



© BUNDESHEER/CHRISTIAN JOHANNES

Schutz kritischer Infrastruktur

# Sicherheitspolitisch relevante Entwicklungen

Eine systemische Betrachtung Teil 2

MAJOR HERBERT SAURUGG, MSC

**A**ll 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: ➤



© BUNDESHEER/KLAUSNER

Interdisziplinäre Zusammenarbeit

*„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 encouraged 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 hundertprozentige 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 alten Konzepten festhalten, wo sich jedoch die Rahmenbedingungen wesentlich verändert haben.

/ Mittel- bis langfristig können mit der derzeitigen Systemgestaltung und den hochgradig vernetzten und wechselseitigen Abhängigkeiten die 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, das mit „vernetztem Denken“ zusammengefasst werden kann. Die bisherigen „(Macht-)Silos“ sind dazu wenig geeignet, da wir es zunehmend mit hochkomplexen und weitreichend vernetzten Querschnittsmaterien 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 erscheint unverzichtbar.

/ 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, nicht-staatlichen 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 das 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 Fußball-Europameisterschaft 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

## **„VERNETZTE UNSICHERHEIT – HYBRIDE BEDROHUNGEN IM 21. JAHRHUNDERT“**

SCHRIFTENREIHE DER LANDESVERTEIDIGUNGS-AKADEMIE

Erscheinungsdatum: Juli 2015

Herausgeber: Oberst Mag. Anton Dengg, Mag. Michael Schurian

Verlag: Landesverteidigungsakademie (LVAK) /

Institut für Friedenssicherung und Konfliktmanagement (IFK)

ISBN: 978-3-902944-71-9

<http://www.bundesheer.at/wissen-forschung/publikationen/publikation.php?id=752>

bzw. eine organisationsübergreifende Verwendung würden zu einem noch besseren Verständnis der jeweils anderen Seite beitragen und ein Handeln im Sinne des Ganzen unterstützen.

/ Möglicherweise wird der zunehmende budgetäre 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 Lebensfähigkeit 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 ➤



© ANDREAS WASTIAN

### **ZUR PERSON**

**Herbert Saurugg, MSc**, war 15 Jahre Berufsoffizier des Österreichischen Bundesheers, zuletzt im Bereich IKT-/Cyber-Sicherheit. Seit 2012 beschäftigt er sich mit den möglichen Auswirkungen der steigenden Vernetzung und Komplexität, welche zu bisher kaum bekannten systemischen Risiken führen. Weiterführende Hintergrundinformationen und Betrachtungen finden Sie unter:

[www.saurugg.net](http://www.saurugg.net)  
[kontakt@saurugg.net](mailto:kontakt@saurugg.net)

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 Ausbreitungsmöglichkeit 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.

## **„Um die gesellschaftliche Sicherheit zu erhöhen, ist auch die Resilienz der Menschen entscheidend.“**

Menschen lassen sich nicht zuverlässig an die Technik anpassen.

### **Resilienz**

Um die gesellschaftliche Sicherheit zu erhöhen, ist neben der Berücksichtigung der genannten 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. Das 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 Störung in den ursprünglichen Zustand zurückkehren oder auf eine verbesserte transformierte Ebene gelangen.

## **„Sicherheit bedeutet nicht die Ausschaltung von Unsicherheiten, sondern den vernünftigen Umgang mit diesen.“**

/ Viele Menschen sind gewohnt, dass immer jemand zuständig ist und zur Hilfe eilen kann („Vollkaskogesellschaft“). Bei strategischen Schockereignissen sind jedoch diese Ressourcen begrenzt. Nur wenn eine gewisse 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, wenn gleich 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 sind 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 Herausforderungen 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.

### 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 Bundesheers 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 flexible 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

## „Das Österreichische Bundesheer stellt eine gesamtstaatliche strategische Reserve dar.“

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 ▶

**1. KOMMT ES ANDERS  
2. ALS MAN DENKT  
3. KEINE SORGE, ICH KÜMMERE  
MICH PERSÖNLICH DARUM**



Bez.Dir. Wolfgang LOIDOLT  
Tel.: 050 350 90-21784  
Fax: 050 350 99-21784  
E-Mail: w.loidolt@staetdtische.co.at

**BUNDESHEERBETREUUNG FÜR SOLDAT/INNEN UND IHRE FAMILIEN**

**VERSICHERUNGSSPEZIALISTEN FÜR AUSLANDSEINSÄTZE**

### TEAM LOIDOLT

Wiener Städtische Versicherung AG  
1210 Wien, Am Spitz 10  
(Eingang Schwaigergasse)

wienerstaetdtische.at  
f/wienerstaetdtische

**WIENER  
STÄDTISCHE**  
VIENNA INSURANCE GROUP

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. Hochvernetzte 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.
- 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.

- 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 sollen 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 denn je! ❌

