch auch positive Beispiele, wo nicht sofort überreagiert wurde. Etwa nach den Anschlägen auf das öffentliche Verkehrssystem in London im Jahr 2005, da man Anschläge erwartet und sich darauf vorbereitet hat. Auch nach dem Einzeltäteranschlag in Norwegen, wo 2011 77 Menschen getötet wurden, wurde auf eine Anlassgesetzgebung und Überreaktion verzichtet.

Ein für die westliche Welt de facto unlösbares Problem stellen die geänderten Zielvorstellungen von aktuellen Terrorgruppen dar. Während im 20. Jahrhundert mit Terrorismus noch vorwiegend (regional)politische Ziele verfolgt wurden, wozu man etwa auch Rücksicht auf die (gegnerische) Bevölkerung nehmen musste, hat sich das seit 9/11 grundlegend geändert. Fundamentalistische, vorwiegend islamische Gruppierungen, verfolgen nicht mehr irdische

Ziele, womit wichtige Hemmschwellen wegfallen. Es sollte daher mit deutlich höheren Schäden durch zukünftige terroristische Anschläge gerechnet werden.

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 wie auch der Soziologe Ulrich Beck sehen 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. Hier besteht wiederum ein unmittelbarer Bezug zu unserer westlichen Lebensweise und zu unserem Konsumverhalten. Eine reine militärische oder sicherheitspolitische Herangehensweise greift daher bei weitem zu Kurz und lässt viele Aspekte unberücksichtigt. Hinzu kommt, dass es hierfür keine einfachen technischen Lösungen, wie sie sonst gerne versprochen werden, gibt.

Cyber-Bedrohungen

Ähnlich wie beim Terrorismus erfolgt die Auseinandersetzung auch mit den Cyber-Bedrohungen. Während sie lange Zeit vernachlässigt wurden, ist hier nun ebenfalls sehr viel Aktionismus und Scheinsicherheit zu beobachten.

Während sich viele Organisationen und Initiativen auf die Erhöhung der Daten- und IT-Sicherheit fokussieren, bleiben andere weit wesentlichere Aspekte oft unberücksichtigt. So gibt es etwa seit Monaten Hinweise auf gezielte Cyber-Angriffe auf westliche Energieversorgungsunternehmen, die vermeintlich aus Russland kommen, was bei Cyber-Angriffen nie eindeutig feststellbar ist. Hier sollten auf jeden Fall die Alarmglocken läuten. 2007 hat die Versetzung eines russischen Denkmals zu einem massiven – nicht, wie häufig dargestellt wird, rein staatlich koordinierten – Cyber-Angriff auf Estland geführt, der auch gerne als erster Cyber-War dargestellt wird. Damals waren weitgehend „nur" virtuelle Systeme betroffen. Heute könnte dabei unsere wichtigste und zugleich kritischste Infrastruktur zum Ausfall gebracht werden, geplant oder auch ungeplant. Dabei sollte dringend davon Abstand genommen werden, einen klaren Akteur auszumachen. Gerade Cyber-Angriffe können äußerst rasch außer Kontrolle geraten und unvorhergesehene Eigendynamiken entwickeln, da jeder, der sich gerade berufen fühlt und die Voraussetzungen mitbringt, daran teilnehmen kann, ohne dass es dazu einer zentralen Koordinierung bedarf – sozusagen eine spontane Selbstorganisation erfolgt. [Bild: Denkmal Talin]

In der Schweiz wurde dieses Szenario als Ausgang für die Sicherheitsverbundsübung 2014 (SVU 14) herangezogen, in Folge dessen es zu Instabilitäten im Stromversorgungssystem kommt, was wiederum zu einem Blackout – einen plötzlichen, überregionalen und länger andauernden Strom- und Infrastrukturausfall – führt. Dabei wurde als noch viel schlimmer die darauffolgende mehrwöchige Strommangellage identifiziert, da wir weder als Gesellschaft noch unsere Infrastrukturen auf ein solches mögliches strategisches Schockereignis vorbereitet sind. Auch der aktuelle Schweizer Risikobericht 2015 schätzt eine Pandemie und eine mehrwöchige Strommangellage bzw. ein Blackout als die wahrscheinlichsten und folgenschwersten Ereignisse für die Schweiz in absehbarer Zukunft ein. All diese Szenarien kennen keine Ländergrenzen. Zum anderen zeigt sich hier, dass die Betrachtung einer Domäne alleine nicht ausreicht, sondern auch die möglichen Querverbindungen („unsichtbaren Fäden") erfasst und berücksichtigt werden müssen.

Auf der Hackerkonferenz Black Hat 2014 zeigten Forscher, wie es ihnen gelungen ist, einen in Spanien bereits millionenfach ausgerollten „intelligenten" Stromzähler („Smart Meter") zu kompromittieren und eine Fernabschaltung über das Netzwerk zu initiieren. Möglicherweise ein neues und finanziell lukratives Geschäftsmodell für die Organisierte Kriminalität, oder für Akteure, die nichts Gutes im Schilde führen. [Bild: Smart Meter]

Aber es muss gar nicht immer ein Angriff sein. Eine aktuelle deutsche Studie kommt zum Schluss, dass mit einem intendierten „Gierverhalten" der Konsumenten beim Einsatz von „intelligenten" Stromzählern Blackouts ausgelöst werden könnten. Das erfordert natürlich zusätzlich ein gerade instabiles System, was derzeit aber immer häufiger gegeben ist. Dabei spielt die Vernetzung und die reine Fokussierung auf monetäre Vorteile eine wesentliche Rolle. Ein solches Verhalten hat bereits 2012 auf der Stromhändlerseite beinahe zur Katastrophe geführt.

Ein anderes Beispiel für nicht intendierte Nebenfolgen passierte am 01.01.2010. Damals versagten in Deutschland rund 30 Millionen EC- und Kreditkarten, da die Mikrochips fehlerhaft programmiert waren. Die betroffenen Kunden konnten weder an Geldautomaten Bargeld abheben noch damit bargeldlos bezahlen. Ein solcher Fehler in einer wichtigen Komponente in einer hoch vernetzen Infrastruktur hätte wahrscheinlich verheerende Folgen.

Auch wenn es bisher überraschender Weise noch keine größeren Zwischenfälle gab, befinden wir uns hier in einer gefährlichen „Truthahn-Illusion". 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. Sein Vertrauen steigt mit jeder positiven Erfahrung (Fütterung). Am Tag vor Thanksgiving (bei dem traditionell die Truthähne geschlachtet werden) erlebt der Truthahn allerdings eine fatale Überraschung. [Bild: Truthahn-Illusion] Auch wir orientieren uns gerne an der Vergangenheit und übersehen dabei leicht die sich vor uns veränderten Rahmenbedingungen.

Aktuelle Cyber-Sicherheitskonzepte berücksichtigen viele dieser Faktoren nur bedingt, geht es doch häufig vorwiegend um Datendiebstahl, Cyber-Kriminalität und Datenschutz bzw. nur um die Verhinderung oder Meldung von Ereignissen. Ganz abgesehen davon, dass Cyber-Defence in einem vernetzten System keine zweite Verteidigungslinie darstellt, wie das derzeit gerne gesehen wird.

Gasversorgung

Im Zusammenhang mit dem schwelenden Konflikt mit Russland wurde im Herbst 2014 ein europäischer Stresstest bei der Gasversorgung durchgeführt. Die Regulierungsbehörden versuchten zu beruhigen, indem festgehalten wurde, dass bei einer Gaslieferunterbrechnung aus Russland für mehrere Monate keine Gefahr droht. Gleichzeitig hätte 2012 der damalige Engpass in der Gasversorgung beinahe zum Blackout geführt. Zum anderen führt eine nähere Betrachtung der Gasversorgung zu Tage, dass wir eigentlich wider den Aussagen der Regulierungsbehörden kaum große Spielräume haben, um längere Gaslieferunterbrechungen kompensieren zu können. Besonders spannend dürfte daher der Winter 2015/16 werden, nachdem im Gegensatz zu 2014 Anfang August die österreichischen Speicher statt mit 81 % nur zu 48 % gefüllt waren. Auch auf europäischer Ebene gab es zu diesem Zeitpunkt eine erhebliche negative Bilanz von fast 20 %. Auch hier wissen wir meistens nicht, welche sonstigen Abhängigkeiten und Wechselwirkungen es noch gibt. Außer etwa, dass die Lebensmittelgrundversorgung massiv von einer funktionierenden Gasversorgung abhängig ist.

Sonnenstürme

Eine völlig andere Bedrohung für unsere moderne Lebensweise geht etwa von Sonnenstürmen (Koronaler Massenauswurf) aus. Die OECD hält dazu in ihrer Studie „Future Global Shocks - Geomagnetic Storms“ fest: [Bild: Sonnenstürme]

> *„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.“*

Flüchtlingsströme

Dieses Thema hat nur bedingt mit der Kritischen Infrastrukturen zu tun, führt aber vor Augen, wie schnell unsere bisher bewährten Bewältigungsmechanismen mit neuen Szenarien überfordert sein können. Wobei es hier wohl mehr am Willen und „Silodenken“ als am Können scheitert. Zudem zeigt sich, dass die Zivilgesellschaft durchaus bereit ist, die Dinge selbst in die Hand zu nehmen und zu helfen, wenngleich es dazu eine viel größere negativ eingestellte Gruppe gibt. Hier zeigt sich, dass man mit ignorieren – was lange genug passiert ist – Probleme nicht aus der Welt schaffen kann. [Bild: Flüchtlingszelt]

Verwundbarkeit unserer Kritischen Infrastrukturen und unserer Lebensweise

All diese Beispiele sollen aufzeigen, dass es gar nicht um mögliche Akteure geht, sondern vielmehr um die Verwundbarkeit unserer modernen Lebensweise, die ganz eng mit der Kritischen Infrastruktur verbunden ist. Die wirkliche Bedrohung für unsere Sicherheit und Gesellschaft geht nicht von Datenverlusten bzw. -diebstählen oder Terroranschlägen aus, sondern von den zunehmend vernetzten und verwundbaren Kritischen Infrastrukturen. Größere Störungen können heute weitreichende Dominoeffekte auszulösen. Wobei es unerheblich ist, ob ein Dominoeffekt durch einen Angriff, einen Fehler, ein technisches Versagen, ein Extremwetterereignis oder was auch immer ausgelöst wird. 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 sind, noch dass wir dafür einen Plan B hätten, oder dass es eine klare Verantwortlichkeit geben würde. Die bisher sehr erfolgreichen und bewährten Krisenmanagement-Modelle reichen dazu bei weitem nicht mehr aus. Hinzu kommt, dass diese Aspekte beim „Schutz Kritischer Infrastrukturen“ (SKI) kaum berücksichtigt werden, was etwa 2013 durch die EU-Kommission auch eingestanden wurde:

> *„The review process of the current European Programme for Critical Infrastructure Protection (EPCIP), conducted in close cooperation with the Member States and other stakeholders, revealed that there has not been enough consideration of the links* [“unsichtbare Fäden”] *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.“*

Der Schutz Kritischer Infrastrukturen im herkömmlichen Sinne reicht daher bei weitem nicht mehr aus. Wir benötigen ebenso einen „Schutz VOR Kritischer Infrastruktur“, einen Plan B, sollte es zu einem größeren Ausfall oder Störungen in diesen Bereichen kommen. Es ist nicht schlimm, dass etwas passieren kann, denn es gibt nirgends eine 100 % Sicherheit. Unverantwortlich ist nur, wenn wir uns einfach darauf verlassen, dass nichts passiert und keine Rückfallebenen vorsehen, wie das derzeit weitgehend der Fall ist bzw. dass wir an alte Konzepte festhalten, wo sich jedoch die Rahmenbedingungen wesentlich verändert haben.

Mittel- bis langfristig kann mit der derzeitigen Systemgestaltung und den hochgradig vernetzten und wechselseitigen Abhängigkeiten Sicherheit und der Schutz der Bevölkerung nicht gewährleistet werden.

Was ist dann die Lösung?
Eine berechtigte Frage. Die schlechte Nachricht: es gibt keine Musterlösung! Es zeichnet sich jedoch ganz klar ab, dass der Umgang mit volatilen, unsicheren, komplexen und ambivalenten Entwicklungen ein an die neuen Rahmenbedingungen angepasstes Denken und Handeln erfordert, dass mit „vernetztem Denken“ zusammengefasst werden kann. Die bisherigen „(Macht-)Silos“ sind dazu wenig eignet, da wir es zunehmend mit hoch komplexen und weitreichend vernetzten Querschnittmaterien zu tun haben, die nicht seriell abgearbeitet werden können, wie das etwa heute im Bereich Cyber-Sicherheit und Cyber-Defence angedacht ist. Um rascher und agiler reagieren und auch agieren zu können, sind flachere und flexiblere Netzwerkstrukturen – nicht nur im technischen Bereich – erforderlich. Auch eine flexible kooperative Zusammenarbeit über bisher bestehende System- und Denkgrenzen hinaus erscheinen unverzichtbar. [Bild: Fragezeichen]

Beispielsweise verzichtet Schweden auf formalisierte Strategien und auf niedergeschriebene Konzepte. Dafür wird vielmehr auf eine flexible und der Realität angepasste Kooperationskultur Wert gelegt. Denn viele Strategiepapiere spiegeln nur formalisierte „Wunschvorstellungen“ wieder. Die tatsächliche Umsetzung weist meist erhebliche Defizite auf bzw. überholt die Realität meist die Umsetzung, wie das etwa auch bei vielen Heeresreformen der vergangenen Jahrzehnte der Fall war.

In der Slowakei wiederum wird ein Schulterschluss zwischen institutionellen, nichtstaatlichen als auch zivilgesellschaftlichen und kommerziellen Akteuren eingefordert. 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.

Ein anderer Aspekt betrifft organisatorische Maßnahmen. So verfügt etwa Schweden über ein Amt für Bevölkerungsschutz und Bereitschaft, Deutschland über hat Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und die Schweiz über das Bundesamt für Bevölkerungsschutz (BABS). Hingegen gibt es in Österreich keine derartige Einrichtung. Ganz im Gegenteil. Der Katastrophenschutz ist föderal organisiert und dementsprechend heterogen ist dieser abgebildet. Nationale oder sogar internationale Krisenlagen oder strategische Schockereignisse sind damit nur unzureichend abzubilden. Die Erfassung von systemischen Risiken ist kaum möglich, auch wenn verschiedene Teilaspekte in unterschiedlichen Ministerien behandelt werden mögen.

Organisationsübergreifende Ausbildung und Zusammenarbeit
In den vergangenen Jahren wurde aufgrund einiger Großereignisse, wie etwa der Europafußballmeisterschaft 2008, die Zusammenarbeit zwischen den unterschiedlichen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) deutlich verbessert. Dazu haben auch die Harmonisierung von Standardprozessen und eine vereinheitlichte Stabs- und Führungsarbeit beigetragen. Eine gemeinsame Ausbildung, zumindest aber übergreifende Ausbildungsmodule bzw. eine organisationsübergreifende Verwendung würden zu einem noch besseren Verständnis der jeweils anderen Seite beitragen und ein Handeln im Sinne des Ganzen unterstützen. [Bild: Interdisziplinäre Zusammenarbeit]

Möglicherweise wird der zunehmende budgetiere Druck dazu führen, dass in Zukunft verstärkt auf Synergiemöglichkeiten geachtet wird. 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 beneidet. Wir sollten sie daher bewusst als Stärke wahrnehmen, fördern und im Sinne des Ganzen nutzen.

Systemgestaltung
Die Systemsicherheit eines jeden Systems kann mit einfachen Grundregeln – gegenüber jeglichen Störungen – erhöht werden, egal wodurch eine Störung ausgelöst wird.

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 sondern Ressourcen generell betrifft. So weist etwa auch unser hochgradig arbeitsteiliges und synchronisiertes Logistik- und Versorgungssystem massive Verwundbarkeiten auf. 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 betrifft die Steuerung von komplexen Systemen. Nachdem sich diese aufgrund der systemimmanenten Wechselwirkungen und Rückkopplungen nicht zentral steuern lassen, sind dezentrale selbstregulierende Rückkopplungsprozesse bzw. Selbstorganisationsfähigkeiten erforderlich. Dezentrale Systeme sind gleichzeitig robuster und resistenter gegenüber Störungen. 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).

Fehlerfreundlichkeit
Ein weiterer Aspekt ist die Fehlerfreundlichkeit bzw. Fehlertoleranz in einem System. 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 die Ausbrei-

tungsmöglichkeit von Störungen zu reduzieren. Diese Fähigkeiten erfordern eine Abkehr von unseren Effizienzbestrebungen aus rein kurzfristigen und monetären Überlegungen. Zum anderen muss der Faktor „Mensch" als nicht berechenbar akzeptiert werden und die Fehlerfreundlichkeit der Technik erhöht werden. Menschen lassen sich nicht zuverlässig an die Technik anpassen.

Resilienz

Um die gesellschaftliche Sicherheit zu erhöhen, ist neben der Berücksichtigung der genanten Aspekte auch die Resilienz der Menschen entscheidend. Dieser Begriff ist im deutschsprachigen Raum noch nicht sehr geläufig. Er beschreibt die Fähigkeit eines Systems, mit Störungen sinnvoll umzugehen, dass bedeutet, sie nicht um jeden Preis ausschalten zu wollen, sondern auch mit Unsicherheiten umgehen zu können. Er wird häufig einfach mit Widerstandsfähigkeit übersetzt, was aber zu kurz greift. Es geht nicht nur um Robustheit (Schutz, entgegenhalten), sondern ebenso um Anpassungs- und Erholungsfähigkeit sowie um Agilität und Flexibilität (ausweichen; wie früher beim Jagdkampf). Dies inkludiert die Fähigkeit, gestärkt aus Störungen herauszugehen und aus Fehlern zu lernen. Resiliente Systeme können nach einer Störungen in den ursprünglichen Zustande zurückkehren, oder auf eine verbesserte transformierte Ebene gelangen. [Bild: Stehaufmännchen]

Viele Menschen sind gewohnt, dass immer irgendjemand zuständig ist und zur Hilfe eilen kann („Vollkaskogesellschaft"). Bei strategischen Schockereignissen sind jedoch diese Ressourcen begrenzt. Nur wenn eine gewissen Eigenvorsorge und Eigenverantwortung vorgenommen wird, lassen sich solche Ereignisse als Gesellschaft mit beschränkten Schäden meistern. Darüber hinaus führt eine Risikomündigkeit und Selbstwirksamkeit automatisch zu mehr Resilienz und zu einer höheren gesellschaftlichen Stabilität.

Zusammenfassung

Mit der vorliegenden systemischen Betrachtung wurde versucht, verschiedene aktuelle sicherheitspolitische Herausforderungen aus einem etwas anderen Blickwinkel zu betrachten. Dabei konnten viele Themen nur angerissen bzw. oberflächlich betrachtet werden. Dennoch sollte damit das Bewusstsein geschärft worden sein, dass die Dinge nicht einzeln und gemäß zugeordneter Verantwortung betrachtet werden können, sondern dass eine Gesamtsicht erforderlich ist. Auch im Sinne der Ökonomie der Kräfte, um etwa gesamtgesellschaftlich möglichst wenig und vor allem die richtigen Ressourcen einzusetzen. Ein Paradigmenwechsel in der Sicherheitsbetrachtung erscheint daher unverzichtbar.

Die alte Weisheit des chinesischen Militärstrategen, Sunzi, wonach der Krieg und der Kampf möglichst vermieden werden sollte, hat auch heute noch seine volle Gültigkeit, wenngleich wir das stärker aus dem Blickwinkel der Verwundbarkeit bzw. Reduktion der Angriffsflächen sehen sollten.

Sicherheit bedeutet nicht die Ausschaltung von Unsicherheiten, sondern den vernünftigen Umgang mit diesen. Denn Sicherheit und Weiterentwicklung ist ohne Unsicherheit nicht möglich. Beide Pole bedingen einander.

Um mit den sich ergebenden Ambivalenzen besser umgehen zu können, ist ein „Sowohl-als-auch-Denken" erforderlich. Unser abendländisches „Entweder-oder-Denken" begrenzt oft die Möglichkeiten und behindert Lösungen.

Eine stärkere kooperative Vernetzung und Zusammenarbeit zwischen Politik, Wirtschaft, Zivilgesellschaft und Wissenschaft ist unverzichtbar, um den neuen vielschichtigen Herausfor-

derungen zu begegnen. Dabei spielen Transparenz, Partizipation und Kollaboration sowie die Bildung von ad-hoc Netzwerken eine wesentliche Rolle. Nicht der Wettkampf bzw. ein Machtdenken, sondern die Kooperation ist in den Vordergrund zu stellen. [Bild: Vernetzung]

Sicherheitspolitische Ableitungen

Hierzu lassen sich aus meiner Sicht einige demonstrative 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 erhalten. Die Armee der Netzwerkgesellschaft ist kleinteilig, flexibel und anpassungsfähig. Das bedingt vor allem flexibler Strukturen, was eine Änderung der Geisteshaltung voraussetzt. Das bedeutet aber auch, dass nicht die Fokussierung auf die Kernaufgaben (militärische Landesverteidigung), sondern eine Flexibilisierung notwendig ist, um auf möglichst viele Ereignisse zum Wohle der Bevölkerung – des Souverän - reagieren zu können. Unabhängig davon, wodurch diese ausgelöst werden und ob sie im klassischen Sinn eine militärische Aufgabe darstellen.
- Eine klassische Landesverteidigung ist nicht völlig obsolet, da es auch weiterhin Länder mit einer vorwiegend industriegesellschaftlichen Prägung inklusive einem Massenheer geben wird. Entsprechende Fähigkeiten, um derartigen Bedrohungen auch weiterhin begegnen zu können, erfordern jedoch transnationale Kooperationen bzw. die Entwicklung von neuen Fähigkeiten auf Basis der Netzwerkgesellschaft.
- Eine Durchlässigkeit zwischen den unterschiedlichen nationalen Sicherheitsdomänen und eine bessere Kooperation erscheinen zur Förderung des gegenseitigen Verständnisses und zur Verbesserung der Zusammenarbeit erforderlich.
- Das Österreichische Bundesheer stellt eine gesamtstaatliche strategische Reserve dar. Dabei geht es nicht nur um militärische Fähigkeiten, sondern auch um Ressourcen, die sonst nicht vorgehalten werden (können), um flexibel auf neue Herausforderungen reagieren zu können. Dies könnte etwa auch bedeuten, dass Soldaten bei einem strategischen Schockereignis auf lokaler Ebene die Führung und Selbstorganisation übernehmen bzw. unterstützen.
- 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/Katastrophe nicht zur Absicherung/zum Objektschutz/zur Cyber-Defence, sondern zum „Aufräumen“ und zur Wiederherstellung von Ordnung und Sicherheit erforderlich sein werden. [Bild: Objektschutz]
- Strategische Schockereignisse können nicht verhindert werden. Wir können zwar die begünstigenden systemischen Risiken minimieren, was dennoch keinen vollständigen

Schutz bietet. Daher gilt es, sich so aufzustellen, dass derartige Ereignisse möglichst rasch und gut bewältigt werden können.

- Eine gesamtstaatliche Sicht und „Orchestrierung“ ist erforderlich, was in einem nationalen Kompetenzzentrum für Bevölkerungsschutz abgebildet werden könnte. Einerseits um die vielschichtigen Herausforderungen und systemischen Risiken zu erfassen und andererseits, um eine nationale oder sogar internationale Koordinierung/“Orchestrierung“ zu gewährleisten. Dabei ist die Vernetzung der bereits vorhandenen Einzelelemente in den Vordergrund zu stellen. Die Krisenbewältigung selbst wird auch weiterhin auf lokaler/regionaler Ebene und bei Bedarf auch autonom und durch Selbstorganisation erfolgen. [Bild: Dirigent]
- Versprechungen von technischen Lösungen sollten nicht unreflektiert akzeptiert werden. Mit vielen vermeintlichen Lösungen werden nur noch größere Probleme geschaffen.

Durch diesen Blick über den Tellerrand soll eine Diskussion und die Bildung von neuen Denkräumen angestoßen werden, wie mit neuen Herausforderungen besser umgegangen werden könnte. Die Zurückziehung auf bisherige „Kernkompetenzen“ erscheint – wenn auch nachvollziehbar – nicht der richtige Weg zu sein, um aus den gegenwärtigen sicherheitspolitischen Krisen wieder gestärkt herauszugehen. Vielmehr scheint der alte Offiziersgrundsatz – anbieten und bewähren – gefragter den je!

Weiterführende Hintergrundinformationen und Betrachtungen sind auf www.saurugg.net zu finden.