In den bisherigen Beiträgen zum Thema „Blackout“ erfolgte eine intensive Auseinandersetzung mit einer komplexen Schadenslage. Dieses Szenario ist nicht das Einzige dieser Kategorie. Verschiedene Analysen gehen davon aus, dass die Gesellschaft in Zukunft häufiger mit völlig unerwarteten und überregionalen Großschadenslagen konfrontiert werden wird. Daher ist eine umfassendere Betrachtung der Umfeldbedingungen erforderlich, um die Gesamttragweite, auch für das nationale Krisenmanagement, erfassen zu können.

Niemand würde freiwillig mit dem Auto vorwärts fahren, indem er dabei ausschließlich in den Rückspiegel blickt, um zu sehen, wie erfolgreich die bisherige Strecke bewältigt wurde, wenn sich dabei die Umfeldbedingungen ändern. Eine derartige Vorgangsweise ist aber in anderen Lebenssituationen durchaus gebräuchlich. Hierbei erfolgen die Orientierung am bisherigen Erfolg und eine lineare Projektion der Vergangenheit in die Zukunft. Diese lineare Fortschreibung führt auch dazu, dass Menschen Daten und Informationen falsch interpretieren und dabei mögliche Fehlentwicklungen zu spät erkennen. Dies lässt sich gut mit zyklischen Veränderungen in der Natur, etwa an den Jahreszeiten, beschreiben. Eine Wärmeperiode im Frühling oder im Herbst weist dieselben Daten auf. Einmal ist jedoch eine generelle Temperatursteigerung und im anderen Fall eine Temperatursenkung zu erwarten. Werden die sonstigen Rahmenbedingen nicht mitberücksichtigt, kommt es zu Fehlentscheidungen.

Systembetrachtung

Ganz wesentlich in einer Problembetrachtung ist die Herangehensweise. Zur leichteren Nachvollziehbarkeit dient

Foto: Schleinzer/Montage: Rizzardi

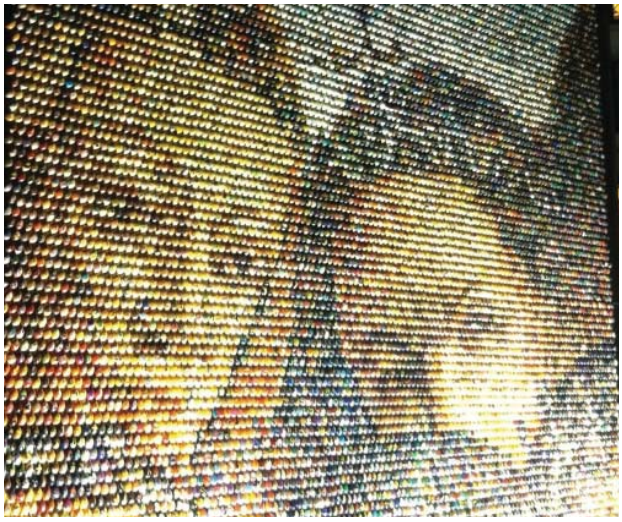
folgender Vergleich: Werden bemalte Ostereier auf einem Bild betrachtet, so ergeben sich eine Reihe von Fragen. Welche Farben wurden verwendet? Welche chemische Zusammensetzung haben diese? Was hat sich der Künstler bei den Motiven gedacht? Welche Rolle spielt die Anordnung? Und noch einige mehr. Das Ergebnis ist eine Menge von Daten und Informationen. Dieser Ansatz ist weit verbreitet und wird vor allem durch die Möglichkeiten der Informations- und Kommunikationstechnik gefördert. Die Zunahme der Datenflut führt aber selten zu einem besseren Gesamtbild. Der zweite Ansatz ist eine Systembetrachtung. Nimmt man etwas Abstand und geht ein paar Schritte zurück, so ergibt sich plötzlich ein Bild. Die Gesamtzusammenhänge werden ersichtlich und begreifbar, die bei der Detailbetrachtung verborgen geblieben sind. Nicht die Details, also die Datenmenge, sondern der Überblick, das „Bild“, hat zum Erfolg geführt. Dieser Ansatz ist auch für die Betrachtung von komplexen Schadenslagen und des nationalen Krisenmanagements erforderlich.

Der Überblick führt zum Erfolg.

Netzwerkgesellschaft

Seit einigen Jahren etabliert sich der Begriff „Netzwerkgesellschaft“ für eine neue Gesellschaftsform, die neben den bisherigen - der „Agrar-“ und der „Indus-

Autor: Major Herbert Saurugg, Jahrgang 1974, Militärrealgymnasium, Theresianische Militärakademie - Jahrgang Ritter von Trapp, Verwendungen im Bereich Führungsunterstützung und IKT-Sicherheit, Auslandsverwendung bei ATHUM/ALBA (1999), KFOR (2000), Junior Projektmanager (PMA), Akademischer Sicherheitsexperte für IKT (FH-Hagenberg), Krisen- und Notfallmanager, BdSI, Masterstudium an der Hochschule für Management Budapest, Mitglied von Cyber Security Austria.



Fotos: Saurugg

Systembetrachtung: Nimmt man etwas Abstand und geht ein paar Schritte zurück, so ergibt sich ein Bild.

triegesellschaft“ - entsteht. Bisher wurden auch die Begriffe „Informations-“ oder „Wissensgesellschaft“ für diese Entwicklung verwendet. Das „Netzwerk“ symbolisiert dabei die bestimmende Organisationsform einer sich verändernden Gesellschaft. Die Vernetzung mit Informations- und Kommunikationstechnik (IKT) und damit einhergehend die elektronische Kommunikation, spielen dabei eine zentrale Rolle.

Bei der Netzwerkgesellschaft handelt es sich um kein temporäres Phänomen, sondern sie beschreibt einen fundamentalen gesellschaftlichen Wandel, ab der Mitte des letzten Jahrhunderts durch die Entwicklung von Computern ausgelöst wurde. Die Netzwerkgesellschaft ist u. a. durch Personalisierung und Individualisierung, Vielfältigkeit, Asynchronität, Dezentralisierung und Miniaturisierung, aber auch durch Transparenz, Partizipation und Zusammenarbeit gekennzeichnet. Hierzu gibt es zahlreiche Beispiele, die laufend mehr werden. Ob dies die dezentrale Energieversorgung, die Nanotechnologie, die Produktwahlmöglichkeiten, das Mit-mach-Web 2.0 oder den immer größer werdenden Dienstleistungssektor betrifft, wir sind täglich mit neuen Entwicklungen der Netzwerkgesellschaft konfrontiert.

Die entstehende Netzwerkgesellschaft erfordert auch neue Spielregeln für das Zusammenleben. Transparenz, Partizipation und Kollaboration spielen dabei eine wichtige Rolle, um mit der von Menschen geschaffenen Komplexität erfolgreich und nachhaltig umgehen zu können. Diese Veränderungen führen ebenso zu innergesellschaftlichen Konflikten, prallen doch dadurch auch verschiedene Weltsichten aufeinander.

Komplexe Systeme

Diese fundamentalen gesellschaftlichen Veränderungen werden durch eine massive technische Vernetzung ermöglicht, die nicht nur zu positiven Effekten führt. So entstehen etwa kom-

Nationales Krisenmanagement

Unter „nationales“ wird in diesem Artikel die Gesamtheit aller Akteure - von der organisierten Hilfe, über die Behörden, die Wirtschaft bis hin zur Bevölkerung - in einem Staat verstanden.
Derzeit deckt in Österreich das „Staatliche Krisen- und Katastrophenschutzmanagement“ (SKKM) den „Bevölkerungs-“ bzw. „Zivilschutz“ ab. Die Analysen des Autors im Rahmen des Masterstudiums führten zur Erkenntnis, dass sich die vorhandenen nationalen Strukturen und Vorbereitungen zur Bewältigung von Krisen immer weniger mit neuen Anforderungen durch die sich immer rascher ändernden Umfeldbedingungen sowie den zu erwartenden komplexen Schadenslagen decken. Dies betrifft weniger die operativen Bewältigungsebenen (Gemeinde - Bezirk - Bundesland), als viel mehr die nationale Koordinierung von präventiven und vorbereitenden Maßnahmen und insbesondere die Steigerung der gesamtgesellschaftlichen Widerstandsfähigkeit („Resilienz“). Diese muss vor allem durch eine aktive Systemgestaltung erreicht werden.
Der Begriff „Krise“ bezeichnet ein außergewöhnliches Ereignis, das nicht mit den vorbereiteten Abläufen und Strukturen bewältigbar ist und hohe Schäden verursachen kann. Als „Krisenmanagement“ werden generelle Vorbereitungen auf außergewöhnliche Ereignisse bezeichnet, die zu einer möglichst raschen Wiederherstellung des Normalzustandes beitragen sollen. Krisenmanagement bedeutet dabei nicht nur die akute Begegnung einer Krise, sondern inkludiert auch alle Maßnahmen zur Vermeidung (Vorsorge und Prävention), Erkennung und Bewältigung sowie Nachbereitung von Krisen.
Eine Krise im Verantwortungsbereich der öffentlichen Hand kann durch eine befugte Behörde zur Katastrophe erklärt werden. Dadurch werden verschiedene temporäre rechtliche Rahmenbedingungen in Kraft gesetzt.

plexe Systeme, die sich durch Nichtlinearität und ständige Rückkoppelungen auszeichnen, welche den weiteren Prozessverlauf beeinflussen. Eingriffe wirken sich häufig zeitverzögert aus, was leicht zur Übersteuerung führt. Indirekte Wirkungen verhindern eine Ursachenzuordnung.

Die Lösung eines Problems führt daher zur Schaffung von mehreren neuen und auch zeitverzögerten Problemen. Erschwerend kommen exponentielle Entwicklungen hinzu, die für Menschen oft schwer erfassbar sind. Noch weitreichender wirkt sich die unkontrollierte Vernetzung über Systemgrenzen hinaus aus. Diese kommt einem medizinischen Krebsgeschwür gleich. Ein solcher Krebs ist auch während der Wachstumsphase sehr erfolgreich - bis zu dem Zeitpunkt, wo er seinen Wirt überfordert und de facto Selbstmord begeht.

Fehler im System

In der Natur bewähren sich nur Systeme, wo sich ein Fehler im Subsystem nicht automatisch auf das ganze System negativ auswirken kann. Diesem Grundsatz wird in unserer technischen Welt vielfach widersprochen, ob dies beim Internet ist, wo sich Schadsoftware in wenigen Minuten über die ganze Welt ausbreiten kann, oder im Bereich der Stromversorgung, wo es heute riesige Netzbereiche gibt.

Wie fatal sich das auswirken kann, hat Ende Juli 2012 eine Serie von Blackouts in Indien gezeigt, wo gleichzeitig bis zu 700 Millionen Menschen betroffen waren. Offenbar handelte es sich dabei um ein einfaches Systemversagen durch Überlastung, da die Versorgung relativ rasch wiederhergestellt werden konnte. Denkt man einen Schritt weiter und stellt sich ein Szenario vor, wo ein solches Systemversagen durch eine Schadsoftware ausgelöst wird, wie dies etwa bei der Schadsoftware „STUXNET“ der Fall war (siehe TD - Heft 2/2011), dann könnte das eine ganze Gesellschaft innerhalb kürzester Zeit in mittelalterliche Verhältnisse zurückkatapultieren.

Mittlerweile steigt unter IKT-Sicherheitsfachleuten die Sorge, dass sich die Schadsoftwareentwicklung verselbstständigen und genau zu solchen Schreckensszenarien führen könnte. Es handelt sich hierbei um keine theoretischen Annahmen mehr. Eine solche Fehlentwicklung könnte jederzeit Realität werden!

Im Jahr 2011 wurde eine nicht repräsentative Umfrage der Sicherheitsfirma McAfee bei deutschen Energieversorgungsunternehmen durchgeführt. Demnach gaben 59 Prozent der befragten Unternehmen an, dass sie die Schadsoftware „STUXNET“ auf ihren Systemen gefunden haben. Diese Schadsoftware war zwar für diese befallenen Systeme ohne Folgen, zeigt aber die Verwundbarkeit der Betreiber von Kritischer Infrastruktur auf. Auch hier lassen sich Parallelen zur Natur ableiten. Die steigende Pandemiegefahr basiert besonders auf der enormen Reisetätigkeit der Menschen, dem globalen Warenhandel und dem engen Zusammenleben von Mensch und Tier bzw. durch die dadurch entstehende „Vernetzung“.

Wachstum in s-förmigen Kurven

In den vergangenen zwei Jahrzehnten wurden in vielen Bereichen Vernetzungen und Abhängigkeiten geschaffen, die kaum bewusst sind. Hinsichtlich der Stromversorgung wurde dies in der bisherigen Artikelserie bereits ausführlich analysiert. In der Natur gibt es Wachstum nur in s-förmigen Kurven. Sie stellt das Grundmuster eines gesunden und natürlichen Wachstums dar. Dieses verläuft zu Beginn langsam, beschleunigt sich nach einer bestimmten Zeit exponentiell, erreicht einen Wendepunkt und flacht dann wieder ab, bis ein Sättigungsniveau erreicht wird. Diese Entwicklung hängt mit den Umfeldbedingungen zusammen. Die Sättigungsgrenze kann etwa durch Nahrungs- oder Platzmangel erreicht werden - das System reguliert sich selbst. Damit eine Weiterentwicklung möglich ist, muss bis zum kritischen Wendepunkt eine neue Entwicklung angestoßen werden, die wiederum in einer s-förmigen Kurve verläuft. Dieses Verhalten ist auch im Technologiebereich zu beobachten. Beispielsweise stellt die Mobiltelefontechnologie die Weiterentwicklung der analogen Telefontechnik dar, die nun wiederum durch Smartphones abgelöst wird. Allen diesen Entwicklungen ist gemein, dass ihre Dynamik und Geschwindigkeit steigen, was sich wiederum auch auf das gesamtgesellschaftliche Leben und damit auch auf das nationale Krisenmanagement auswirkt.

Kritischer Wendepunkt

Eine exponentielle Wachstumsphase ist grundsätzlich stabil. Daher neigen Menschen in dieser Phase zu einer linearen und zur fatalen Fehlinterpretation. Der für einen Neubeginn entscheidende, „kritische“ Wendepunkt wird versäumt. Die Folge ist ein unvermeidbarer Kollaps. Aktuell gibt es einige Beispiele aus dem Technologiebereich, wie etwa bei Nokia oder RIM (Blackberry), wo scheinbar

Komplexe Schadenslage

Eine „komplexe Schadenslage“ beschreibt ein außergewöhnliches Ereignis, das einerseits sehr selten vorkommt, das bisher Erlebte jedoch bei weitem übersteigen und das Potenzial aufweisen kann, das tägliche Leben zumindest lokal massiv zu verändern. Dabei sind hohe menschliche Verluste oder Zerstörungen möglich. Darunter fallen vor allem überregionale Ereignisse, wie etwa ein Blackout, ein großräumiger Ausfall des Sektors Informations- und Kommunikationstechnik oder eine Pandemie. Aber auch ein schwerer Kernkraftwerksunfall in Mitteleuropa würde zu einer komplexen Schadenslage führen, wenngleich dabei andere zeitliche Rahmenbedingungen zum Tragen kommen. Für die Bewältigung einer komplexen Schadenslage ist eine überregionale Zusammenarbeit erforderlich. Die Ressourcen der organisierten Hilfe reichen nicht aus.

der kritische Wendepunkt versäumt wurde und ein Crash bereits kolportiert wird.

Krisen

Viele aktuelle und globale Krisen, wie etwa die Finanz-, Wirtschafts-, Staatsschulden- oder Energiekrise, der Klimawandel oder die Bevölkerungsexplosion, basieren auf den bisherigen Denkweisen aus dem Industriezeitalter und einer linearen Fortschreibung der Vergangenheit („Rückspiegeleffekt“).

Die bisherigen Lösungskompetenzen und -wege sind immer weniger dazu geeignet, die anstehenden Probleme zu lösen. Dies liegt auch daran, dass hier die Einflüsse der Netzwerkgesellschaft - wie etwa durch die Vernetzung - eine wichtige Rolle spielen, aber noch zu wenig berücksichtigt werden. Beispielsweise ist die bisher übliche Organisationsform der Hierarchie immer weniger in der Lage, mit den Anforderungen der Netzwerkgesellschaft und damit einhergehend mit der immer komplexer, vernetzter und dynamischer werdenden Welt Schritt zu halten. Zur Verdeutlichung dient auch die Gegenüberstellung einzelner Parameter in der Grafik unten.

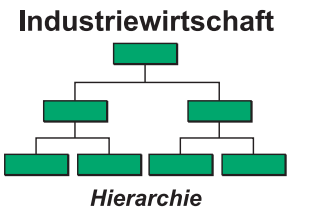
Eine zentrale Ursache für viele Fehlentwicklungen ist auch in der seit den 1990er Jahren verfolgten kurzsichtigen Gewinnmaximierung zu suchen. Durch die Missachtung einer langfristigen und nachhaltigen Planung wird die Überlebensfähigkeit von Organisationen und Systemen aufs Spiel gesetzt.

Vernetztes Denken

Um die steigende Komplexität bewältigen zu können, ist vernetztes und systemisches Denken unverzichtbar. Niemand ist heute in der Lage, alle Aspekte eines vernetzten Systems zu erfassen. Daher ist es notwendig, möglichst viele Aspekte durch unterschiedliche Betrachtungswinkel zu erfassen. Hier schafft die Netzwerkgesellschaft völlig neue Möglichkeiten. Das neu entwickelte „Mit-mach-Web 2.0“ ermöglicht etwa eine völlig unbürokratische und sehr flexible sowie transparente und auf Basis von Partizipation und Kollaboration durchführbare Zusammenarbeit (Stichwort: „Schwarmintelligenz“). Damit können Ergebnisse geschaffen werden, die vor wenigen Jahren noch völlig undenkbar waren. So wurden etwa innerhalb kürzester Zeit, langjährig bewährte Lexika weitgehend durch die Online-Enzyklopädie Wikipedia verdrängt, die auf diesen Grundprinzipien erstellt und gewartet wird. Ein anderes Beispiel sind Crisis-Mapping-Projekte wie Ushahidi, mit denen heute innerhalb kürzester Zeit und ohne zentrale Steuerung ein Lagebild in Krisen- und Katastrophenregionen geschaffen wird. Vernetztes Denken und Handeln ist aber nicht nur auf technischer Basis relevant. In vielen Bereichen sind Low-Tech- und No-Tech-Lösungen gefordert. Technik kann zwar oftmals unterstützen, aber die zentrale Rolle werden auch weiterhin Menschen spielen. Daher ist eine verstärkte zwischenmenschliche und organisationsübergreifende Vernetzung erforderlich, um vielfältige und komplexe Probleme nachhaltig lösen zu können. Vernetztes Denken ist keine isolierte Fähigkeit, sondern im Großen und Ganzen die Überschreitung von künstlich geschaffenen (Denk-)Grenzen und der Einsatz eines „gesunden Hausverstandes“.

Eine wesentliche Hürde stellt dabei unser bisheriges Ausbildungssystem dar, das im Wesentlichen nach wie vor auf die Anforderungen der Industriegesellschaft ausgerichtet ist. Dabei werden Sachverhalte relativ isoliert betrachtet, was sich etwa in der Klassifizierung von Wissenschaftsdisziplinen niederschlägt. So erweist sich die Klassifizierung des Themas „(IKT-)Sicherheit“ als Spezialfach zunehmend als Sackgasse. Sicherheit ist ein Querschnittthema und muss von allen Akteuren verstanden und berücksichtigt werden. Aber auch die klassische Aufteilung in Innere und Äußere Sicherheit spiegelt dieses alte Klassifizierungsschema wieder, das immer weniger den aktuellen Herausforderungen entspricht. Daher sind auch Querschnittprobleme, wie etwa aus dem Cyberspace, nicht mehr mit dieser „Silo-Kategorisierung“ zu lösen.

Um die erforderlichen Dimensionen von vernetztem Denken bei komplexen Schadenslagen zu verdeutlichen, dient folgendes Beispiel: Bei einem Stromausfall in einer Kläranlage kippt nach rund 24 Stunden das äußerst wichtige biologische Bakteriensystem. Betrifft dies eine Anlage, ist ein temporärer Ausfall für die Umwelt verkraftbar bzw. können erforderliche Ersatzmaßnahmen getroffen werden. Betrifft dies aber eine ganze Region oder hunderte Kläranlagen, dann sieht die Situation völlig anders aus: einerseits, was die Umweltverträglichkeit und andererseits, was die Verfügbarkeit von Knowhow und Ressourcen (z. B. Bakterienkulturen) zum Wiederaufbau des biologischen Systems und damit der Kläranlagen betrifft. Derartige Betrachtungen sind aber beim Thema „Blackout“ zwingend erforder-



	Industriewirtschaft	Informationswirtschaft
	Hierarchie	*Vernetzung*
Hierarchiestufen	viele	wenige
Arbeitsteilung	weitreichend	gering
Mitarbeiterstellung	austauschbar, gehorsam, angepasst	engagiert, loyal, informiert, selbstständig
Vernetzung	gering	hoch
Arbeitsabläufe	streng geregelt, starre Zuständigkeiten	flexibel, ad-hoc; Projektorganis. auf Zeit
Einfluss/Macht	abhängig von Hierarchieebene	abhängig von Wissen und Können
Mitwirkungsumfang	gering	groß
Organis. Ausrichtung	betriebswirtschaftlich	Eigeninteresse, Betrieb & Gemeinschaft
Wichtigstes Ziel	Outputmaximierung	Nutzenoptimierung

Grafik: Ind-WiGesellschaft - Weiber Rolf

Gegenüberstellung einzelner Parameter zwischen Industrie- und Informationswirtschaft.

Die Großkläranlage der Stadt Wien in Simmering.

lich, um festzustellen, ob es vielleicht einfache Möglichkeiten gibt, das Worstcase-Szenario - den Ausfall von vielen Kläranlagen über einen längeren Zeitraum - zu verhindern. Hier wäre auch die Frage zu stellen, wer für eine solche übergeordnete Betrachtung zuständig ist. Derzeit gibt es dazu in Österreich keine Strukturen oder Prozesse.

Im Bereich des österreichischen Staatlichen Krisen- und Katastrophenschutzmanagementes (SKKM) ist vernetztes Denken durchaus vorhanden, wie auch die Aktivitäten in einigen Bundesländern erkennen lassen. Einen wesentlichen Beitrag dürfte hierzu die in den vergangenen Jahren durchgeführte Vereinheitlichung der Führungsstrukturen und -prozesse geleistet haben. Verbesserungspotenzial besteht jedoch besonders bei der Vernetzung auf nationaler behördlicher und internationaler Ebene sowie zu den Betreibern von Kritischer Infrastruktur. Als ein positives Beispiel im Bereich der strategischen Informationsinfrastruktur kann die Vernetzung über den Austrian Trust Circle (ATC) angeführt werden. Diese Vernetzung soll vor allem bei der Behebung von Sicherheitsproblemen in den jeweiligen Infrastruktursektoren unterstützen und eine Vertrauensbasis schaffen, um im Ernstfall gemeinsam agieren zu können.

Die Initiative wurde durch das nationale Computer Emergency Response Team Austria (CERT.at) mit dem Bundeskanzleramt (BKA) gestartet. Als weiteres positives Beispiel ist der CERT-Verbund Österreich anzuführen, wo ebenfalls eine solche Vernetzung zur Vertrauensbildung initiiert wurde. Diese Vernetzung darf sich aber nicht allein auf einzelne Bereiche oder Sektoren beschränken.

Systemgestaltung

Wie sich am Beispielszenario Blackout zeigt, bedeuten komplexe Schadenslagen eine völlige Überforderung der derzeit für die Krisenhilfe vorgesehenen Hilfsstrukturen. Daher ist eine aktive Einbindung der Bevölkerung, insbesondere durch die Stärkung der Selbsthilfefähigkeit (siehe TD Heft 4/2012) und die Erhöhung der gesamtgesellschaftlichen Resilienz, unverzichtbar. Dabei zeichnet sich immer stärker ab, dass diese zukünftigen Herausforderungen nur durch eine entsprechende proaktive Systemgestaltung zu bewerkstelligen sein werden. Diese muss auf vielen Ebenen erfolgen: beginnend von der technischen, wo die unkontrollierte Fehlerausbreitung verhindert werden muss, bis über die gesellschaftliche Ebene, wo die Krisenprävention und -reaktion nicht auf einzelne Akteure beschränkt sein darf, sondern eine umfassende Einbindung aller möglicherweise betroffenen Akteure erforderlich ist. Hierzu sind auch komplett neue Lösungsansätze erforderlich. Vor allem ist es notwendig, das bisher noch weit verbreitete „Klassifizierungsdenken“ zu überwinden und vernetzt zu denken.

Von der Natur abschauen

In der Natur gibt es nur komplexe Systeme, die keine zentrale Steuerung oder Planung aufweisen. Diese Selbstregula-

Crisis-Mapping - Ushahidi

Ushahidi (http://ushahidi.com) ist eine freie Software (Open-Source-Plattform), die zur Dokumentation von Wahlbetrug, Umweltvergehen oder Menschenrechtsverstößen, aber auch bei Katastrophen wie etwa beim Erdbeben in Haiti oder Japan, mittlerweile weltweit zum Einsatz kam. Durch die offene Einbindung der Bevölkerung und Visualisierung entsteht sehr rasch ein öffentliches Lagebild. Wie sich auf Haiti gezeigt hat, führte dies auch zu einer kybernetischen Selbstorganisation. Das für die Hilfsorganisationen erforderliche Kartenmaterial war zum Zeitpunkt der Katastrophe völlig veraltet. Es fanden sich aber via Internet innerhalb kürzester Zeit genug Freiwillige, die verfügbare Satellitenbilder und sonstiges Kartenmaterial digitalisierten und somit die Arbeit der Hilfsorganisationen wesentlich erleichterten.

tion hat sich über Milliarden von Jahren bewährt, natürlich auch dadurch, dass sich Systeme an die sich laufend verändernden Umfeldbedingungen angepasst haben oder verschwunden sind. Von der Natur können daher viele praktische Erkenntnisse, sowohl was die Systemgestaltung als auch das Krisenmanagement betrifft, gewonnen werden. Eine Wissenschaft, die sich damit sehr intensiv auseinandersetzt, ist die Kybernetik, die Wissenschaft von der Regelung/Lenkung/Steuerung und Kommunikation in Lebewesen und Maschinen, oder vereinfacht ausgedrückt - die Steuerung von komplexen Systemen. Durch ihre Erkenntnisse war es erst möglich, Computer zu bauen. Sie hat den Anstoß für die Netzwerkgesellschaft geliefert und kann daher auch zur Entwicklung von neuen Lösungskompetenzen beitragen.

Energiebedarfssenkung

Eine solche Erkenntnis aus der Kybernetik bzw. aus der Natur lautet, dass sich in der Natur bisher nur Systeme durchsetzen konnten, die in der Lage waren, ihren Energieverbrauch durch evolutionäre Weiterentwicklungen zu senken. Diese Energieverbrauchssenkung, die sich bereits in wenigen Jahren massiv auf die „energiehungrigen" Gesellschaften auswirken könnte, ist vor allem in Anbetracht des Rückganges von billigen fossilen Energieträgern (Stichwort „Peak Oil") eine enorme Herausforderung. Daher greifen die derzeitigen Debatten um die Energiewende weitgehend zu kurz. Es geht nicht nur um die Umstellung der Energieversorgung auf erneuerbare Energieträger, sondern um eine völlige Neuausrichtung der Energieversorgung und des Energieverbrauchs. Die absehbaren Energiepreissteigerungen werden sich deutlich auf die Entwicklung der Volkswirtschaften auswirken und bergen enormes Potenzial für gesellschaftliche Umbrüche, die wiederum auch das nationale Krisenmanagement betreffen werden. Daher ist es umso wichtiger, dass das nationale Krisenmanagement nicht nur reaktiv tätig wird, sondern bereits aktiv bei der „Spielregelgestaltung" mitwirkt und sich mit Themen auseinandersetzt, die noch gar nicht aktuell sind.

Nationales Kompetenzzentrum

Um die erforderliche nationale Vernetzung zu verbessern, eine nationale und organisationsübergreifende Risikobeurteilung aufzubauen oder aktiv bei Systemgestaltungen mitwirken zu können, sind entsprechende neue Strukturen erforderlich, die sich in Österreich bisher noch nicht gebildet haben. Ein nationales Kompetenzzentrum für Bevölkerungs- und Zivilschutz könnte die vorhandenen Ressourcen vernetzen und bündeln und die bisherige „Silo-Klassifizierung" überwinden. Keinesfalls dürfen damit neue Parallelstrukturen geschaffen werden.

Dieses Kompetenzzentrum sollte auch eine Wissens-Drehscheibe darstellen. Der österreichische Staat gibt viel Geld für die Sicherheitsforschung aus. Die Erkenntnisse daraus könnten durch eine klar verantwortliche und mit Querschnittthemen beauftragte Stelle gezielter auf operativer Basis zur Umsetzung gebracht werden. Dabei ist die übergreifende Koordinierung und Begleitung auch außerhalb des Forschungsbereiches in den Vordergrund zu stellen.

Eine weitere wichtige Aufgabe wäre der Aufbau bzw. die Koordinierung eines gesamtheitlich und gesamtstaatlich ausgerichteten Risikomanagementes, was etwa für die Einführung von intelligenten Stromzählern dringend notwendig gewesen wäre. Gegenwärtig gibt es keine klar verantwortliche Stelle, die das Thema Systemsicherheit umfassend und organisationsübergreifend betrachtet und auch entsprechend in die Umsetzungsplanungen einbringt. Dieser Schritt ist vor allem proaktiv erforderlich, um frühzeitig Fehlentwicklungen entgegenwirken zu können. Aktives Krisenmanagement muss sich bereits in der Entwicklungs- und Planungsphase von großen Neuentwicklungen einbinden („Systemgestaltung") und beurteilen, ob das erwartbare gesamtgesellschaftliche Restrisiko durch ein Krisenmanagement überhaupt bewältigbar ist. Andernfalls muss hier frühzeitig entgegengesteuert werden. Dies verdeutlicht auch die Notwendigkeit eines gesamtheitlichen und nicht nur reaktiven Krisenmanagementes.

Eine andere Aufgabe wäre die Unterstützung bei der Vereinheitlichung und Qualitätssicherung der Ausbildung für die regionalen Krisenmanager, aber auch bei den Hilfsorganisationen und bei den Betreibern von kritischer Infrastruktur. Dieser Schritt ist vor allem für eine überregionale Zusammenarbeit bei komplexen Schadenslagen unverzichtbar. Es gibt hierzu zwar einzelne Ausbildungsmodule durch das Staatliche Krisen- und Katastrophenschutzmanagement, wie etwa „Rechtliche und Organisatorische Grundlagen" oder „Führen im Katastropheneinsatz". Weitere Angebote für „Risiko- und Krisenkommunikation" sowie „Risikoanalyse und Katastrophenschutzplanung" befinden sich in Ausarbeitung. Diese Module erreichen

aber nicht alle relevanten Akteure. Direkt damit verbunden ist auch eine Qualitätssicherung der regionalen Vorbereitungsmaßnahmen. Hier geht es nicht um lokale Kompetenzeingriffe, sondern um die Schaffung und Definition von gemeinsamen Qualitätsstandards. Nur so kann gewährleistet werden, dass alle vom Selben sprechen und im Anlassfall die gleiche Leistung von den anderen erwarten können.

Ein nationales Kompetenzzentrum sollte auch die Moderationsrolle zwischen den verschiedenen Akteuren einnehmen. Nur so können rasch Lösungen auch bereits vor einer Krise erzielt werden, was gerade bei der Vorbereitung auf komplexe Schadenslagen mit ihrer sehr hohen Dynamik unverzichtbar ist.

In Deutschland gibt es etwa das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) oder in der Schweiz das Bundesamt für Bevölkerungsschutz (BABS). Auch in anderen Ländern gibt es Kompetenzzentren für das nationale Krisenmanagement. Dabei kann grundsätzlich zwischen zwei Ansätzen unterschieden werden:

Der prozessorientierte „Interagency"-Ansatz, bei dem ein der Regierung nahestehendes und entsprechend in der Hierarchie verankertes Organ die Bestrebungen der involvierten Behörden koordiniert und der institutionelle Ansatz der „Homeland"-Security, bei dem zahlreiche Institutionen in einer einzigen Behörde mit Befehlsgewalt vereinigt sind.

In Österreich existiert der prozessorientierte Ansatz, der aber aufgrund verfassungsmäßiger Einschränkungen (Subsidiaritätsprinzip; siehe TD - Heft 4/2012), der steigenden Dynamik und der neuen Herausforderungen immer häufiger nur reaktiv zur Wirkung kommt, was bei komplexen Schadenslagen zu kurz greift.

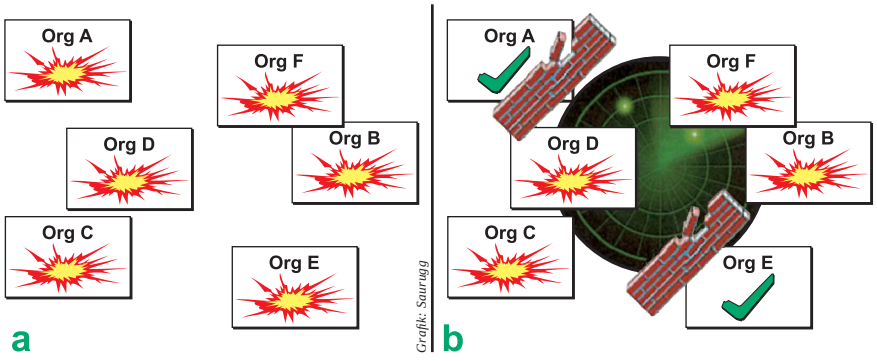
Nationales Lagebild

Das Einsatz- und Krisenkoordinierungscenter (EKC) des Österreichischen Innenministeriums erstellt gemeinsam mit der Bundeswarnzentrale (BWZ) ein permanent aktuelles Lagebild zur Sicherheit in Österreich. Mitte 2012 wurde durch das Österreichische Bundeskanzleramt eine nationale IKT-Sicherheitsstrategie vorgestellt. Darauf aufbauend wird bis Ende 2012 auf breiter Zusammenarbeit eine nationale Cyber-Sicherheitsstrategie erarbeitet. Als eine zentrale Notwendigkeit wurde bereits in der IKT-Sicherheitsstrategie die Etablierung eines nationalen Cyber-Lagezentrums identifiziert.

Eine große Herausforderung wird dabei die Vernetzung der bisherigen und zukünftigen Lagezentren darstellen, da nur so ein gemeinsames Lagebild entstehen kann. Hier sollte auch auf die Erfahrungen der bisherigen Harmonisierung im Bereich des Staatlichen Krisen- und Katastrophenschutzmanagementes, etwa durch die Vereinheitlichung der Stabsgliederung und Stabsarbeit, zurückgegriffen werden.

Eine noch wesentlich höhere Hürde stellen der zeitnahe Informationsaustausch und die Kommunikation mit den Betreibern von Kritischen Infrastrukturen (CI) dar. Derzeit gibt es etwa auf nationaler Ebene keine klaren und einheitlichen rechtlichen Vorgaben für die Zusammenarbeit zwischen den Betreibern von CI und dem Staatlichen Krisen- und Katastrophenschutzmanagement. Es gibt jedoch etwa eine EU-Richtlinie zur Fernmeldegesetzgebung, die eine Vorfallberichterstattung für den Telekommunikationssektor vorsieht (Sicherheit und Integrität „Artikel 13a" EU-Direktive 2009/140/EC).

Durch die hohe und weiter steigende technische Vernetzung steigen auch die gegenseitigen Abhängigkeiten. Daher wird für die Krisenprävention und vor allem für eine rasche Krisenreaktion eine enge Kooperation mit den CI-Betreibern immer bedeutender. Dies umso mehr, als mit der technischen Vernetzung und Abhängigkeit (Komplexität), etwa bei einem Strom- oder IKT-Ausfall, eine sehr rasche Eskalation erfolgt. Zur leichteren Nachvollziehbarkeit dient das in der Grafik unten dargestellte vereinfachte Beispiel. Im Szenario (siehe Grafik a) sind alle Organisationen von einem Vorfall betroffen. Aufgrund des fehlenden Lagebildes werden die Ausfälle erst bei entsprechenden Abhängigkeiten, hier durch die Distanz der Organisationen zueinander, dargestellt bzw. zeitverzögert etwa über Medienberichte, für die anderen Organisationen wahrnehmbar. Dadurch ist ein präventiver Schutz von noch nicht betroffenen Organisationen kaum möglich. Im Szenario (siehe Grafik b) gibt es eine Früherkennung durch ein Lagebild. Dadurch kann eine frühzeitige Intervention die Ausbreitung auf alle Organisationen verhindern, wie beispielsweise die Ausbreitung einer Schadsoftware und damit verbunden ein Ausfall von Infrastruktur. Dies bezieht sich auf Systeme, die nicht direkt mit dem Internet verbunden sind und wodurch eine Ausbreitung unter Umständen noch rechtzeitig gestoppt werden kann, wie etwa derzeit noch häufig in der Industrieanlagensteuerung. Eine Ausbreitung von Schadsoftware im Internet ist de facto nicht zu stoppen, da innerhalb von wenigen Minuten eine weltweite Verbreitung möglich ist. Daher spielt eine entsprechende Systemgestaltung in der Krisenprävention eine zentrale Rolle.



Fehlt das Lagebild, ist der präventive Schutz noch nicht betroffener Organisationen kaum möglich.

Resilienz

Resilienz bezeichnet die Fähigkeit eines Systems, trotz externer Einflüsse stabil zu bleiben bzw. bei Störungen möglichst rasch den Normalzustand wiederherzustellen (Regenerationsfähigkeit). Synonym werden die Begriffe „Widerstandsfähigkeit“ oder „Robustheit“ verwendet.

Um dieses Lagebild zu erhalten, ist eine Schnittstelle zwischen dem Krisenmanagement der Organisationen und dem staatlichen Krisenmanagement erforderlich, die nicht erst im Krisenfall aktiviert wird, sondern permanent zur Verfügung steht. Komplexe Schadenslagen entwickeln sich weitgehend überraschend.

Zur bisherigen Notfall- und Krisenorganisation sind daher zwei wesentliche Erweiterungen erforderlich. Aus der gesamtstaatlichen Sicht besteht die Notwendigkeit einer Trennung zwischen Betreibern von nicht-kritischen und kritischen Infrastrukturen. Der Status der ersten Gruppe ist möglicherweise im Krisenfall für das nationale Krisenmanagement relevant.

Der Status der zweiten Gruppe (CI) ist auch bereits dann für das nationale Krisenmanagement relevant, wenn die Krisenbewältigung noch innerhalb der Organisation möglich ist oder scheint. Denn kommt es zu einer weiteren Eskalation oder befinden sich mehrere Organisationen parallel in einer Krisenlage, kann durch ein übergeordnetes systemisches Lagebild frühzeitig reagiert und gegengesteuert werden.

Dieses nationale Lagebild darf sich aber nicht nur auf aktuelle Ereignisse beschränken, sondern muss auch ein Bild über Abhängigkeiten und Vernetzungen zur Verfügung haben, um jederzeit Wenn-Dann-Fragen beantworten zu können. Nur so kann es gelingen, vorausschauend Fehlentwicklungen zu erkennen und rechtzeitig und nachhaltig entgegenzusteuern.

Besonders wichtig erscheint der systemische Ansatz - die Betrachtung eines Problems aus der Distanz. Es geht nicht darum, einen möglichst hohen technischen Vernetzungsgrad zu erzielen und viele Daten zu sammeln, sondern um die wichtigen Eckpunkte, die zur Erkennung eines Gesamtbildes notwendig sind. Daher ist vor allem eine zwischenmenschliche und auf gegenseitigem Vertrauen basierende Vernetzung zu schaffen. Dadurch ergibt sich automatisch ein anlassbezogener und sachbezogener „Filter“ beim Informationsfluss. In letzter Konsequenz bedeutet das den Ausbau des klassischen Verbindungswesens, da eine nichttechnische Vernetzung mit den Betreibern von kritischen Infrastrukturen im Vordergrund stehen sollte. Der derzeit bereits mehrfach angedachte Weg - die Betreiber melden Daten an eine zentrale Stelle, ohne zu wissen, was dann mit diesen passiert - etwa durch die EU-Direktive 2009/140/EC, Artikel 13a, die eine Vorfallberichterstattung für den Telekommunikationsbereich vorsieht, erscheint wenig erfolgversprechend bzw. wird, wie auch andere Beispiele zeigen, in der Praxis scheitern.

Sensitivitätsanalyse

Um Wenn-Dann-Fragen beantworten zu können bzw. Abhängigkeiten und Vernetzungen zu erkennen, ist eine systemische Analyse erforderlich. Im Zuge der Bearbeitungen dieses Themas wurde durch den Autor gemeinsam mit einem Vertreter des Krisenmanagementes der Stadt Wien eine Sensitivitätsanalyse durchgeführt.

Das Sensitivitätsmodell nach Professor Vester wurde zur Analyse von komplexen Systemen entwickelt und ist universell einsetzbar. Dabei werden die vernetzten Zusammenhänge in einem System herausgearbeitet. Diese sind auch für ein präventives Krisenmanagement und für die aktive und nachhaltige Systemgestaltung von besonderer Relevanz. Durch die transparente, partizipative und kollaborative Bearbeitung erfüllt das Modell auch die Anforderungen der Netzwerkgesellschaft. Insgesamt konnte festgestellt werden, dass die Sensitivitätsanalyse ein taugliches Instrument für ein präventives Krisenmanagement darstellt und daher dieser Ansatz weiter verfolgt werden sollte.

Internationale Zusammenarbeit

Im Bereich der Krisenreaktion nimmt das Einsatz- und Krisenkoordinationscenter des Bundesministeriums für Inneres die Rolle eines nationalen und internationalen Point of Contact (PoC) wahr.

Die internationale Zusammenarbeit muss sich aber gerade bei komplexen Schadenslagen bereits in den Phasen der Vermeidung und Vorbereitung niederschlagen, da die meisten Szenarien auch einen internationalen Kontext aufweisen werden. Darüber hinaus ist die Verfügbarkeit einer Vernetzung auch zu Stellen außerhalb des unmittelbaren Schadensbereiches eine wichtige Erkenntnis aus der Natur. Und letztendlich gilt hier das Gleiche wie auf nationaler Ebene.

Man muss seine Nachbarn bzgl. ihrer Fähigkeiten und Ressourcen einschätzen können, um im Anlassfall besser zusammenarbeiten zu können.

Die Netzwerkgesellschaft und das nationale Krisenmanagement

Der Artikel basiert auf der Masterarbeit des Autors *„Die Netzwerkgesellschaft und das nationale Krisenmanagement - Anforderungen an das nationale Krisenmanagement bei komplexen Schadenslagen am Beispiel Österreichs“* und steht auf der Homepage von Cyber Security Austria, Verein zur Förderung der Sicherheit Österreichs strategischer Infrastruktur, www.cybersecurityaustria.at, zur Verfügung.

Bei komplexen Schadenslagen sind die Hilfsstrukturen völlig überfordert und werden nicht ausreichen. Daher ist eine aktive Einbindung der Bevölkerung, insbesondere durch die Stärkung der Selbsthilfefähigkeit und die Erhöhung der gesamtgesellschaftlichen Resilienz unverzichtbar.

Bei den derzeit absehbaren Szenarien im Bereich der komplexen Schadenslagen ist nur eine überregionale und internationale Zusammenarbeit zielführend. Auch in der EU gibt es verstärkte Bestrebungen, diese Zusammenarbeit zu fördern, gleichwohl es nicht ganz unberechtigte Befürchtungen gibt, dass es durch die EU zu starke regionale Eingriffe geben könnte. Hier ist wie so oft ein Mittelweg zu finden.

Zusammenfassung

Mit diesem abschließenden Beitrag zum Thema „Blackout“ sollte verdeutlicht werden, dass dieses Thema zwar sehr wichtig ist, aber leider nicht das einzige Szenario einer komplexen Schadenslage darstellt. Weiters wurde versucht, in der gebotenen Kürze anzureißen, dass die Ursachen, aber auch Chancen bei diesen neuen Herausforderungen in der Vernetzung liegen. Damit die vorhandenen Chancen auch ergriffen werden können, ist vor allem vernetztes Denken, auch über Systemgrenzen hinaus, zwingend erforderlich. Wenn es hier bereits viele positive Beispiele gibt und dies in gewisser Weise auch immer ein Bestandteil des militärischen Denkens war (Stichwort Kampf der verbundenen Waffen), so zeigt sich dennoch, dass für das vernetzte Denken in der Netzwerkgesellschaft noch einige zusätzliche Schritte notwendig sind. Trotz aller technischen Möglichkeiten wird auch in Zukunft der Mensch insbersonders im Krisenmanagement die zentrale Rolle spielen, Die Technik kann zwar unterstützen, sie sollte aber nicht überbewertet werden. Die Kommunikation - eine Krise bedeutet eine Kommunikationsstörung oder -unterbrechung - spielt dabei immer eine wesentliche Rolle. Bei der derzeitigen Risiko- und Krisenkommunikation wird die Bidirektionalität noch zu wenig berücksichtigt. Bisherige Sender-Empfänger-Konzepte sind weitgehend überholt. Für die Bewältigung von zukünftigen Krisen wird die aktive Einbindung der Menschen immer wichtiger.

Eine weitere Erkenntnis ist, dass bei komplexen Schadenslagen die vorgesehenen Hilfsstrukturen völlig überfordert werden und nicht ausreichen. Daher ist eine aktive Einbindung der Bevölkerung, insbesondere durch die Stärkung der Selbsthilfefähigkeit und die Erhöhung der gesamtgesellschaftlichen Resilienz, unverzichtbar. Oft fehlt es nicht am Knowhow, sondern an der Zusammenführung und Bündelung und an der Umsetzung. Diese Bündelung ist jedoch nicht im Sinne von Zentralisierung, sondern im Sinne von Vernetzung zu verstehen.

Komplexen Schadenslagen kann nur durch eine proaktive Systemgestaltung nachhaltig begegnet werden. Daher muss der Fokus verstärkt auf die vernetzte Krisenprävention gerichtet werden, und dies am besten noch vor der ersten Krisenerfahrung, da die erwartbaren Schäden in keiner Relation zum Aufwand in der Krisenprävention stehen. Dies erfordert aber auch neue Herangehensweisen in der Risikobeurteilung, Risikokommunikation und im Aufbau einer gesamtgesellschaftlichen Resilienz.