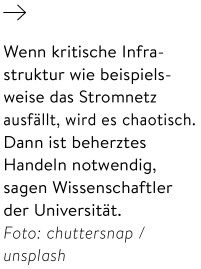
Es ist ein beklemmendes Szenario, das Thriller-Autor Marc Elsberg in seinem 2012 erschienenen Buch „Blackout“ beschrieben hat: Ein europaweiter Stromausfall führt nach nur wenigen Tagen zu Mord und Totschlag auf dem Kontinent. Offenbar ein realistisches Szenario, nicht nur beim Strom.
Die Digitalisierung wichtiger Infrastruktur birgt auch die Gefahr der Angriffe von außen, sei es durch Hacker oder spezielle militärische Einheiten. Zudem sind komplexe Netze in sich sehr fragil. Auch Schwankungen des Stromnetzes sind gefährlich: Mehrfach stand Europa 2019 vor Stromausfällen, so wie es Mitte 2019 bereits in großen Teilen Südamerikas geschah. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe rief bereits dazu auf, sich auf breitflächige Stromausfälle vorzubereiten. Wie groß ist die Gefahr wirklich? Experten der Universität Bremen geben Antworten: Ein Gespräch mit dem Elektrotechniker und Informatiker **Professor Kai Michels**, Leiter des Instituts für Automatisierungstechnik (IAT), und dem Rechtswissenschaftler **Dr. Dennis-Kenji Kipker** vom Institut für Informations-, Gesundheits- und Medizinrecht (IGMR).



Wenn kritische Infrastruktur wie beispielsweise das Stromnetz ausfällt, wird es chaotisch. Dann ist beherztes Handeln notwendig, sagen Wissenschaftler der Universität.
Foto: chuttersnap / unsplash

„Wir schalten jetzt Hamburg ab“

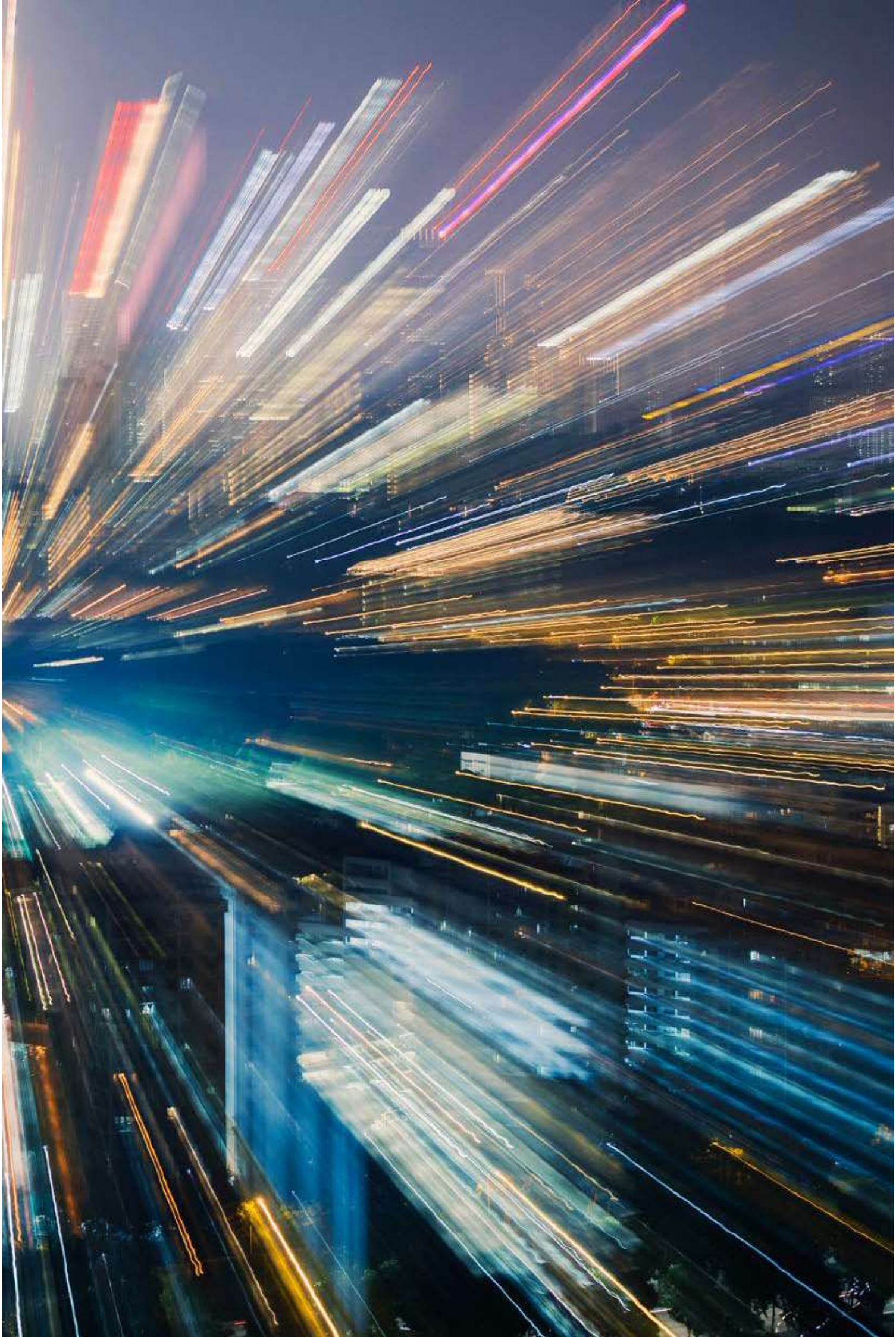
Zwei Experten der Universität Bremen bestätigen, dass großflächige Stromausfälle durchaus passieren können

Interview: Kai Uwe Bohn

Herr Michels, Herr Kipker, haben Sie vorgesorgt und für einen großflächigen Stromausfall schon Nahrungsmittelvorräte für wenigstens 14 Tage angelegt, wie es das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe empfiehlt?
Kai Michels: Meine Frau und ich denken darüber nach. Das mindeste, was man tun sollte, ist, etliche Kisten Wasser zu Hause zu deponieren. Da wird es zuerst eng, weil kein Wasser mehr aus der Leitung kommt. Zum Essen findet man vielleicht noch was für einige Tage.
Dennis-Kenji Kipker: Ich habe mir darüber noch nie Gedanken gemacht. Ich beschäftige mich zwar mit kritischen Infrastrukturen, aber die persönliche Betroffenheit ist bislang auf der Strecke geblieben.

Herr Michels, Systemdynamik und Regelungstechnik im Kraftwerksbereich sind ihr Fachgebiet. Wie groß schätzen Sie die Gefahr von Stromausfällen ein – aus welchen Gründen auch immer?
Michels: Die Gefahr ist da. Cyberangriffe halte ich für möglich. Wobei es nicht die Leitwarten für die großen Stromnetze treffen wird, denn die sind wirklich sehr gut gegen Angriffe von außen geschützt. Kraftwerke sind etwas weniger gesichert, weil sie zunehmend auch Fernwartungsmöglichkeiten haben. Wenn die Kraftwerkshersteller über das Netz auf die dortigen Rechner zugreifen können, können Hacker das auch. Und dann gibt es natürlich in jeder Stadt und in jeder Region noch mal kleinere Netzbetreiber. Ich bezweifele, dass die so gut abgesichert sind wie die großen. Wenn man die koordiniert angreift, kann man sicherlich Schaden anrichten.

Es gab 2019 mehrere Vorfälle, in denen nicht Hacker am Werk waren, sondern erhebliche Frequenzschwankungen in den europäischen Stromnetzen fast zu einer Abschaltung geführt hätten …
Michels: Das kann schon durch die Schwankungen der regenerativen Einspeisung passieren. Die meisten Solaranlagen



↑ Zwei Experten, eine Meinung: Die kritische Infrastruktur in Deutschland ist angreifbar, vor allem auf den dezentralisierten mittleren und unteren Ebenen. Professor Kai Michels (links) und Dr. Dennis-Kenji Kipker halten weitere Schutzmaßnahmen, Gesetze und Regelungen für dringend erforderlich. *Foto: Harald Rehling / Universität Bremen*

auf Deutschlands Dächern haben zum Beispiel eine automatische Notabschaltung. Wenn zu wenig Leistung im Netz ist und dadurch die Frequenz unter 49,8 Hz sinkt, gehen diese Anlagen aus, damit ihre empfindliche Elektronik geschützt wird. Wenn die sich automatisch alle auf einmal abschalten – in einem Moment, in dem wir sowieso schon viel zu wenig Leistung im Netz haben –, dann bricht das Netz zusammen. Genau in diesem Moment muss es in den großen Netzleitwarten Leute geben, die sofort sehr mutig und konsequent handeln – und zwar, indem sie ganze Städte abschalten. Die müssen dann entscheiden: „Wir schalten jetzt Hamburg ab." Und zwar innerhalb von Minuten. Und da ist das Risiko: Ob die dann auch den Mut haben, das zu tun. Wenn nicht, geht das Netz womöglich als Folge einer Kettenreaktion komplett in die Knie. Und dann haben wir den totalen Blackout. In Italien hat es das 2003 schon mal gegeben.

Herr Kipker, Sie haben sich in Ihrer wissenschaftlichen Arbeit unter anderem auf Cybersecurity spezialisiert. Wie groß ist die Gefahr, dass Terroristen, Hacker oder Geheimdienste den Kippschalter für unsere Stromnetze auf „off" stellen?

Kipker: Mir ist kein großflächiger Angriff auf Infrastruktur in Deutschland bekannt, aber es gibt meines Erachtens durchaus eine reale Gefahr. Der Gesetzgeber hat dies ja auch erkannt und Maßnahmen eingeleitet, um kritische Infrastruktur besonders zu regulieren und zu schützen. In anderen Sektoren – zum Beispiel im Gesundheitssektor – hat es schon größere Angriffe gegeben, wodurch Krankenhäuser nicht mehr arbeitsfähig waren oder personenbezogene Daten abgeflossen sind. Auch Wasserwerke wurden schon angegriffen. Wie Herr Michels bereits andeutete, haben kleine regionale Versorger oft gar nicht die Ressourcen, um IT-Sicherheit im vernünftigen Rahmen zu betreiben. Der TÜV hat beispielsweise einen sogenannten Honeypot aufgestellt, also ein ungesichertes Wasserwerk simuliert. Da haben Leute dann innerhalb kürzester Zeit versucht, die Industriesteuerungsanlagen zu beeinflussen. Es gibt die Bedrohung. Allerdings lässt sie sich schwer in Zahlen bemessen.

„Das mindeste, was man tun sollte, ist, etliche Kisten Wasser zu Hause zu deponieren."

Professor Kai Michels

Zur Person

Dr. Dennis Kenji-Kipker hat an der Universität Bremen Rechtswissenschaft studiert. Anschließend war er in der Arbeitsgruppe von Professor Benedikt Buchner tätig; 2015 promovierte er mit der Arbeit „Informationelle Freiheit und staatliche Sicherheit – Rechtliche Herausforderungen moderner Überwachungstechnologien." Seit 2016 ist Dennis-Kenji Kipker wissenschaftlicher Geschäftsführer am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) der Universität Bremen. Er war unter anderen an der bundesweiten Studie „Monitor IT-Sicherheit kritischer Infrastrukturen" beteiligt.

Professor Kai Michels hat an der TU Braunschweig Elektrotechnik und Informatik studiert und dort auch promoviert. Als wissenschaftlicher Mitarbeiter forschte er anschließend in Braunschweig am Institut für Regelungstechnik, ehe er 1997 in die Wirtschaft wechselte und für die Siemens AG im Bereich Kraftwerksleittechnik und Kraftwerkssimulation sowie Gasfördertechnik arbeitete. Von 2002 bis 2010 war Michels für die Fichtner Ingenieurberatung GmbH in Stuttgart und Ludwigshafen – dort als Geschäftsführer – tätig. Seit 2010 ist er Leiter des Instituts für Automatisierungstechnik der Universität Bremen, wo er den Lehrstuhl für Systemdynamik und Regelungstechnik bekleidet.

„Viele Anwendungen werden durch Computerisierung heute komfortabler, aber dadurch steigen zwangsläufig auch die Risiken."

Dr. Dennis Kenji-Kipker

Es heißt ja oft, der nächste Krieg würde nicht mehr nur konventionell oder atomar, sondern auch im Internet ausgefochten ....
Kipker: Das wird so sein. Schon 2010 hat der Computerwurm Stuxnet Geschichte gemacht: Er wurde geschrieben, um in bestimmte Siemens-Steuerungen einzugreifen, die in Wasserwerken, Klimatechnik oder Pipelines eingesetzt werden. Weil Stuxnet vor allem Schaden in einer Wiederaufbereitungsanlage und einem Kernkraftwerk im Iran anrichtete, muss von einem politisch motivierten Angriff ausgegangen werden. Wer dahinter steckt, ist bis heute unbekannt, da gibt es nur Vermutungen. Das Beispiel zeigt aber: So etwas ist grundsätzlich möglich.

Stuxnet wurde mutmaßlich über einen USB-Stick eingeschleust. Heutzutage ist jedoch alles miteinander vernetzt und über das „Internet der Dinge" erreichbar. Ist das nicht das ideale Einfallstor?
Michels: Das ist das, was mich tatsächlich unruhig macht und wovor ich auch in Vorträgen immer wieder warne. Diese ganze Diskussion um „Industrie 4.0", in der jedes Gerät einen eigenen Internetzugang hat und damit manipulierbar ist – von wem auch immer. Ich habe sogar schon mal gedacht, ob nicht eine Strategie des amerikanischen Auslandsgeheimdienstes NSA dahintersteckt, dass alle plötzlich so wild hinter diesem Thema her sind. Smarte Geräte sind manipulierbar! Der Thriller von Marc Elsberg basiert ja auf manipulierten Stromzählern – genau so ein Szenario halte ich für vorstellbar. Interessanterweise sind unsere Kernkraftwerke nicht angreifbar, die haben nämlich gar keine Computer. Die laufen noch mit Schalttechnik aus den 1970er-Jahren. Das ist immer noch die einzige Technologie, die den extrem hohen Sicherheitsanforderungen in diesem Bereich genügt. Wenn wir in Zukunft unsere Stromversorgung über regenerative Erzeugungsanlagen dezentralisieren, die ans Internet angebunden sind, könnte man mit einem flächendeckenden Angriff Schaden anrichten.
Kipker: Auch den USB-Stick – also den Innentäter – halte ich immer noch für möglich. Was die Gefahren durch die Vernetzung angeht, sehe ich es ähnlich. Viele Hersteller von Geräten oder Komponenten der „Industrie 4.0" hatten bis vor kurzem nichts mit Cybersecurity zu tun. Da werden dann Bauteile von Zulieferern eingebaut, deren Sicherheit überhaupt nicht geprüft wird. Viele Anwendungen werden durch Computerisierung heute komfortabler, aber dadurch steigen zwangsläufig auch die Risiken. Wenn man sich den Bereich „Gesetzgebung und Cybersicherheit" anschaut, ist es so, dass im Energiesektor auch einige Einrichtungen benannt werden, die zur kritischen Infrastruktur gehören. Die müssen technische und organisatorische Sicherheitsmaßnahmen ergreifen. Aber wann gilt eine Einrichtung für die Versorgung der Bevölkerung als kritisch? Der Schwellenwert liegt derzeit bei einem Versorgungsgrad von etwa 500.000 Personen. Man versucht momentan im Rahmen einer Gesetzesänderung, auch kritische Infrastruktur unterhalb dieses Schwellenwerts zu erfassen und zu sichern. Das IT-Sicherheitsgesetz von 2015 war ein erster Aufschlag, nun muss punktuell nachgebessert werden.

Herr Michels, wenn dann tatsächlich mal alles „schwarz" ist – wie kommt der Strom wieder zurück?
Michels: Manche Kraftwerke haben extra Notstromdiesel, um sich selbst wieder hochzufahren. Aber weil die noch am Netz hängen und alle Verbraucher, die von jetzt auf gleich ausgefallen sind, noch auf „An" stehen, würde es gleich wieder in die Knie gehen. Man muss also dieses Kraftwerk erst mal „freischalten" und seine Belastung verringern, damit es geordnet hochfahren kann. Dann muss es mit anderen Kraftwerken vernetzt werden, die ebenfalls „sauber" gestartet wurden. Man müsste also das Netz langsam Stück für Stück zuschalten. Wie das aber bei einem großflächigen Ausfall gehen soll, wenn die komplette Kommunikation zusammengebrochen ist – da bin ich auch mal gespannt. Natürlich gibt es Notfallpläne, aber die wurden bisher nur in der Theorie durchgespielt. Man weiß ja zu keinem Zeitpunkt, wie lange es dauert, und tappt im wahrsten Sinne des Wortes im Dunkeln. Deswegen ist nach ausreichend Wasser auch das batteriebetriebene Radio Pflicht. ●