**Zeitschrift:** ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

**Herausgeber:** Schweizerische Offiziersgesellschaft

**Band:** 178 (2012)

**Heft:** 5

**Artikel:** Die Gefährdung vernetzter Gesellschaften

**Autor:** Wolfram, Matthias

**DOI:** https://doi.org/10.5169/seals-309572

# Die Gefährdung vernetzter Gesellschaften

**Der technologische Fortschritt mit seiner immer dichteren Vernetzung grosser Teile der Welt birgt Sicherheitsrisiken, die bisher kaum beachtet werden. Die Abhängigkeit von bestimmten Dienstleistungen und Services schafft Angriffspunkte für disruptive Attacken, die stark vernetzte moderne Gesellschaften empfindlich treffen könnten.**

Matthias Wolfram

Nach dem Auftauchen der Schadsoftware Stuxnet, die vielfach als erste virtuelle Waffe kategorisiert wird, steht in vielen Medien der Cyberkrieg als neue Sicherheitsbedrohung im Zentrum der Aufmerksamkeit. Unabhängig von der Einschätzung der Wahrscheinlichkeit und Gefährlichkeit dieser Attacken jedoch missachtet diese Diskussion die der Bedrohung zu Grunde liegende Problematik: Die Vernetzung zwischen und innerhalb von Gesellschaften mit immer grösseren Abhängigkeiten in allen Lebensbereichen, ohne dass in allen Fällen deren Stabilität und Ausfallsicherheit gegeben ist. Ihre mögliche Unterbrechung, die Disruption, ist als erhebliche Gefahr zu bewerten und bedarf einer erhöhten Aufmerksamkeit.

## Kritische Infrastrukturen sind die Nabelschnur der modernen Gesellschaft

Nicht nur Angriffe auf Maschinen oder Steuerungsanlagen über virtuelle Netzwerke, wie im Falle von Stuxnet geschehen, auch die direkte physische Schädigung oder Ausschaltung neuralgischer Kontrollmechanismen und Steuerungsfunktionen oder essentieller Bestandteile von Kritischen Infrastrukturen können eng getaktete Abläufe unterbrechen und damit unter Umständen ganze gesellschaftliche Bereiche lahmlegen. Moderne, hochgradig vernetzte Gesellschaften sind auf Grund ihrer häufig auf unmittelbare Abfolgen von Vorgängen abgestimmten Prozesse extrem anfällig für Unterbrechungen ihrer Informations- und Kommunikationsströme, aber auch ihrer eng aufeinander abgestimmten Waren- und Dienstleistungsströme und ihrer technologiegesteuerten Infrastruktur. Eingriffe in diese oft mit nur wenigen Reserven ausgelegten Bereiche können leicht zu erheblichen Einschnitten in den verschiedenen


Feuerwehr rüstet sich mit ABC-Schutzanzügen aus. Bild: ZEM

Teilsystemen mit gravierenden Konsequenzen führen. Auch wenn Cyberattacken durch ihre extrem schwierige Attribution und ihre globale Reichweite von besonderer Bedeutung sind, stellen sie nur einen Teil potenzieller disruptiver Angriffe dar. Daneben haben vor allem der Einsatz von Mikrowellengeneratoren, die elektronische Schaltkreise zerstören können, die gezielte Störung von Satellitennavigationssystemen oder konventionelle Angriffe auf Infrastruktureinrichtungen als Auslöser von Kaskadeneffekten das Potential zur Disruption mit weitreichenden Auswirkungen. Auch Attacken mit radiologischen oder chemischen respektive biologischen Giftstoffen, die Bereiche verseuchen und damit im Wesentlichen unzugänglich machen, fallen in diese Kategorie. Bestimmte Mittel sind daher bei entsprechendem Einsatz als «Weapons of mass disruption»[1] zu betrachten.

**«Die hohe Vernetzung von Gesellschaften erzeugt einen erhöhten Schutzbedarf, der durch die Technologisierung von Infrastrukturen weiter steigt.»**

## Verletzlichkeit von zugänglichen Netzen

Ein gutes Beispiel bietet die Verletzlichkeit von Stromnetzen.[2] So nennt der NERC/DOE-Bericht vom Juni 2010 die Stromversorgung eine von Nordamerikas kritischsten Infrastrukturen und schreibt den untersuchten «High-Impact, Low-Frequency (HILF) events» potenziell katastrophale Auswirkungen zu.[3] Ein konzentrierter Angriff auf die Stromversorgung, der absichtlich Kaskadeneffekte wie beim «Northeast power blackout» in den USA 2003 herbeiführt, könnte in bestimmten Bereichen lang andauernde Stromausfälle zur Folge haben.[4] Angesichts der zahlreichen gesellschaftlichen und wirtschaftlichen Prozesse von der Patientenversorgung in Krankenhäusern über die Verkehrsindustrie bis hin zur Finanzwirtschaft, die von ununterbrochener Strombereitstellung abhängig ist, sind schwerwiegende Folgen denkbar. Die Anbindung von Versorgungsnetzen an das Internet zur Wartung und Steuerung öffnet dabei tendenziell Einfalltore für disruptive Angriffe, doch sind letztlich alle computergesteuerten Prozesse als anfällig anzusehen. Vor diesem Hintergrund legte die deutsche Reaktorsicherheits-Kommission fest, dass deutsche Kraftwerke auf entsprechende Gefahren hin zu untersuchen sind.[5] Ähnliche Schlussfolgerungen gelten auch für Kommunikationsnetze, auf die Wissensgesellschaften und global vernetzte Wirtschaften heute angewiesen sind.

## Synchronisation als Schwachstelle?

Satellitennavigationsdaten werden für die Synchronisierung von Finanztransfers, die Steuerung elektrischer Leitungs- und

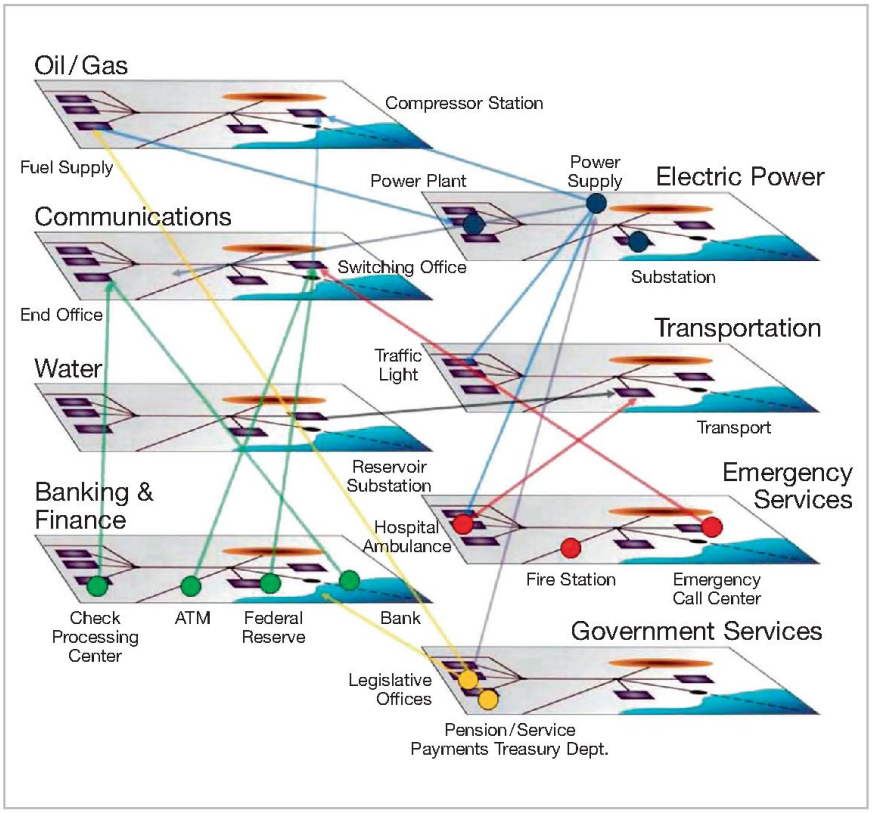
Kommunikationsnetze sowie viele Logistikprozesse eingesetzt. Die Verfügbarkeit der Daten ist daher nicht nur für militärische Anwendungen, sondern für die gesamte Gesellschaft essentiell. Durch ihre Unterbrechung kann in eng getakteten Prozessen ein Kaskadeneffekt entstehen, der Wirtschaftsprozesse erheblich beeinträchtigt.[6] Zwar sind zentrale Systeme wie die Empfänger von Flugzeugen und Schiffen in aller Regel abgeschirmt und damit kaum gefährdet. Dass eine Störung des Empfanges technisch jedoch möglich ist, zeigen unter anderem sowohl in Deutschland als auch in den USA angemeldete Patente.[7]

Die nur indirekte und mittelbare Gefahr für Menschenleben bei einem solchen Eingriff darf jedoch nicht dazu verleiten, diese Gefahren zu unterschätzen. Mittelbar sind vor allem bei einem plötzlichen flächendeckenden Stromausfall oder entsprechend schwerwiegenden Angriffen durchaus Todesfälle zu erwarten. Die Reihe der «Länderübergreifenden Krisenmanagementübung» (LÜKEX) in Deutschland spiegelt eben diese Erkenntnis wider, dass hochgradig vernetzte Gesellschaften durch bestimmte Schadensereignisse erheblich beeinträchtigt werden können. Zudem darf nicht unterschätzt werden, dass disruptive Angriffe andere Krisensituationen gezielt verschärfen können und das Potenzial besitzen, Regierungen und Verwaltungen von weniger auffälligen Geschehnissen und Bedrohungen abzulenken und zu binden.

**«Ende 2011 gab das U.S. Department for Homeland Security bekannt, dass Hacker beinahe Teile der amerikanischen Infrastruktur lahmgelegt hätten.»**

Solche Eingriffe sind selbstverständlich weder einfach und von jedermann durchzuführen noch als hochwahrscheinlich einzustufen. Dennoch sind disruptive Angriffe bei genauer Analyse essentieller Systeme möglich und müssen in die Sicherheitsvorsorge einbezogen werden. Dabei kommt es nicht darauf an, bestimmte Angriffsvektoren auszuschliessen und eine kaum zu erreichende garantierte Sicherheit anzustreben, sondern Systeme gegen einen Ausfall mit weitreichenden Konsequenzen zu sichern. Redundante Auslegung von Netzwerken und der Einbau von Reserven, so dass Teilausfälle keinen kompletten Netzwerkausfall provozieren und Kaskadeneffekte vermieden werden können, sowie die Dezentralisierung von Funktionen bieten systemische Auswege. Vor allem vor dem Hintergrund von in fast allen Bereichen notwendigen Wirtschaftlichkeitsüberlegungen müssen daher konkrete Konsequenzanalysen durchgeführt werden, um Mittel und Ressourcen in ausreichendem Umfang für die Gefahrenabwehr bereitzustellen. Dies mit Augenmass zu analysieren und über den kleinen Kreis damit befasster Experten hinaus für die möglichen Gefahren zu sensibilisieren, bleibt daher in naher Zukunft eine zentrale Herausforderung. ■

**Gegenseitige Abhängigkeit aller Elemente einer kritischen Infrastruktur.**
Grafik: Sandia National Laboratories




1 Vgl. Miller, Robert/Kuehl, Daniel: Cyberspace and the «First Battle» in 21st-century War, National Defense University, Defense Horizons, No. 68, 09/2009, S. 2.
2 Vgl. z. B. Reichenbach, Gerold/Göbel, Ralf/Wolff, Hartfrid/Stokar von Neuforn, Silke (Hrsg.): Risiken und Herausforderungen für die Öffentliche Sicherheit in Deutschland. Grünbuch des Zukunftsforums Öffentliche Sicherheit. Szenarien und Leitfragen, Berlin/Bonn, 09/2008.
3 North American Electric Reliability Corporation (NERC) and U.S. Department of Energy (DOE): High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, Washington, D.C., 2010, S. 8ff.
4 Baker, Stewart/Filipiak, Natalia/Timlin, Katrina: In the Dark: Crucial Industries confront cyberattacks, Santa Clara 2011, S. 7.
5 Vgl. RSK/ESK-Geschäftsstelle beim Bundesamt für Strahlenschutz: RSK-Stellungnahme SÜ, 437. RSK, 11.-14.05.2011, S. 111.
6 Vgl. Jasper, Scott/Giarra, Paul: Disruptions in the Commons, in: Jasper, Scott (Hrsg.): Securing Freedom in the global commons, Stanford Security Studies, Stanford 2010, S. 9.
7 Vgl. bspw. Anordnung zur Störung von fremden Satellitennavigationsempfängern, Patent DE202006014908U1 vom 08.03.2007.

Major i Gst
Matthias Wolfram
Dr. phil.
Austauschoffizier
75007 Paris