KRITISCHE ENERGIE-INFRASTRUKTUR IN GEFAHR DURCH CYBERBEDROHUNGEN

Frank Umbach

Ende Mai wurde ein neuer Superwurm mit dem Namen Flame entdeckt, der noch erheblich aufwendiger und komplizierter sein soll als der im Sommer 2010 entdeckte Stuxnet-Sabotagewurm.[1] Beide waren gegen den Iran und seine Nuklearanlagen gerichtet. Flame ist allerdings primär ein allumfassender Spionagewurm. Zugleich verdichteten sich die Anzeichen, dass der Stuxnet-Wurm, der zum Angriff auf Steuerungs- und Kontrollsysteme von Industrieanlagen unter dem Code-Wort „Olympische Spiele" entwickelt worden war, tatsächlich den USA in Kooperation mit Israel zuzuschreiben war.[2] Die Aufdeckung und „Enttarnung" des Urhebers des Stuxnet-Wurms musste zugleich nicht unwesentliche politische Kollateralschäden haben[3] – vor allem in Hinsicht auf die gegenwärtigen Verhandlungen der Weltgemeinschaft und der USA mit dem Iran, der verdächtigt wird, ein Nuklearwaffenprogramm zu betreiben. Langfristig könnten die USA sogar der größte Verlierer sein, da die Schadprogramme wie Stuxnet und Flame auch von ihren Opfern und dritter Seite kopiert, modifiziert und

Dr. Frank Umbach ist Associate Director des European Centre for Energy and Resource Security (EUCERS) am King's College in London, Leiter des Programms International Energy Security am Centre for European Security Strategies (CESS GmbH) in München und Non-Resident Senior Fellow des US Atlantic Council in Washington DC.

1 | Vgl. David E. Sanger, „Obama Stepped up Wave of Cyberattacks on Iran", *The New York Times*, 01.06.2012; Nicole Perlroth, „Researchers Find Clues in Malware", *The New York Times*, 30.05.2012; Michael Borgstede, „Ein Virus nach dem Baukastenprinzip", *Die Welt*, 30.05.2012, 6; „‚Der Feind am Ende der Leitung hört mit' – Interview mit Alexander Gostew, Chef-Experte des Antiviren-Unternehmens Kaspersky Lab", *Die Welt*, 30.05.2012, 10; Thomas Erdbrink, „Iran Confirms Attack by Virus That Collects Information", *The New York Times*, 29.05.2012.

2 | Vgl. Ansgar Graw, „Barack Obama führt den Krieg der Zukunft", *Die Welt*, 03.-06.06.2012, 4; ders., „US-Präsident befahl Angriff mit Stuxnet-Virus", *Die Welt*, 02.06.2012, 1.

3 | Vgl. Sandro Gaycken, „Strategische Kollateralschäden", *Handelsblatt*, 06.06.2012.

weiterentwickelt werden können. Zwar besitzen die USA heute das größte Potenzial an offensiven Cyberwaffen, sie sind aber zugleich als hochtechnisierte Industriegesellschaft durch die vernetzte IT auch am verwundbarsten, zumal die Defensivfähigkeiten nicht mit ihren Offensivfähigkeiten mithalten können. Haben die USA mit dem Stuxnet-Wurm somit die Büchse der Pandora selbst geöffnet?

KRITISCHE NATIONALE INFRASTRUKTUREN BEDROHT

Die Brisanz in der Aufdeckung dieser digitalen Schadsoftwareprogramme liegt vor allem darin begründet, dass die staatliche Entwicklung und Förderung offensiver Cyberwaffen gegen Industrieanlagen und damit auch gegen kritische Infrastrukturen wesentlich weiter vorangeschritten ist als dies bis 2010 auch von Experten zumeist angenommen worden war. Nach Ansicht des früheren Anti-Terror-Beraters Richard Clarke haben inzwischen 20 bis 30 Staaten Fähigkeiten für offensive Cyberkriegsführung aufgebaut.[4] Hierzu gehören nicht nur die USA, China und Russland, sondern auch kleinere Staaten und zahlreiche Mittelmächte, einschließlich Iran und Nordkorea. Seit 2011 liefern sich israelische und arabische Hackergruppen eine regelrechte Cyberschlacht mit immer neuen „Vergeltungsschlägen" als eine Art neuer unerklärter Krieg.[5]

20 bis 30 Staaten haben Fähigkeiten für offensive Cyberkriegsführung aufgebaut. Hierzu gehören nicht nur die USA, China und Russland, sondern auch kleinere Staaten und Mittelmächte, einschließlich Iran und Nordkorea.

In den letzten Jahren sind Cyberangriffe und Cyberkriminalität eine große Gefahr für Industrie und Regierungen geworden. Sie verursachen inzwischen weltweit einen Verlust in Höhe eines dreistelligen Milliarden-Betrages in Euro. Zwar bezifferte das Bundeskriminalamt (BKA) die durch Cyberkriminelle verursachten Schäden 2011 auf 71 Millionen Euro. Doch ist die Dunkelziffer auch in Deutschland um ein Vielfaches höher.[6] Auch hier sind private und staatliche

4 | Vgl. auch Richard A. Clarke und Rob Knake, *World Wide War. Angriff aus dem Internet*, Hoffmann und Campe, 03/2011.

5 | Vgl. Max Borowski, „Cyberschlacht im Nahen Osten", *Financial Times Deutschland*, 11.01.2012, 11; Tom Gara, „Uprisings Spark an Increase in Malicious Activity Online", *Financial Times*, 27.03.2012, 1.

6 | Vgl. Annika Graf, „Unternehmen erschweren Schutz vor Hacker-Attacken", *Financial Times Deutschland*, 31.05.2012, 3; Hans Evert, „Unternehmen im Netz der Wirtschaftspione", *Die Welt*, 04.04.2012, 12.

Akteure häufig eng verbunden. Das Russian Business Network (RBN) gilt weltweit als die mächtigste und gefährlichste Cyberkriminalitätsorganisation. Sie ist zugleich die einzige Organisation dieser Art, die auch von der NATO als eine Hauptbedrohung eingestuft wurde. Allein rund 40 Prozent der globalen Cyberkriminalität soll auf ihr Konto gehen, das in 2007 bereits mehr als 100 Milliarden US-Dollar ausgemacht haben soll.[7] Derartige Cyberangriffe bedrohen die Sicherheit all unserer Aktivitäten, da die Welt in allen Lebensbereichen zunehmend von den Informationstechnologien und deren weltweiter Vernetzung durch das Internet abhängig ist.[8]

Cyberangriffe bedrohen die Sicherheit all unserer Aktivitäten, da die Welt in allen Lebensbereichen zunehmend von den Informationstechnologien und deren weltweiter Vernetzung durch das Internet abhängig ist.

Dabei sind nicht nur Privatpersonen und Unternehmen vom Diebstahl persönlicher Kundendaten oder sensitiver betrieblicher Informationen betroffen, sondern zunehmend auch Regierungen, ihre Kommunikationskanäle und Infrastrukturen. So waren Anfang 2011 vor allem Kanada und Frankreich Opfer von Cyberangriffen, doch war und ist fast jeder westliche Staat von derartigen Angriffen betroffen. Häufig handelt es sich hierbei nicht nur um Datendiebstahl, sondern auch um so genannte Distributed Denial of Service (DDS)-Angriffe, bei denen Webserver mit so vielen Anfragen bombardiert werden, dass sie kollabieren und für ihre Kunden nicht mehr erreichbar sind. Derartige Cyberattacken werden erst dann eingestellt, wenn entsprechendes „Lösegeld" bezahlt wird.[9]

Dabei stehen nicht nur einzelne Hacker oder lose organisierte politische Gruppierungen wie Anonymous oder Lulzsec hinter den Angriffen, sondern auch feindselige Regierungen, die sich hinter „unheiligen Allianzen" mit Verbrechersyndikaten, Terroristen oder nationalistischen Bewegungen und Personen verstecken, ohne jedes Risiko, entdeckt oder identifiziert zu werden. Unter Sicherheitsexperten gelten vor allem so genannte „kritische Infrastrukturen" als besonders gefährdet, da sie für das Überleben des

7 | Vgl. Newsweek (Hrsg.), „The (Evil) Cyber Empire", 29.12.2009; Alexander Klimburg, „Mobilising Cyber Power", *Survival*, 03-04/2011, 41-60, hier: 48 ff.

8 | Vgl. auch Sandro Gaycken, *Cyberwar. Das Internet als Kriegsschauplatz*, München, 2011.

9 | Vgl. auch Misha Glenny, *Cybercrime. Kriminalität und Krieg im digitalen Zeitalter*, München, 2012.

Staates und die Aufrechterhaltung seiner vitalen staatlichen Funktionen von herausragender Bedeutung sind. Kritische Infrastrukturen schließen Informations- und Telekommunikationssysteme ebenso ein wie die Sektoren Transport und Verkehr, Energieversorgung, Gesundheitswesen, Finanz- und andere sensible Dienstleistungen.[10] Diese kritischen Infrastrukturen sind durch ein hohes Maß an interner Komplexität und einer hochgradigen gegenseitigen Abhängigkeit sowie Verwundbarkeit gekennzeichnet. Gleichzeitig sind die konkreten Verantwortlichkeiten, gesetzlichen Vorschriften und Regularien zwischen den Mitgliedstaaten innerhalb der EU-27 sehr unterschiedlich verfasst. Dies setzt sich auf nationaler Ebene vor allem in föderalen Staatsgebilden wie in Deutschland zwischen der Bundes- und Landesebene ebenso fort wie zwischen verschiedenen Ministerien. Zudem sind in Europa wie in Deutschland rund 80 Prozent aller kritischen Infrastrukturen in der Hand von Privatunternehmen. Das erfordert eine kontinuierliche Kooperation zwischen staatlichen Dienststellen und der Privatwirtschaft. Diese aber war bis vor wenigen Jahren in kaum einem EU-Land institutionell organisiert, ebenso wenig waren die jeweiligen Zuständigkeiten zwischen Staat und Privatwirtschaft klar und einvernehmlich geregelt.

In Europa wie in Deutschland sind rund 80 Prozent aller kritischen Infrastrukturen in der Hand von Privatunternehmen. Das erfordert eine kontinuierliche Kooperation zwischen staatlichen Dienststellen und Privatwirtschaft.

Die Notwendigkeit des Schutzes kritischer Infrastrukturen als aufkommendes nationales und internationales Sicherheitsrisiko wurde zwar schon ab Mitte der 1990er Jahre erkannt, wird aber verstärkt erst seit 2001 wahrgenommen

10 | Vgl. „Council Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection“, 2008/114/EC, Brüssel, 08.12.2008; ‚Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure‘, research project funded by European Union/DG Justice, Freedom and Security, Final Report, 2009; Federal Ministry of the Interior (BMI), „Protecting Critical Infrastructures – Risk and Crisis Management“, Berlin, 01/2008. Siehe auch die Webseiten der Kommission: „Energy Infrastructure: Critical Infrastructure Protection“, http://ec.europa.eu/energy/infrastructure/critical_en.htm [23.07.2012]; „Critical Information Infrastructure Protection“, http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm [23.07.2012]; „European Programme for Critical Infrastructure Protection (EPCIP)“, http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm [23.07.2012].

und ist durch die internationalen Terrorentwicklungen sowie die Bildung des US Department of Homeland Security wesentlich geprägt. In den letzten Jahren hat sich jedoch der Schwerpunkt der Sicherheitsbesorgnisse zunehmend von physischen Terror- auf Cyberangriffe verlagert. Kritische Infrastrukturen wurden seit den Terroranschlägen vom 11. September 2001 immer häufiger Zielscheibe von Cyberangriffen. So wurden 2009 Viren im amerikanischen Stromnetz entdeckt, die aus China und Russland stammen sollen und die USA womöglich in einer außenpolitischen Krise mit den beiden Staaten politisch erpressbar machen könnten.

Die Schädigung oder Unterbrechung sensitiver Funktions- und Kommunikationsprozesse innerhalb und zwischen „kritischen Infrastrukturen" kann weitreichende politische, soziale und wirtschaftliche Auswirkungen haben, die sich zudem kaskadenartig schnell auch auf andere (Nachbar-) Staaten erstrecken können.[11] Alle kritischen Infrastrukturen sind in modernen Industriegesellschaften durch eine zunehmende integrierte Vernetzung gekennzeichnet und durch zwei Dinge miteinander verbunden: Energie und Internetdienste. Gelingt die längerfristige Unterbrechung von Energieversorgung und/oder Internetanbindung, sind lebenswichtige staatliche Funktionen wie die Verbraucherversorgung mit Energie und Wasser und damit viele andere kritische Infrastrukturen nicht mehr gewährleistet.[12] Je stärker eine Industriegesellschaft und deren kritische Infrastrukturen durch das Internet vernetzt sind, umso stärker sind auch die potenziellen Risiken und Verwundbarkeiten ausgeprägt.[13]

Gelingt die längerfristige Unterbrechung von Energie- und Internetanbindung, sind lebenswichtige staatliche Funktionen wie Energie- und Wasserversorgung und damit viele andere kritische Infrastrukturen nicht mehr gewährleistet.

11 | Vgl. auch Commission of the European Communities, „Protecting Europe from Large-Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience", SEC(2009) 399/SEC(2009)400, Brüssel, 30.03.2009, COM(2009)149 final; Frank Umbach, „Waking Up to Cyber-Attack Threats in All Walks of Life", Special Report, *Geopolitical Information Service*, 13.10.2011, 4.

12 | Vgl. auch Frank Umbach, „Europe's New Electricity Networks Face Danger of Cyber-Attacks", Special Report, *Geopolitical Information Service*, 18.10.2011.

13 | Vgl. Fn. 11.

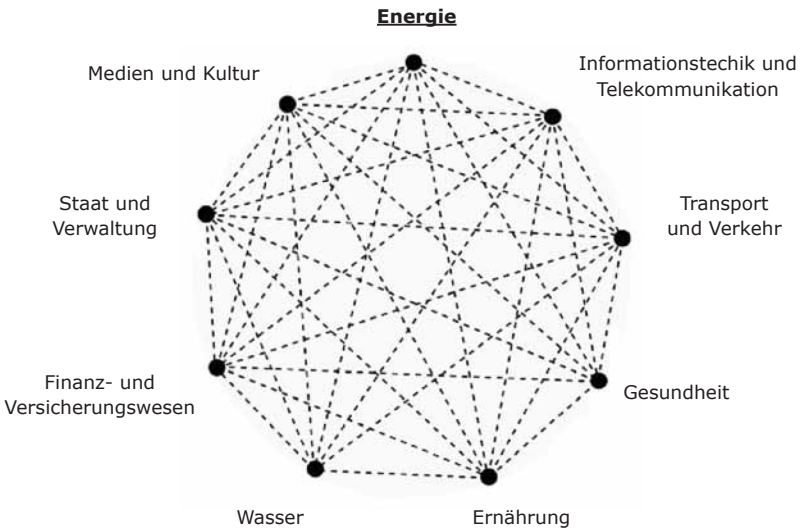
Dabei gelten unter westlichen Sicherheitsexperten Cyberangriffe für die europäische Energieversorgung und für kritische Energieinfrastrukturen als die wahrscheinlich größte aller Bedrohungen. Die kritischen Energieinfrastrukturen umfassen Einrichtungen und Netzwerke insbesondere zur Stromerzeugung, aber auch zur Förderung von Öl und Gas, Lagerung und Raffinerien, Flüssiggasterminals sowie Transport- und Verteilungssysteme. Als besonders verwundbar und sensitiv gelten Energiekontrollzentren mit ihren SCADA-Systemen zur Steuerung und Kontrolle der Energieversorgung.[14]

Als besonders verwundbar gelten Energiekontrollzentren mit ihren SCADA-Systemen zur Steuerung und Kontrolle der Energieversorgung.

Auch wenn das Sicherheitsbewusstsein wegen vermehrt auftretender Cyberangriffe bei westlichen Regierungen und Industrieunternehmen in den letzten Jahren allgemein gestiegen ist, so hat dieses dennoch nicht mit den qualitativ neuen Gefahren und der Verletzbarkeit im Cyberspace Schritt gehalten. Das fehlende Sicherheitsbewusstsein kann jedoch alle Bereiche des privaten und öffentlichen Lebens, den nationalen und internationalen Handel sowie die Verteidigungspolitik von Ländern und multinationalen Organisationen wie der Europäischen Union und der NATO beeinflussen.

14 | Vgl. auch Frank Umbach und Uwe Nerlich, „Asset Criticality in European Gas Pipeline Systems – Increasing Challenges for NATO, its Member States and Industrial Protection of Critical Energy Infrastructure“, in: Adrian Gheorghe und Liviu Muresan (Hrsg.), „Energy Security. International and Local Issues, Theoretical Perspectives and Critical Energy Infrastructures“, *NATO Science for Peace and Security Series – C: Environmental Security*, Springer, Dordrecht, 2011, 273-303; Frank Umbach, „Critical Energy Infrastructure Protection in the Electricity and Gas Industries. Coping with Cyber Threats to Energy Control Centers“, *OSCE-CTN Newsletter*, Special Bulletin: „Protecting Critical Energy Infrastructure from Terrorist Attacks“, Wien, 01/2010, 25-28.

Abb. 1
Interdependenzen Kritischer Infrastrukturen



Quelle: Bundesministerium des Innern (BMI), *Schutz kritischer Infrastrukturen. Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden*, Berlin, 05/2011, 10.

Immerhin haben die EU-27 und ihre Mitgliedstaaten seit 2005 die potenziellen Gefahren derartiger Cyberangriffe auf kritische Infrastrukturen zunehmend erkannt und entsprechende nationale und multilaterale Gegenstrategien entwickelt. Doch hapert es noch immer bei der Implementierung sowohl auf staatlicher als auch auf EU-Ebene. Traditionell favorisiert jeder Staat nicht zuletzt aufgrund historischer Gegebenheiten und Traditionen seine eigenen Sicherheitskonzepte, verantwortliche Institutionen sowie Programme, um auf die neuen Sicherheitsbedrohungen für den Schutz kritischer Infrastrukturen, einschließlich der kritischen Informationsinfrastrukturen (*critical information infrastructure*, CII) adäquat zu reagieren. Doch greifen auch hierbei nationale Sicherheitskonzepte allein zu kurz, da solche Cyberangriffe ein nie dagewesenes Niveau an Raffinesse erreicht haben und die Verletzlichkeit von digitalen Systemen und Netzwerken in den letzten Jahren exponenziell angewachsen ist. Die Schäden, die auf Cyberkriminalität und Cyberspionage zurückzuführen sind, haben vor allem in zahlreichen westlichen Ländern erschreckende Ausmaße

angenommen, weil die technischen Bemühungen der Staaten und die neu verabschiedeten Gesetze und Regulierungen immer hinterherhinken.

Tabelle 1
Wegmarken des Critical Infrastructure Protection (CIP)-Programmes der EU

2005	Grünbuch über ein europäisches Programm für den Schutz kritischer Infrastrukturen
2006	Europäisches Programm für den Schutz kritischer Infrastrukturen (EPSKI)
2008	EU-Richtlinie über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern
2009	Mitteilung über den Schutz kritischer Informationsinfrastrukturen
Mai 2010	Annahme der digitalen Agenda, in der Sicherheit als eine Bedingung für Informations- und Kommunikationstechnologien ausgewiesen wird
September 2010	Die Europäische Kommission nimmt einen Vorschlag für eine Richtlinie an
September 2010	Vorschlag der EU-Kommission, die Europäische Agentur für Netz- und Informationssicherheit ENISA auszubauen
November 2010	Gründung der gemeinsamen Arbeitsgruppe zu Cyber-Security und Cybercrime der EU und der USA
März 2011	Mitteilung der EU-Kommission über den Schutz kritischer Informationsinfrastrukturen „Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit“
Ende 2011	Gemeinsame Cyber-Sicherheits-Übung der EU und der USA
2013	ENISA wird mit dem Betrieb von EISAS (European Information Sharing and Alert System) beginnen

Quelle: *EurActive*.

Im uralten Kampf zwischen Angreifer und Verteidiger erscheint derzeit der Angreifer mehr denn je im Vorteil. Er ist besser gerüstet, wählt die Intensität des Angriffs sowie das Ziel und wird nicht mehr länger durch geografische Entfernung oder staatliche Grenzen behindert. Zudem kann der Angreifer heimlich vorgehen, bleibt zumeist anonym und hat so die Möglichkeit, effiziente und „kostengünstige“ asymmetrische Strategien auszuwählen.

All diese neuen Cyberbedrohungen kritischer nationaler Infrastrukturen haben eine weltweite Nachfrage für moderne Sicherheitstechnologien, Dienstleistungen und Managementfähigkeit geschaffen. Die Märkte für Produkte und Dienstleistungen der zivilen Verteidigung mitsamt ICT- und Softwareproduzenten zum Schutz vor Terroristen, Piraten, Verbrechern und Hackern weisen heute die größten Wachstumsraten der Welt auf. Der globale Markt für Netzsicherheit wird allein auf 60 Milliarden US-Dollar geschätzt und soll in den nächsten drei bis fünf Jahren weiter durchschnittlich um zehn Prozent pro Jahr wachsen.[15]

EIN „DIGITALES PEARL HARBOR"? DIE QUALITATIV NEUEN SICHERHEITSRISIKEN UND VERWUNDBARKEITEN KRITISCHER INFRASTRUKTUREN DURCH CYBERANGRIFFE[16]

Cyberangriffe können durch bösartige Softwareprogramme in Form von Viren, Würmern, Trojanern und DDS-Angriffen durch Einzelne sowie durch Verbrecher- oder Terrororganisationen erfolgen. Sie dienen sowohl zur Spionage als auch zur Störung und Schädigung von Steuerungs-, Kontroll-, Informations- und Kommunikationsprozessen kritischer Infrastrukturen und Unternehmen. Die meisten Cyberangriffe dienen jedoch noch immer dem Ziel des Ausspähens und Diebstahls sensibler persönlicher Kundendaten oder betrieblicher Geheimnisse. Einer der ersten Fälle eines so genannten Cyberkriegs ereignete sich bereits 1982, als das Computerkontrollsystem einer kanadischen Firma vom sowjetischen Geheimdienst gestohlen worden war und später eine sowjetische Ölpipeline zur Explosion brachte. Der Software-Code war zuvor von

Einer der ersten Fälle eines so genannten Cyberkriegs ereignete sich bereits 1982, als ein Computerkontrollsystem einer kanadischen Firma vom sowjetischen Geheimdienst gestohlen worden war.

15 | Vgl. „Kalter Krieg im Internet", *Die Welt*, 04.05.2012, 14.

16 | Die folgende Analyse baut unter anderem auch auf Ergebnissen von größeren Forschungsprojekten der Europäischen Kommission (Octavio, Inspire) aus den letzten Jahren auf, in die der Autor und die CESS GmbH in München involviert waren. Vgl. „Octavio: Energy System Control Centers Security – an EU Approach", research project funded by European Union/DG Justice, Freedom and Security under Program C 2008/60/03: Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks, *Final Report 2009*; *Inspire: Increasing Security and Protection Through Infrastructure Resilience*, research project funded by European Union under 7th FWP (Seventh Framework Program), 31.10.2010.

der CIA manipuliert worden, um so eine „logische Bombe" zu schaffen.[17]

Die Entwicklung von Botnetzen durch infizierte Computer, die für kriminelle Zwecke missbraucht werden und schlafende Viren als Trojaner unbemerkt für Internetnutzer auf deren Rechnern einschleusen können, hat die Situation um einiges brisanter gemacht. Diese Virenprogramme können mit einem Netzwerk gekaperter Computer auf der ganzen Welt von den Angreifern immer und überall aktiviert werden und Internetseiten und Server mittels gezielter Überlastung durch DDS-Angriffe lahmlegen. Sie erlauben Kriminellen oder Terroristen massive Angriffe im Bereich der Datenspionage, der Datenfälschung, der Zerstörung oder Veränderung sowie Manipulation vertraulicher Daten mit äußerst schädlichen Auswirkungen auf die Industrie und auch auf kritische nationale Infrastrukturen. Die derzeit wohl gefährlichste Botnetzbedrohung Conficker soll weltweit mehr als 1,5 Millionen Computer infiziert haben und ggf. weitere fünf Millionen Computer in 122 Ländern rekrutieren und kommandieren können. Auch wenn dieser Wurm bisher nicht „erweckt" worden und aktiv geworden ist, so ist weder seine Herkunft bekannt geworden noch konnten bisher Gegenstrategien entwickelt werden.[18] Vor diesem Hintergrund warnte z.B. der Vorsitzende des Permanent Monitoring Panel on Information Security at the World Federation of Scientists, Henning Wegener, im Jahr 2009: „Die Verwundbarkeit der digitalen Endgeräte und der sie verbindenden Netze wird unterschätzt – obwohl die Gefahren und Schäden mit zunehmender Beschleunigung und höherer technischer Raffinesse alarmierend und exponenziell wachsen. Die Dynamik dieses Wachstums, das unkontrollierte Wuchern der Angriffe im Cyberspace und die enorme Potenzierung der Gefahren zeigen: Wir stehen vor einem Quantensprung im Bereich der digitalen Bedrohungen."[19]

Virenprogramme können mit einem Netzwerk gekaperter Computer auf der ganzen Welt von den Angreifern immer und überall aktiviert werden und Server mittels gezielter Überlastung lahmlegen.

17 | David J. Betz und Tim Stevens, *Cyberspace and the State. Toward a Strategy for Cyber-Power*, Adelphi Series IISS, Nr. 424, London-Abindon-Oxon, 2011, 20 f.

18 | Vgl. auch Mark Bowden, *Worm. Der erste digitale Weltkrieg*, Berlin, 2012.

19 | Henning Wegener, „Der unsichtbare Feind. Die neuen Gefahrenlagen im digitalen Raum", *Internationale Politik*, 09-10/2009, 48-57, hier: 48.

Der erste größere und gut koordinierte Cyberangriff mit staatlicher Beteiligung erfolgte im Zuge diplomatischer Konflikte zwischen Russland und Estland 2007/2008 sowie zwischen Russland und Litauen 2008, als estnische und litauische Regierungs- und Kommunikationsnetze angegriffen und zeitweise außer Betrieb gesetzt wurden. Auch vor und während des militärischen Konflikts zwischen Russland und Georgien im Sommer 2008 wurden parallel georgische Regierungs- und andere wichtige Kommunikationsstrukturen erfolgreich angegriffen und nachhaltig gestört, einschließlich eines Angriffs zur Außerdienststellung und fremden Steuerung der Baku-Tbilisi-Ceyhan-Ölpipeline. Doch trotz vieler Hinweise und Indikatoren konnten weder Estland noch Georgien oder die NATO und die EU eindeutig beweisen, dass die Angriffe von Russland ausgingen.[20] Im Juli 2009 wurden mehr als 12.000 Computer in Südkorea und 8.000 weitere in den USA und anderen Ländern aus Nordkorea angegriffen, ohne dass eindeutig nachgewiesen werden konnte, wer hierfür verantwortlich war.

Im Juli 2009 wurden mehr als 12.000 Computer in Südkorea und 8.000 weitere in den USA und anderen Ländern aus Nordkorea angegriffen, ohne dass eindeutig nachgewiesen werden konnte, wer hierfür verantwortlich war.

Die große Zunahme privater und staatlicher Cyberangriffe durch einzelne Hacker, lose politische Gruppierungen, transnationale Kriminalitätsstrukturen, terroristische Zellen oder auch staatliche Institutionen (wie Geheimdienste, fremde Streitkräfte etc.) erklärt sich vor allem aus den folgenden Umständen:

- Derzeit kann allenfalls nachgewiesen werden, aus welchen Ländern Cyberangriffe erfolgt sind, nicht aber von wem sie tatsächlich ausgingen. Unter bestimmten Umständen könnten die Computer eines Landes auch von anderen Gruppierungen außerhalb des Landes missbraucht worden sein. Solange die internationalen Staaten derartige Angriffe nicht eindeutig nachweisen und die konkreten Angreifer feststellen können, fühlen sich diese sicherer denn je und erhalten jedes Jahr vermehrt Zulauf, wie die internationalen Kriminalitätsstatistiken belegen. Vor allem auch gut organisierte transnationale Mafiastrukturen

20 | Vgl. Bruce Averill und Eric A.M. Luiijf, „Canvassing the Cyber Security Landscape: Why Energy Companies Need to Pay Attention“, *Journal of Energy Security*, 18.05.2010, 1, http://ensec.org/index.php?option=com_content&view=article&id=243 [24.07.2012].

dürften zukünftig nicht nur ein Interesse am Diebstahl von Kundendaten haben, sondern nicht zuletzt ein zunehmendes Interesse an Industriespionage und Erpressung von Unternehmen entwickeln.

- Die unzähligen neuen Sicherheitsrisiken sind das Ergebnis der Verbreitung von Informations- und Kommunikationstechnologien (ICT), die in den kommenden Jahren ebenso dramatisch zunehmen werden wie die weltweite Informationsflut. Dies wird auch die Vernetzung der Informations- und Kommunikationsstrukturen weiter erhöhen und damit zusätzliche Sicherheitsrisiken schaffen.

- Die Marktliberalisierung und die Privatisierung ehemals staatlicher Infrastrukturbetreiber sowie neue Regelungen haben die Privatindustrie und staatliche Agenturen immer abhängiger von externen Zulieferern für Güter und Dienstleistungen gemacht. Gleichzeitig wurde aus finanziellem Kosten- und Konkurrenzdruck die Entwicklung von spezifischer Software ausschließlich für die Industrie aufgegeben und stattdessen durch auf dem Markt befindliche kommerzielle Produkte aus dem Regal (COTS) ersetzt.

- Fast jede einzelne Dienstleistung hängt direkt oder indirekt von einer sicheren Stromversorgung ab. Die physischen, virtuellen und logischen Netzwerke sind in Größe und Komplexität gewaltig gewachsen. Als Ergebnis der wachsenden gegenseitigen Abhängigkeit verschiedener kritischer Infrastrukturen sind die Abhängigkeit und die Folgen von Versorgungsengpässen und Versorgungsunterbrechungen meist nicht offensichtlich, solange keine Krise eintritt und die Versorgung nicht völlig zusammenbricht. Doch bereits kleinere Stromschwankungen, Ausfälle und Unterbrechungen können dramatische Auswirkungen haben, die in immer komplexeren Systemen nicht vorausgesehen werden können.

- Die Allgegenwärtigkeit der Bedrohung und die Effektivität von Cyberangriffen gelten inzwischen als die neue fünfte Front der Kriegsführung nach Land, Wasser, Luft und Weltraum. Sie sind eine neue, nie dagewesene Herausforderung für die internationale Staatengemeinschaft in einer sich ohnehin rasch verändernden globalen Sicher-

heitslage.[21] Diese Gefahren stellen auch die traditionellen Vorstellungen und Ideen von nationaler und kollektiver Sicherheit sowie Verteidigung zunehmend in Frage. Die neue Ära des Cyberkriegs wird bereits mit historischen Technologiesprüngen wie dem ersten Einsatz des Schießpulvers, der Erfindung des Panzers oder dem Abwurf der ersten Atombombe in Hiroshima verglichen.[22]

Dabei gilt die Gefahr eines „digitalen Pearl Harbor" im 21. Jahrhundert inzwischen als real und ist nicht mehr länger nur ein Konzept der Science-Fiction, da die Grenzen zwischen Cyberkriminalität, Cyberterrorismus und einem von Privaten oder von Staaten unterstützten Cyberkrieg als eine neue Form einer „asymmetrischen Kriegführung" zunehmend fließend sind. Bereits 2008 hatte das World Economic Forum gewarnt, dass eine zehn- bis 20-prozentige Wahrscheinlichkeit eines großflächigen Zusammenbruchs der CII in den nächsten zehn Jahren bestehe und dieser einen weltweiten ökonomischen Schaden von 250 Milliarden US-Dollar verursachen könne.[23] US-Experten warnten inzwischen vor einem erfolgreichen Cyberangriff auf die amerikanische Stromversorgung, der ökonomische Kosten von 700 Milliarden US-Dollar hervorrufen könne, und verglichen diesen mit einem gleichzeitigen Einschlag von 40 bis 50 großen Hurricanes: „Einen derart großen wirtschaftlichen Schaden hat eine moderne Wirtschaft noch nicht erlebt. […] Er ist größer als die Große Depression. […] Er ist größer als der Schaden, den unsere strategischen Bomben während des Zweiten Weltkriegs in Deutschland ausgelöst haben."[24]

US-Experten warnten vor einem erfolgreichen Cyberangriff auf die amerikanische Stromversorgung und verglichen diesen mit einem gleichzeitigen Einschlag von 40 bis 50 großen Hurricanes.

21 | Vgl. auch Joachim Zeppelin, „Schutz im unsichtbaren Cyberkrieg", *Financial Times Deutschland*, 11.06.2012, 25.
22 | Clemens Wergin, „Der Krieg der Zukunft", *Die Welt*, 02.06.2012, 1.
23 | Vgl. Commission of the European Communities, „Protecting Europe from Large-Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience", SEC(2009)399/SEC(2009)400, Brüssel, 30.03.2009, COM(2009)149 final, 2.
24 | So Scott Borg, Chief Economist at US Cyber Consequences Unit, ein privater gemeinnütziger Thinktank, zitiert in: J.N. Gordes und M. Myirea, „A New Security Paradigm Is Needed to Protect Critical US Energy Infrastructure from Cyberwarfare", *Foreign Policy Journal*, 14.09.2009.

Russische Hacker sind nachweislich schon im Mai 2008 in das System eines Atomkraftwerks nahe St. Petersburg eingedrungen. Die Funktion des Kraftwerks wurde durch den Einbruch zwar nicht beeinflusst. Es wurden jedoch Gerüchte bekannt – möglicherweise absichtlich verbreitet –, dass Radioaktivität aus dem Kraftwerk ausgetreten sei. Für einige Stunden soll auch die Kommunikation zwischen dem Kraftwerk und dem Kraftwerks betreiber Rosatom gestört gewesen sein.[25]

Tabelle 2
Staatlich finanzierte und unterstützte Cyberangriffe

Estland: April-Mai 2007
Litauen: Juni-Juli 2008
Georgien: Juli-August 2008
Südkorea und USA: Juli 2009 (in Südkorea wurden 12.000 Computer angegriffen und 8.000 in anderen Ländern; der Angriff ging von Nordkorea aus)
Großbritannien 2006: verantwortlich für die Abschaltung des Computersystems des Britischen Parlaments und 2007 Angriffe auf das Netzwerk des Britischen Außenministeriums und anderer wichtiger Abteilungen
Indien: Angriffe auf Ministerien, Telekommunikationszentren/-unternehmen; Streitkräfte und militärische Einrichtungen, Botschaften und Konsulate; verschlüsselte diplomatische Kommunikation und das Sekretariat des Nationalen Sicherheitsrates.
Niederlande: DigiNotar, das Privatunternehmen der niederländischen Regierung, zuständig für die Authentifizierungszertifikate der staatlichen Webseiten
USA: die Computer im Pentagon werden 250.000 Mal in einer Stunde abgetastet, bis zu sechs Millionen Mal pro Tag.
Die NATO hatte 2010 auf täglicher Basis mit hunderten bösartigen Cyber-Vorfällen zu tun.
April 2012: Mehr als 600.000 Apple-Computer, die bisher als wesentlich sicherer und weniger anfällig als mit Windows-Software betriebene Rechner galten, wurden mit dem Flashback-Trojaner infiziert.

Beunruhigend ist auch die Tatsache, dass Hacker Anfang 2010 und 2011 auch auf dem Europäischen Markt für CO_2-Emissionszertifikate (ETS) zuschlugen und damit einmal

25 | Vgl. „How Vulnerable are Energy Facilities to Cyber Attacks“, *Intelligence Report*, Securing America's Future Energy (SAFE), Washington DC, Jg. 3, Nr. 1, 20.01.2010, 2, http://secure energy.org [23.07.2012]; Averill und Luiijf, Fn. 19, 2.

mehr das Potenzial von Cyberangriffen demonstrierten, um Marktpreise zu manipulieren und zu beeinflussen, wer Energieverträge abschließen kann. Mehr als zwei Millionen Zertifikate, die allerdings nur 0,02 Prozent der Gesamtzertifikate ausmachten, sollen nach dem Angriff im Januar 2011 illegal auf bestimmte Konten transferiert worden sein. Bereits zuvor war der Europäische Emissionsrechtehandel vorübergehend geschlossen worden, nachdem zunächst 475.000 CO_2-Zertifikate bei einem Hacker-Angriff auf das tschechische Emissionsregister gestohlen worden waren. Auch andere Plattformen wie die France Bluenext Exchange waren gezwungen, zu schließen. Österreich, Polen, Estland und Griechenland sperrten ebenfalls ihre entsprechenden Handelsregister. Die Verluste wurden mit mehr als fünf Milliarden Euro beziffert. Noch weitaus problematischer ist jedoch die dadurch untergrabene Glaubwürdigkeit des Emissionsrechtehandels als das derzeit wichtigste Instrument zur Reduzierung des Schadstoffausstoßes in Europa.[26]

Der Europäische Emissionsrechtehandel war vorübergehend geschlossen worden, nachdem 475.000 CO_2-Zertifikate bei einem Hacker-Angriff auf das tschechische Emissionsregister gestohlen worden waren.

Auch Manipulationen wie diese können zu Unterbrechungen der Energieversorgung und Stromausfällen führen. So funktionieren der Energie-Spotmarkt und andere Handelsplätze auf dem Energiemarkt, wie z.B. die Amsterdam Power Exchange (APX), Paris Powernext und die European Energy eXchange (EEX) in Deutschland, alle über das normale Internet und sind somit dem Risiko externer Computermanipulation ausgesetzt.[27] Dies zeigte sich im Februar 2011, als die Nasdaq Stock Exchange in New York ebenfalls Opfer eines Cyberangriffes wurde, wenngleich die Hacker jedoch nicht in das zentrale Handelssystem eindringen konnten. Dennoch verdeutlichten diese Beispiele die potenzielle Verwundbarkeit von Börsen, die inzwischen zumeist vollkommen computerisiert sind.[28]

26 | Vgl. European Commission, „Emissions Trading: Q & As Following the Suspension of Transactions in National ETS Registries for at least One Week from 19:00CET on Wednesday 19 January 2011“, Brüssel, 21.01.2011; Michael Gassmann, „Emissionsstelle dichtet Sicherheitslecks ab“, *Financial Times Deutschland*, 23.02.2010, 5; Averill und Luiijf, Fn. 19, 4.

27 | Vgl. Rowena Mason, „European Carbon Market Suspended over Frauds“, *The Telegraph*, 19.01.2011.

28 | Vgl. Graham Bowley, „Hackers Gained Access to Nasdaq Systems, but not Trades“, *The New York Times*, 05.02.2011.

Tabelle 3
Auswahl jüngerer Cybercrime-Angriffe

Angriffsziel	Jahr	
Internationaler Währungsfonds (IMF)	2011	Großer und durchdachter Angriff auf eine Datenbank, die potenzielle marktbeeinflussende Informationen enthält, inklusive geheimer internationaler Hilfsmaßnahmen.
Citigroup	2011	Hacker eigneten sich Datensätze von 200.000 Kreditnehmern mit Adressen, Passwörtern usw. an.
Dropbox	2011	Ein beliebter Service, um Dokumente und andere Daten in einer Computing Cloud zu speichern.
Comodo Group	2011	Internet-Sicherheitsfirma, die Zertifikate für die Authentizität von Webseiten für Browser zur Verfügung stellt, die von Google, Yahoo, Microsoft, Skype und Mozilla betrieben werden (mehr als 676 Organisationen lassen hier zertifizieren).
Nasdaq Stock Exchange, New York	2011	Einbruch, aber kein Eindringen in das System, das den Handel abwickelt.
Lockheed Martin	2010/2011	Industriespionage (aus China).
MasterCard, Visa und PayPal	2010	Eine lose Gruppe von Hackern aus aller Welt erklärte MasterCard, Visa und PayPal den Cyberkrieg, weil diese ablehnten, Spenden an Wikileaks weiterzuleiten.
Google	2009/2010	Google und 30 weitere High-Tech-Unternehmen in den USA.
Sony Webseite		Persönliche Informationen wie Kennwörter, E-Mail-Adressen und Postadressen von über 52.000 Kunden wurden gestohlen.
RSA Security	2010	RSA Security konzipiert Kennwörter für große Unternehmen, damit sie sich vor Eindringlingen schützen können.
Energieindustrie, Großbritannien	2009	Night-Dragon-Angriffe auf die Energieindustrie, die mehr als 30 Milliarden Euro an Kosten verursacht haben sollen. Sie sollen von China aus seit November 2009 erfolgt sein.

AMERIKANISCHE LEHREN – DIE INTERNATIONALEN DIMENSIONEN

Während in Großbritannien 2009 ein finanzieller Schaden von 30 Milliarden Euro als Folge der Cyberangriffe beziffert wurde, sollen die USA nach Angaben des US-Präsidenten Barack Obama im gleichen Jahr sogar rund eine Billion US-Dollar als Folge von Cyberkriminalität verloren haben. Daraufhin verkündete die US-Regierung ein digitales Verteidigungsprogramm im Wert von 17 Milliarden

US-Dollar und ernannte Howard A. Schmidt, einen lang gedienten Computerspezialisten, zum Beauftragten des Weißen Hauses, der die Anstrengungen zur Verteidigung gegen Cyberkriegskapazitäten koordinieren soll. Im Jahr 2009 wurde auch das US Cyber Command (USCYBERCOM) geschaffen, das vom Vier-Sterne-General Keith Alexander geführt wird. Im Juli 2011 stellte das US-Verteidigungsministerium schließlich die lang erwartete Strategy for Operating in Cyberspace vor, die warnte: „Unsere Abhängigkeit vom Cyberspace steht in einem großen Gegensatz zur Unzulänglichkeit unserer Cyber-Security."[29] Auch Beamte im Pentagon mussten inzwischen zugegeben, dass selbst ihre geschützten Intranets, die vom normalen Internet weitgehend getrennt sind, vor Cyberangriffen nicht immun sind.

General Keith Alexander, Direktor der NSA und Leiter des US Cyber Command, bei einer Veranstaltung des Center for Strategic and International Studies (CSIS) im Jahr 2010. | Quelle: CSIS (CC BY-NC-SA).

Das Verteidigungsprogramm der US-Regierung gegen Cyberangriffe war wesentlich die unmittelbare Folge des Angriffs auf die weltweit bekannteste Suchmaschinenfirma Google. Chinesische Hacker hatten in großem Umfang geistiges Eigentum und sensible Kundendaten von Google gestohlen (Operation Aurora). Doch wie sich in den folgenden Monaten herausstellen sollte, war der Angriff auf Google nur die Spitze des Eisbergs. Insgesamt wurden 30 weitere amerikanische High-Tech-Firmen (wie z.B. Adobe oder Cisco Systems) aus China angegriffen. Diese Angriffe

29 | Department of Defense, „Strategy for Operating in Cyberspace", Washington DC, 07/2011.

beschleunigten ein ohnehin im Prozess befindliches strategisches Umdenken und einen Paradigmenwechsel bezüglich der Cybersicherheit in den USA. Chinesische Cyberangriffe wurden nun als derart aggressiv und alles durchdringend wahrgenommen, dass nun US-Firmen von ihrer Regierung verlangten, starken politischen Druck auf China auszuüben, während sie davor bisher eher gewarnt hatten, um den Zugang zum chinesischen Wachstumsmarkt oder größere Geschäftsanteile nicht zu verlieren. Als Google auch nach dreimonatigen internen Recherchen nicht feststellen konnte, wie viele sensible Informationen ausgespäht und gestohlen worden waren, hatte das Unternehmen keine andere Wahl, als sich an die National Security Agency (NSA) zu wenden.[30]

Das GhostNet-System ist ein Cyberspionagesystem, das von einem Server in China aus in mehr als 1.300 Computer in staatlichen Behörden, Botschaften, internationalen Organisationen, und Medienunternehmen eingedrungen war.

Bereits zuvor war im gleichen Jahr durch ein kanadisches Universitätsinstitut das so genannte GhostNet-System aufgedeckt worden. Dieses ist ein automatisches Cyberspionagesystem, das von einem Server in China aus in mehr als 1.300 Computer in 103 Ländern eingedrungen war. Darunter waren auch zahlreiche Rechner in staatlichen Behörden, Botschaften, internationalen Organisationen, NGOs und Medienunternehmen. Das Spionagesystem durchsuchte weltweit die Computer nicht nur nach Informationen und kopierte E-Mails, sondern verwandelte sich auch in eine gigantische Abhöranlage. Viele amerikanische Unternehmen, auch aus der digitalen Wirtschaft, hatten bis zur Aufdeckung des „GhostNet"-Systems nicht einmal bemerkt, dass sie angegriffen worden waren, und fühlten sich daher bis zur Aufdeckung durch die NSA völlig sicher. Diese ausgeklügelten Computerangriffe aus China waren von beispielloser zerstörerischer Wirksamkeit. Für internationale Sicherheitsexperten sind derartige offensive Cyberangriffe nur mit staatlicher Unterstützung möglich. Und nur wenige Organisationen außerhalb des Verteidigungs- und Geheimdienstsektors können ihnen standhalten.[31]

30 | Vgl. auch John Markoff, „Cyberattack on Google Said to Hit Password System", *The New York Times*, 19.04.2010, http://nytimes.com/2010/04/20/technology/20google.html [23.07.2012].

31 | Vgl. auch Malcolm Moore, „China GloblCyber-Espionage Network GhostNet Penetrates 103 Countries", *Telegraph*, 29.03.2009; Kathrin Hille und Joseph Menn, „Hackers in Frontline of China's Cyberwar", *Financial Times*, 13.01.2010.

Im November 2011 kam eine gemeinsame Untersuchung von 14 US-Geheimdiensten für den US-Kongress zum Ergebnis, dass China und Russland führend beim staatlich unterstützten Internetdiebstahl von ökonomischen Geheimnissen und Technologien seien.[32] Das FBI konnte 2009 allein aus China mehr als 90.000 Cyberangriffe auf das Pentagon nachweisen. Chinesische Hacker wurden auch für das zeitweise Abschalten des Computersystems des British House of Commons 2006 verantwortlich gemacht.[33] Westliche Geheimdienstquellen gehen von mehr als 500.000 Hackern aus, die gewillt sind, an Cyberangriffen und -spionage teilzunehmen.[34] In einem journalistischen Insiderbericht von 2007 heißt es, zahlreiche chinesische Hackergruppierungen arbeiteten „freiberuflich" sowohl für die chinesische Regierung als auch für deren Geheimdienste und die Industrie, die untereinander über ein enges Beziehungsgeflecht verfügen und durch einen Mix aus Nationalismus, technischem Ehrgeiz und finanziellen Interessen sowie persönlichem Ruhmesstreben motiviert sind.[35] Während die chinesische Regierung offiziell alle chinesischen Cyberangriffe in Abrede stellt und die eigenen Cyberkriegführungsstrategien als ausschließlich defensiv bewertet, weisen chinesische Experten darauf hin, dass auch in China die Cyberkriminalität stark zunimmt, zunehmend professioneller wird und immer besser organisiert ist.[36]

32 | Vgl. Thom Shanker, „U.S. Report Accuses China and Russia of Internet Spying", *The New York Times*, 03.11.2011; „Chinese cyberspies stealing key data, U.S. analysts say", *CBC news*, 12.12.2011, http://cbc.ca/news/technology/story/2011/12/12/china-hackers-us.html [23.07.2012].

33 | Vgl. auch Duncan Gardham, „‚Al-Qaeda, China and Russia, pose cyber war threat to Britain', warns Lord West", *Telegraph*, 25.06.2009, http://telegraph.co.uk/news/uknews/law-and-order/5634820/Al-Qaeda-China-and-Russia-pose-cyber-war-threat-to-Britain-warns-Lord-West.html [23.07.2012].

34 | Vgl. David Barboza, „Hacking for Fun and Profit in China's Underworld", *The New York Times*, 02.02.2010, http://nytimes.com/2010/02/02/business/global/02hacker.html [23.07.2012]; S. Nandan Andey, „Red Guests. Hacktivism of Chinese Characteristics and the Google Inc. Cyber Atack Episode", *Denkwürdigkeiten*, PMG e.V., Nr. 63, 04/2010.

35 | Vgl. Scott Henderson, „The Dark Visitor. Inside the World of Chinese Hackers", 10/2007.

36 | Vgl. Kathrin Hille, „Chinese Military Mobilises Cybermilitias", *Financial Times*, 12.10.2011, http://www.ft.com/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html [23.07.2012].

Im November 2009 wurden zudem neue verdeckte, aber gut koordinierte und zielgerichtete chinesische Cyberangriffe gegen weltweit tätige Unternehmen in den Bereichen Energie und Petrochemie bekannt. Die so genannten Night Dragon-Operationen hatten auch Remote Administration Tools (RATs) benutzt, die zielgerichtet sensitive Informationen zu Eigentumsfragen und projektbezogenen Finanzierungen für den Kauf von Öl- und Gasfeldern der westlichen Energieunternehmen gestohlen haben.[37] Wie zahlreiche WikiLeaks-Dokumente beweisen, können derartige Cyberangriffe von halbunabhängigen chinesischen Hackergruppierungen wie die Patriotic Hackers oder die Honker Union bis ins Jahr 2002 zurückgeführt werden. Zudem sollen zumindest einzelne chinesische Politbüromitglieder derartige Cyberangriffe auf westliche Regierungen und Unternehmen offenbar ausdrücklich und kontinuierlich unterstützt haben. Doch hätten weder die USA noch die EU Beijing jemals ausdrücklich zur Rede gestellt, um die ohnehin nicht konfliktfreien bilateralen Beziehungen nicht zusätzlich zu belasten, zumal sie die Kooperation Chinas auf vielen anderen Feldern benötigten.[38] Zugleich zeigt sich die chinesische Regierung aber auch zunehmend besorgt über Cyberangriffe auf ihre eigenen Computernetzwerke sowie zunehmende Angriffe auf die schnell expandierenden Öl- und Gaspipelines sowie Stromnetze.[39]

Weder die USA noch die EU haben Beijing jemals ausdrücklich zur Rede gestellt, um die ohnehin nicht konfliktfreien bilateralen Beziehungen nicht zusätzlich zu belasten.

In den USA wird die industrielle Cyberspionage nach den deprimierenden Erfahrungen der letzten Jahre inzwischen als größtes Aufklärungsdesaster seit dem Verlust der nuklearen Geheimnisse Ende der 1940er Jahre gewertet. Wie der *Economist* 2010 feststellte: „A spy might once have

37 | Vgl. McAfee, „Global Energy Cyberattacks: ‚Night Dragon'". White Paper, Santa Clara, 10.02.2011.

38 | Vgl. Joseph Mann, „US Fears Beijing Still Backs Hacking", *Financial Times*, 05.12.2010, http://www.ft.com/cms/s/0/9a0eabc2-0016-11e0-ad1d-00144feab49a.html [23.07.2012]; Ellen Nakashima und William Wan, „China's Denials about Cyberattacks Undermined by Video Clip", *Washington Post*, 24.08.2011, http://washingtonpost.com/world/national-security/state-media-video-candidly-depicts-chinas-developing-cyber-weaponry/2011/08/22/gIQAqyWkbJ_story.html [23.07.2012].

39 | Vgl. Xin Dingding und Wan Zhihong, „China Faces New Risk: Attacks on Pipelines' and Gabe Collins, Smart Moves – China Secures Energy Infrastructure", *Jane's Intelligence Review*, 16.09.2010.

been able to take out a few books' worth of material, now they take the whole library. And if you restock the shelves, they will steal it again."[40] Vor diesem Hintergrund ist eine Eliminierung der Bedrohung unrealistisch. Der Schutz zur Aufrechterhaltung der Geschäftsoperationen und betrieblicher Produktionsprozesse für Wachstum und Innovation wird zum obersten Gebot und zu einer Top-Management-Aufgabe in den kommenden Jahren und Jahrzehnten.[41] Die gegenwärtige Situation der Überlegenheit des Angreifers gegenüber dem Verteidiger erklärt sich auch aus dem Umstand, dass das organisierte Verbrechen eine bessere Finanzierung aufweist, da zahlreiche Unternehmen kaum bereit sind, ausreichend Gelder für entsprechenden Schutz und Sicherheit aufzuwenden, wie zahlreiche Interviewumfragen und Expertenanalysen auch in jüngster Zeit zeigen: „Unternehmer haben oftmals zu wenig Kenntnis über IT-Sicherheitsrisiken und die notwendigen Maßnahmen, um die Kosten für Investment, Risiken und Käuferverhalten gegeneinander abzuwägen."[42]

Die Überlegenheit des Angreifers erklärt sich auch aus dem Umstand, dass das organisierte Verbrechen eine bessere Finanzierung aufweist. Zahlreiche Unternehmen sind kaum bereit, ausreichend Gelder für Sicherheit aufzuwenden.

Demnach werden die Sicherheitsherausforderungen und -risiken auf Seiten vieler Unternehmen trotz einer zunehmenden medialen Berichterstattung noch immer unterschätzt. Bezeichnenderweise wurde in einer neuen Analyse der US-Sicherheitsfirma McAffee von 2011 nur noch zwischen Unternehmen unterschieden, welche die Angriffe erkannt hätten, und solchen, die bis zuletzt von Angriffen auf ihre Unternehmen nichts wussten.[43] In einer weiteren Analyse von Ende 2011, die eine Art Jahresbilanz der Auswertung von weltweiten Cyberangriffen war, wurde erneut bestätigt, dass sich auch 2011 die Bedrohungen und Verwundbarkeiten angesichts einer weltweiten Steigerung von 77 auf 82 gezielte größere Spionageangriffe weiter erhöht

40 | Vgl. *The Economist*, 03.07.2010 [ARTIKELNAME?].
41 | James Kaplan, Allen Weinberg und Shantu Sharma, „Meeting the Cybersecurity Challenge", *McKinsey Quarterly*, 06/2011, 1.
42 | Ebd., 3.
43 | Vgl. Dmitri Alperovitch, „Revealed: Operation Shady RAT. An Investigation of Targeted Intrusions into 70+ Global Companies, Governments and Non-Profit Organizations during the last 5 Years", McAfee-White Paper, 2011.

hatten.[44] Im Oktober 2011 enthüllte eine Studie der Sicherheitsfirma Symantec weltweit mindestens 48 koordinierte Angriffe auf Chemie- und Verteidigungsfirmen, vor allem in den USA und Großbritannien.[45]

Besonders beunruhigen müsste allerdings die im Februar 2012 bekannt gewordene Tatsache, dass der inzwischen bankrotte amerikanische Netzwerkausrüster Nortel über zehn Jahre unbemerkt ausgespäht worden war, nachdem die Angreifer die Passwörter von hochrangigen Führungskräften des Unternehmens gekapert hatten. So konnten alle E-Mails, Forschungsberichte, technischen Dokumentationen, vertraulichen Dokumente und Geschäftsberichte gelesen werden.[46]

STUXNET UND FLAME – IST DER RUBIKON ÜBERSCHRITTEN?

„Was Stuxnet vor allem so weltbewegend werden lässt, ist die Tatsache, dass er entwickelt wurde, um einen noch nie da gewesenen Schritt von der digitalen in die physikalische Welt zu machen. Stuxnet hat die Art und Weise, wie Forscher mit Schadprogrammen umgehen und wie sie Sicherheitsrisiken einschätzen, verändert."[47] Der ursprüngliche Stuxnet-Computerwurm, der im Juli 2010 entdeckt wurde, infizierte mehr als 60.000 Computer weltweit. Im Gegensatz zu Viren verbreiten sich Würmer selbstständig. Sie haben die Viren in den letzten Jahren zunehmend ersetzt. Stuxnet zielte jedoch auf die iranischen Urananreicherungsanlagen und das Siemens-Steuerungssystem Simatic in Natanz, die im Sommer 2010 sabotiert

Im Gegensatz zu Viren verbreiten sich Würmer wie Stuxnet selbstständig. Sie haben die Viren in den letzten Jahren zunehmend ersetzt.

44 | Vgl. Stewart Baker, Natalia Filipiak und Katrina Timlin, „In the Dark: Crucial Industries Confront Cyberattacks", *Second Annual Critical Infrastructure Report*, McAffee und CSIS, Washington DC/Santa Clara, 2011.

45 | Vgl. Eric Chien und Gavin O'Gorman, „The Nitro Attacks. Stealing Secrets from the Chemical Industry", Symantec-White Paper, 10/2011.

46 | Vgl. Annika Graf, „Hacker spähten Nortel zehn Jahre lang aus", *Financial Times Deutschland*, 15.02.2012, 8; Benedikt Fuerst, „Hacker hatten Zugang zu allem", *Die Welt*, 15.02.2012, 12.

47 | So die Sicherheitssoftwarefirma Symantec, „The Stuxnet Worm", http://www.symantec.com/business/outbreak/id==stuxnet [18.10.2011].

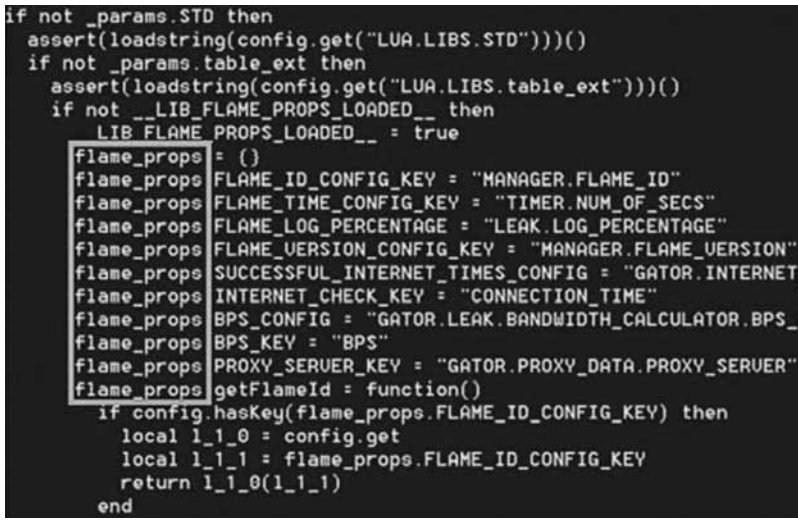
wurden.[48] Nur durch den Zufall, dass der Stuxnet-Virus, durch einen USB-Stick im Iran übertragen, unbeabsichtigt ins Internet gelangte, war er überhaupt bekannt geworden. Für viele Cyberexperten kam die Entdeckung des „digitalen Erstschlags" einem Schock gleich, galten doch derartig hochkomplizierte Virenprogramme mit dem Ziel, industrielle Steuerungs- und Kontrollzentren anzugreifen, bis dahin als eine ferne zukünftige Option. Nun aber erscheinen auch Angriffe auf zahlreiche kritische Infrastrukturen, einschließlich Energiekontrollzentren, weitaus realistischer. Der Vorstandsvorsitzende und Gründer von Kaspersky Lab, Eugene Kaspersky, bezeichnete den Stuxnet-Wurm als einen „neuen Prototyp zukünftiger Cyberwaffen".[49] Andere Experten fürchten, dass diese neue „Präzisionscyberwaffe" einen neuen Rüstungswettlauf auslösen werde.[50] Aufgrund seiner Komplexität wurden sofort die Geheimdienste der USA und Israels verdächtigt, den „Wurm aller Würmer" entwickelt zu haben.[51]

48 | Vgl. John Markoff, „Worm Can Deal Double Blow to Nuclear Program", *The New York Times*, 19.11.2010, http://nytimes.com/2010/11/20/world/middleeast/20stuxnet.html [23.07.2012]; Najmeh Bozorgmehrin, „Web Virus Aimed at Nuclear Work, Says Teheran", *The New York Times*, 27.09.2010; John Markoff und David E. Sanger, „In a Computer Worm, a Possible Biblical Clue", *The New York Times*, 29.09.2010, http://nytimes.com/2010/09/30/world/middleeast/30worm.html [23.07.2012]; William J. Broad, John Markoff und David E.Sanger, „Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *The New York Times*, 15.01.2011; David E. Sanger, „Iran Fights Malware Attacking Computers", *The New York Times*, 25.09.2010; William J. Borad und David E. Sanger, „Worm was Perfect for Sabotaging Centrifuges", *The New York Times*, 18.11.2010, http://nytimes.com/2010/11/19/world/middleeast/19stuxnet.html [23.07.2012]; Sandro Gaycken, „Wer war's? Und wozu?", *Die Zeit*, 25.11.2011, 31; Alard von Kittlitz, „Stuxnet und der Krieg, der kommt", *Frankfurter Allgemeine Zeitung*, 04.12.2010, 33.

49 | Vgl. „Stuxnet-Wurm befällt iranisches Atomkraftwerk", *Welt-Online*, 26.09.2010, http://welt.de/wirtschaft/webwelt/article9884891/Stuxnet-Wurm-befaellt-iranisches-Atomkraftwerk.html [23.07.2012].

50 | Vgl. Michael Schrage, „Stuxnet Was about What Happened Next", *Financial Times*, 16.02.2011, http://ft.com/cms/s/0/c8142b5a-3a04-11e0-a441-00144feabdc0.html [23.07.2012].

51 | Vgl. William J. Broad, „Report Suggests Problems with Iran's Nuclear Effort", *The New York Times*, 23.11.2010, http://nytimes.com/2010/11/24/world/middleeast/24nuke.html [23.07.12]; John Markoff, „Worm Can Deal Double Blow to Nuclear Programme and Ari Rusila, Cyber War Has Become a Tool between Political and Military Options", *Europe's World*, 19.01.2011.



```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
      __LIB_FLAME_PROPS_LOADED__ = true
      flame_props = {}
      flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_C
      flame_props.BPS_KEY = "BPS"
      flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
```

Zunächst im Einsatz gegen den Iran, hat sich der Flame-Virus inzwischen erheblich verbreitet. | Quelle: AFP (CC BY-NC-SA).

Obwohl viele Experten und die Medien den Stuxnet-Wurm als das fortgeschrittenste Computerprogramm beschrieben, um in ferne industrielle Steuerungssysteme einzudringen, die Kontrolle über sie zu erlangen und Stromzufuhr sowie Geschwindigkeit von Gaszentrifugen in quasi autonomer Weise regeln zu können, scheint er doch weniger fortgeschritten und ausgeklügelt zu sein als ursprünglich angenommen, wie neuere Untersuchungen belegen.[52] Zudem konnte er im Iran nur 1.000 der 5.000 Zentrifugen temporär schädigen. Insofern war auch die Stuxnet-Waffe nur bedingt erfolgreich und konnte das vermutete Nuklearwaffenprogramm Irans nur verlangsamen.[53]

Dennoch veränderte der Stuxnet-Wurm die Einschätzung der Bedrohung von Industrie und Staat, weil er speziell dafür geschaffen worden war, Industriekontrollsysteme zu sabotieren. Die Sicherheitssysteme der SCADA-Systeme (Supervisory Control and Data Acquisition Systems) als eigentliche Industriekontrollysysteme von großen und komplexen kritischen Infrastrukturen, liegen jedoch genau wie die der Informations- und Kontrollzentren im Vergleich zur

52 | Vgl. James P. Farwell und Rafal Rohozinski, „Stuxnet and the Future of Cyber War", *Survival*, 02-03/2011, 23-40.

53 | Vgl. auch William J. Broad, „Report Suggests Problems with Iran's Nuclear Effort", *Medium?*, 23.11.2010; Markoff, Fn. 51.

Sicherheit von Laptops oder Desktops etwa fünf bis zehn Jahre zurück.[54] Im August 2011 demonstrierte ein Wissenschaftler auf einer Sicherheitskonferenz, wie leicht er in industrielle Computeranlagen für automatisierte Kontrollprozesse von Siemens-Anlagen trotz Passwortschutzsystemen auch mit einem weniger komplizierten und fortschrittlichen Wurm einbrechen konnte.[55]

Im Oktober 2011 entdeckte ein ungarisches Forschungsinstitut der Budapester Universität für Technologie und Wirtschaft per Zufall einen neuen und ähnlich gefährlichen Wurm, der Duqu genannt wurde und als eine Art Vorgänger für zukünftige Stuxnet-vergleichbare Angriffe eingestuft wurde. Eigentlich waren die Forscher auf der Suche nach einem anderen gefährlichen Wurm (Wiper genannt), den weder sie noch andere Experten bisher finden konnten. Der Flame-Wurm war offenbar von demselben Forschungsteam wie der Stuxnet-Wurm entwickelt worden, um umfangreiche Aufklärungsinformationen über industrielle Einrichtungen, Infrastrukturen und deren SCADA-Systeme zu sammeln, die später für einen erfolgreichen Angriff entscheidend sein können.[56]

Die Entdeckung des noch komplizierteren und gegenüber Stuxnet 20-mal größeren Flame-Virus hat die besorgniserregende Entwicklung staatlich geförderter offensiver Cyberwaffen noch einmal unterstrichen. Flame ist im Gegensatz zu Stuxnet primär eher ein allumfassendes Spionageprogramm, das nicht nur Daten kopiert, sondern als eine Art Audio-Spion auch selbständig Mikrofone von fremden Computern und vernetzten Smartphones einschalten, die Gespräche mitschneiden und dann sofort an die Server der Viren-Urhebern abschicken kann. Da auch dieser Wurm

54 | Vgl. auch Uwe Nerlich und Frank Umbach, „European Energy Infrastructure Protection: Addressing the Cyberwarfare Threat", *Journal of Energy Security*, 27.10.2009, 8, http://ensec.org/index.php?option=com_content&view=article&id=219 [23.07.2012].

55 | Vgl. Joseph Mann, „US Regulators War Utilities over Cyber Attacks", *Financial Times*, 07.08.2011, http://ft.com/intl/cms/s/2/78f94f14-bec0-11e0-a36b-00144feabdc0.html [23.07.2012].

56 | Vgl. Symantec, „W32.Duqu. The Precursor to the Next Stuxnet, Version 1.4", 23.11.2011; John Markoff, „New Malicious Program by Creators of Stuxnet Is Suspected", *The New York Times*, 18.10.2011, http://nytimes.com/2011/10/19/technology/stuxnet-computer-worms-creators-may-be-active-again.html [23.07.2012].

gegen den Iran eingesetzt wurde, die Programmiersprache und die Software-Architektur aber eine andere ist, spricht einiges dafür, dass er ebenfalls in den USA entwickelt wurde. Durch ein herunterladbares Zusatzmodul lässt sich Flame allerdings auch schnell in eine Malware verwandeln, die dann auch physische Schäden an Industrieanlagen anrichten kann.[57]

STEIGENDE ABHÄNGIGKEITEN UND VERWUNDBARKEITEN BEI DEN ENERGIEINFRASTRUKTUREN

Früher war die Energieversorgung dezentralisiert, mit einem Kraftwerk für jede Region und einem lokalen Verteilungsnetzwerk, das die Produzenten mit den Konsumenten verband. Fiel das Kraftwerk aus, war die ganze Region von einem Stromausfall betroffen. Als dann die Regionalnetze durch interregionale Übertragungsnetze verbunden wurden, verbesserte sich die Versorgungssicherheit nachhaltig, weil nun die Möglichkeit bestand, Energie zwischen regionalen Netzwerken auszutauschen. Dies sparte zugleich finanzielle Ressourcen, besonders auf Seiten der Produzenten.

Heute haben sich diese regionalen Netzwerke auf ganze Länder ausgedehnt, und die einzelnen EU-Mitgliedstaaten sind wiederum miteinander verbunden, um so einen liberalisierten, gemeinsamen Energiemarkt für die EU-27 zu schaffen (früher UCTE, heute ENTSO-E). Aus dieser Verknüpfung zur Stärkung der Energieversorgungssicherheit der Mitgliedstaaten resultiert jedoch auch eine immer stärkere Abhängigkeit von der Robustheit und Stabilität der Elektrizitätsnetze der Partner. Das gemeinsame europäische Versorgungs- und Verteilungssystem ist demnach nur so stark wie sein schwächstes Glied.[58] Werden die

57 | Vgl. Michael Borgstede, „Ein Virus nach dem Baukastenprinzip; ‚Der Feind am Ende der Leitung hört mit'. Interview mit Alexander Gostew, Chef-Experte des Antiviren-Unternehmens Kaspersky Lab", *ebd.* (?); Annika Graf und Joachim Zepelin, „Neuer Computerschädling eifert Stuxnet nach", *Financial Times Deutschland*, 30.05.2012, 7; Annika Graf und Lukas Heiny, „Da ist der Wurm drin", *Financial Times Deutschland*, 07.06.2012, 23, http://ftd.de/it-medien/medien-internet/70047098.html [24.07.2012].

58 | Vgl. auch Alexander Bakst, „The Coming Breakdown of the Power Grid (or Why Electric Cars Can Work only If Consumers Turn to Smart Charging)", *European Energy Review (EER)*, 29.09.2011; Karel Beckmann, „The Growing Vulnerability of the European Energy System", *EER*, 14.03.2011.

Frequenz- und Laststeuerungsprozesse gestört, die auf SCADA-Systemen mit verwundbaren Internetverbindungen basieren, oder sollten Fehlfunktionen in der Koordination zwischen Transmission System Operators (TSO) in den jeweiligen Kontrollregionen auftreten, kann dies schnell länderübergreifende Auswirkungen haben und zu großflächigen Stromausfällen führen. Dabei gelten vor allem die Energiekontrollzentren und ihre SCADA-Systeme als besonders verwundbar. Sollte es Angreifern tatsächlich gelingen, diese Systeme nachhaltig zu stören, zu manipulieren oder gar zu kontrollieren, könnte dies katastrophale Auswirkungen auch auf alle anderen kritischen Infrastrukturen haben, die von einer stabilen Energieversorgung und einem sicheren Zugang zum Internet abhängig sind.[59] Somit führen die gemeinsame und integrierte europäische Energiepolitik sowie die transnationalen Netze zwar einerseits zur Stärkung der Energieversorgungssicherheit, vor allem in Krisenzeiten, andererseits aber auch zu neuen Verwundbarkeiten.[60]

Tabelle 4
Internationale Stromausfälle und die Folgen

2000 brach das gesamte EC-Bankkartensystem der Schweiz zusammen, als Ergebnis eines Fehlers in einem einzigen Computerzentrum.
2003 gab es großflächige Stromausfälle in acht US-Bundesstaaten, auch in New York City und Teilen Kanadas. Es entstand ein Schaden von bis zu zehn Milliarden US-Dollar. 50 Millionen Menschen waren betroffen. Die Stromausfälle beeinträchtigten zentrale Dienstleistungen und den Handel, brachten den Verkehr zum Erliegen, Kläranlagen schalteten sich ab und die Wasserversorgung funktionierte nicht, die Produktion wurde unterbrochen und auch die Notfallkommunikation versagte.
2005 verursachten eine Kombination aus starkem Schneefall, Eis und Stürmen einen fünftägigen Stromausfall im deutschen Münsterland, von dem mehr als 80.000 Menschen in Deutschland, Belgien und den Niederlanden betroffen waren. Der Schaden durch den Stromausfall betrug rund 20 Millionen Euro.
2005, **2007 und 2009** waren laut Auskunft der CIA und anderer US-Quellen 50 Millionen Menschen in Brasilien – ein Viertel der Bevölkerung – von Stromausfällen betroffen. Diese waren zumindest in ein bis zwei Fällen unmittelbare Folge von Cyberangriffen auf SCADA-Systeme. Die brasilianische Regierung leugnet allerdings bis heute, dass irgendwelche Cyberangriffe stattgefunden hätten.
2006 führte ein dreitägiger Stromausfall im Emsland zu einer Kettenreaktion vom Norden bis in den Süden Deutschlands. Betroffen waren auch 15 Millionen Menschen in elf benachbarten Ländern wie Österreich, Kroatien und Ungarn. Die Auswirkungen waren bis Marokko zu spüren.

59 | Vgl. Fn. 29.
60 | Vgl. Thomas Petermann et al., „Was bei einem Blackout geschieht. Folgen eines lang andauernden und großräumigen Stromausfalls“, Studien des Büros für Technikabschätzung (TAB) des Deutschen Bundestages, Berlin, 2011, 30 f.

Wie eine Studie eines Forschungsinstitutes des deutschen Bundestags 2011 bestätigte, können großflächige Stromausfälle zur Unterbrechung der Funktionsfähigkeit aller anderen kritischen Infrastrukturen führen, da all diese von einer stabilen Stromversorgung abhängig sind. Demnach würden sich großflächige Stromausfälle auf die Lebensmittelversorgung, den Gesundheitsbereich, die Trinkwasserversorgung, die Abwasserentsorgung, den Mobilitäts- und Transportsektor sowie auf die Finanzdienstleistungen und die Aufrechterhaltung der Kommunikationssysteme auswirken und diese nachhaltig stören sowie funktionsunfähig machen. Innerhalb einer Woche wäre ein völliger Zusammenbruch des öffentlichen Lebens und der staatlichen Ordnung wahrscheinlich oder zumindest nicht auszuschließen. Das gesamte Land könnte durch einen großflächigen Stromausfall nachhaltig und dauerhaft destabilisiert werden: „Die Folgeanalysen haben gezeigt, dass bereits nach wenigen Tagen im betroffenen Gebiet die flächendeckende und bedarfsgerechte Versorgung der Bevölkerung mit (lebens)notwendigen Gütern und Dienstleistungen nicht mehr sicherzustellen ist. Die öffentliche Sicherheit ist gefährdet, der grundgesetzlich verankerten Schutzpflicht für Leib und Leben seiner Bürger kann der Staat nicht mehr gerecht werden. Die Wahrscheinlichkeit eines langandauernden und das Gebiet mehrerer Bundesländer betreffenden Stromausfalls mag gering sein. Träte dieser aber ein, kämen die dadurch ausgelösten Folgen einer nationalen Katastrophe gleich. Diese wäre durch eine Mobilisierung aller internen und externen Kräfte und Ressourcen nicht ‚beherrschbar', allenfalls zu mildern."[61]

Nach einem großflächigen Stromausfall wäre innerhalb einer Woche ein völliger Zusammenbruch des öffentlichen Lebens und der staatlichen Ordnung nicht auszuschließen.

Die Auswirkungen würden zudem nicht auf das eigene Land beschränkt bleiben, zumal der gemeinsame europäische Energiemarkt durch den Neubau zahlreicher transnationaler Stromnetze sowie Gas- und Ölpipelines bei den physischen Infrastrukturen bereits existent ist und weiter voranschreitet. Dies stärkt zwar einerseits auch ein Krisenmanagement in Form gegenseitiger Energielieferungen, wie sie 2009 bei der letzten großen Gaskrise zwischen Russland und der Ukraine nur zwischen bestimmten EU-Staaten möglich war, weil hierfür auch entsprechende Gaspipeline-Verbindungen existierten. Andererseits schafft die

61 | Ebd.

zunehmende Integration nationaler Energiemärkte vor allem im Strombereich eine Vielzahl neuer Abhängigkeiten und Verwundbarkeiten, die Stromausfälle in immer größeren Regionen zur Folge haben können. Während die Auswirkungen großflächiger Stromausfälle international gut untersucht sind, gilt dies nicht hinsichtlich eines Internet-Blackouts und seinen Folgen.[62]

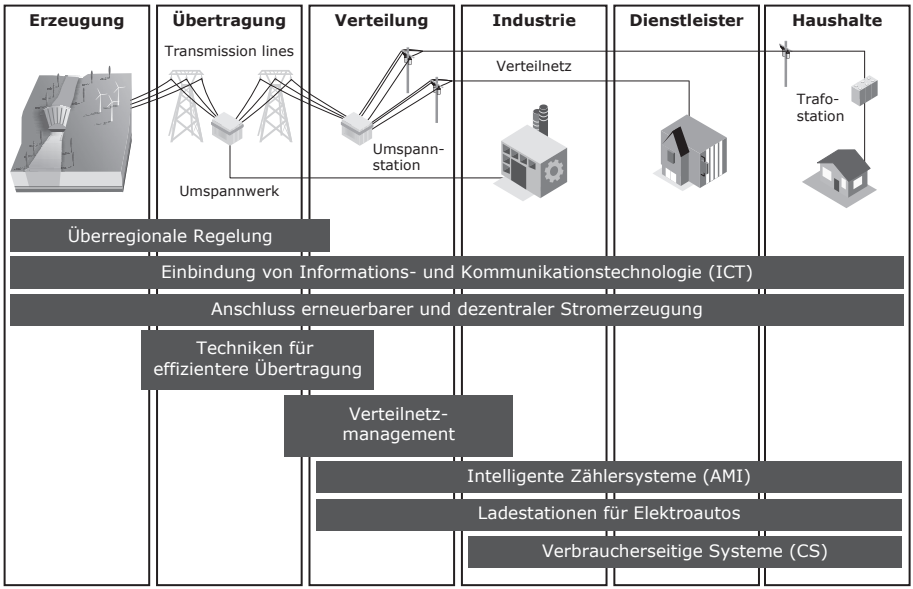
Während die Auswirkungen großflächiger Stromausfälle international gut untersucht sind, gilt dies nicht hinsichtlich eines Internet-Blackouts und seinen Folgen.

Vor diesem Hintergrund ist besorgniserregend, dass die Cyberrisiken und -verwundbarkeiten infolge der deutschen Energiewende durch die Einführung zahlreicher neuer Technologien für intelligente Stromnetze, so genannte *Smart Grid*- und *Smart Home*-Technologien, noch erheblich zunehmen werden[63], ohne dass bisher diese neuen Sicherheitsherausforderungen im Zuge des Umbaus des deutschen Energiesystems integraler Bestandteil der innenpolitischen Diskussionen der Energiewende geworden sind. Wenn überhaupt finden derartige Sicherheitsdiskussionen über die mangelnden Sicherheitsstandards und die Auswirkungen der Einführung zahlreicher neuer Technologien zur weiteren Vernetzung mit dem Internet in völlig von der Energiewende getrennten Diskussionsforen zwischen Regierung und Ministerien, der Privatwirtschaft und der Wissenschaft statt.

62 | Vgl. Ulrich Clauss, „Wird das Internet zusammenbrechen?“, *Die Welt*, 07.03.2012, 22.

63 | Vgl. auch *Technology Roadmap. Smart Grids*, Internationale Energieagentur (IEA), Paris, 2011, http://iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf [27.08.2012]; Josef Auer, *Smart Grids. Energy Rethink Requires Intelligent Electricity Networks*, Deutsche Bank Research, Frankfurt am Main, 21.06.2011; James Osborne, „Smart Grids Move from Research to Early Industzrialisation Phase“, *EER*, 09.02.2012; Jude Clement, „The Security Vulnerabilities of Smart Grid“, *Journal of Energy Security (JES)*, 18.06.009; Guido Bartels, „Combating Smart Grid Vulnerabilities“, *JES*, 15.03.2011; Ev Tebroke, „Verräterrische digitale Stromzähler“, *Welt am Sonntag*, 20.11.2011, 65; Claudia Eckert, Christoph Krauß und Peter Schoo, „Sicherheit im Smart Grid. Eckpunkte für ein Energieinformationsgesetz“, *Stiftungsreihe* 90, Alcatel-Lucent Stiftung für Kommunikationsforschung, Stuttgart, 2011, http://www.stiftungaktuell.de/files/sr90_sicherheit_im_energieinformationsnetz_gesamt_1.pdf [27.08.2012]; Harald Orlamünder, „Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen – ein Nachhaltiges Energieinformationsgesetz“, *Stiftungsreihe* 85, Alcatel-Lucent Stiftung für Kommunikationsforschung, Stuttgart, 2009, http://www.stiftungaktuell.de/files/sr85_newise_energieinformationsnetz_2.pdf [27.08.2012].

Abb. 2
Smart Grid-Technologien und Energiesektoren



Quelle: IEA, Fn. 63.

Die Anfälligkeit von größeren Stromausfällen im Elektrizitätssektor könnte sich in Zukunft weiter vergrößern, da neue Sicherheitskonzepte und Technologien zum Schutz und zur Härtung der Stromnetze nicht ausreichend schnell entwickelt werden. Die Einführung von *Smart Grid*-Technologien ist jedoch vor allem im Elektrizitätssektor der nächste und zentrale Schritt der Energiewende und eine Vorbedingung der kombinierten Verwendung von erneuerbaren und konventionellen Energiequellen. Dies verlangt zahlreiche quantitative und qualitative Veränderungen, zum Beispiel in der Art wie Elektrizität innerhalb und zwischen Ländern transportiert wird. Ohne diese Schlüsseltechnologien sind die ehrgeizigen Zielsetzungen der Energiewende, aber auch der deutschen und EU-Klimapolitik nicht zu erreichen.

Andererseits wird bei der Diskussion über die Umsetzung der Energiewende weitgehend übersehen, dass die Einführung dieser neuen Schlüsseltechnologien aufgrund der massiven Ausweitung von Drahtlosnetzwerken, *cloud computing* sowie der erweiterten Benutzung von Netzinfrastruktur-Plattformen (*Commodity IT*) wie *Smart Home* und *Smart Grids* weiter rasant zunehmen wird und die künftige

Stromversorgung sowie das Strommanagement mehr denn je gefährden könnte. *Smart Grid*-Technologien verwenden intelligente Stromübertragungs- und Verteilungsnetzwerke für einen ständigen digitalen Wechselfluss von Energie und Informationen. Sie basieren auf hochentwickelten, aber dennoch kostengünstigen Messsystemen und Sensoren. Die neuen intelligenten Stromzähler sollen weniger als 50 US-Dollar kosten und kontinuierlich Daten sammeln und analysieren, um so den Konsumenten dabei zu helfen, seinen Energieverbrauch in Echtzeit zu überwachen und zu reduzieren.

Die intelligenten Messsysteme und Netzwerke, die als Verteilungspunkt und Endpunkt für Kommunikation und Sensorknoten dienen, sind automatisierte Minicomputer. Sie beinhalten Schnittstellen für Drahtlosnetzwerke und verbinden Netzwerksoftware, die in der Industrie als *remote disconnect* bezeichnet werden. Die aktuelle Generation verschiedener *Smart Grid*-Technologien wurde jedoch weder in Europa noch in den USA mit inhärenten Sicherheits- und Verteidigungsanforderungen entwickelt. Erst jetzt wird begonnen, diese Sicherheitsstandards zu entwickeln und einzuführen. Wenn Sicherheit und Verteidigung nicht bereits in der Designphase von *Smart Grid*-Technologien beachtet werden, wird es nach der Markteinführung und der Anwenderbenutzung keine ausreichenden Sicherheitslösungen mehr geben.

Heutige Smart Grid-Technologien wurden weder in Europa noch in den USA mit inhärenten Sicherheits- und Verteidigungsanforderungen entwickelt. Erst jetzt wird begonnen, Sicherheitsstandards zu entwickeln.

Diese fortschrittlichen, digitalen Funktionen innerhalb der elektrischen Infrastruktur sollen die Verlässlichkeit, die Effizienz, die Flexibilität und die Sicherheit verbessern. Damit wird das künftige Elektrizitätsnetz jedoch noch viel abhängiger von computerbasierten Kontrollsystemen sein und wegen der Vielzahl an Kontaktstellen zum Internet von Cyberverwundbarkeiten gekennzeichnet sein. Mit der Vervielfachung der neuen Kontaktstellen zum Internet drohen somit auch die Verwundbarkeiten noch weiter dramatisch zuzunehmen, ohne dass eine vergleichbare Robustheit des Gesamtsystems wie früher besteht.

SCHLUSSFOLGERUNGEN UND PERSPEKTIVEN

Die Identifizierung des Stuxnet-Computerwurms im Juni 2010 hat gezeigt, wie verletzlich die SCADA-Systeme von Energie- und anderen Industriekontrollzentren sind. Doch können nicht nur andere Staaten, sondern auch terroristische Gruppierungen oder transnational agierende kriminelle Organisationen auch so komplexe Schadprogramme wie Stuxnet, Flame oder Duqu nachbauen, modifizieren und weiterentwickeln, um sie dann auch gegen ihren eigentlichen Urheber einzusetzen. Dies ist angesichts der IT-Fortschritte und der gleichzeitig weiter dramatisch zunehmenden Verwundbarkeiten für Sicherheitsexperten nur eine Frage der Zeit. Cyberwaffen sind unsichtbar, anonym und können von verheerender Wirkung sein. Beim Einsatz verschwinden die Grenzen von offensiv und defensiv wie auch zwischen privat und staatlich. Vor allem aber lässt sich bisher nicht feststellen, wer angreift. Gerade deshalb muss eine weiter stark ansteigende Cyberkriminalität ebenso befürchtet werden wie auch ein beschleunigter Rüstungswettlauf bei offensiven Cyberwaffen.

Beim Einsatz von Cyberwaffen verschwinden die Grenzen zwischen offensiv und defensiv sowie privat und staatlich. Vor allem lässt sich nicht feststellen, wer angreift.

Mit der breiten Einführung verschiedenster intelligenter Stromzähler (*Smart Meter*) und anderer *Smart Home*-Technologien sowie *Smart Grid*-Systeme, aber auch durch die Anbindung bisher autonom agierender Systeme an das Internet nimmt die Vernetzung aller Lebensbereiche weiter dramatisch zu – und bietet damit auch zwangsläufig viele neue Angriffspunkte. Daher müssen Sicherheit und Datenschutz künftig noch einen viel größeren Stellenwert erhalten als bisher. Zugleich müssen kritische Infrastrukturen robuster werden, wenn ein Rückbau, das heißt die Abkoppelung vom regulären Internet und der Aufbau von parallelen Intranets, nicht möglich erscheint oder nicht gewollt ist. Daher werden Redundanzen und Reservekapazitäten künftig mehr denn je von zentraler strategischer Bedeutung für die künftige Energieversorgungssicherheit sein, insbesondere bei der Strom- und Netzstabilität, um für die qualitativ völlig neuen Cybergefahren und die Risiken großflächiger Stromausfälle gewappnet zu sein. Gerade das langfristige Energiekonzept der Bundesregierung sieht vor, dass derartige Redundanzen und Reservekapazitäten zur

Aufrechterhaltung der Energieversorgungssicherheit abgebaut werden und Deutschland langfristig zum Nettoimporteur auch bei der Stromversorgung für die kritischen Infrastrukturen wird. Dies birgt mit Blick auf die Sicherheitsanforderungen gegen künftige Cyberangriffsfähigkeiten auf industrielle Steuerungs- und Kontrollanlagen auch große Risiken. Jede Art der Störung des Teilsektors Elektrizität kann sich auf andere Orte, Branchen oder Sektoren auswirken mit Folgen über EU-Landesgrenzen hinaus. Unternehmen, ebenso wie der Staat, benötigen daher umfassende, mehrschichtige und mit Business-Development integrierte Sicherheitskonzepte, die zudem Teil eines adäquaten europäischen Sicherheitskonzepts auf EU-Ebene werden müssen.

Jede Art der Störung des Teilsektors Elektrizität kann sich auf andere Orte, Branchen oder Sektoren auswirken mit Folgen über EU-Landesgrenzen hinaus.

Je mehr die EU ihre nationalen Energie- und Elektrizitätsmärkte integriert, desto mehr verstärkt sie zwar einerseits die Energieversorgungssicherheit aller Partner und verringert dabei auch die Kosten. Andererseits erhöht die zunehmende Verbindungsflexibilität der nationalen Märkte aber auch die Wahrscheinlichkeit möglicher Kettenreaktionen. Die Sicherheit und Widerstandsfähigkeit nationaler kritischer Energieinfrastrukturen kann künftig nicht allein durch unkoordinierte, rein nationale Strategien gesichert und gestärkt werden. Die regionale und globale Zusammenarbeit zum Schutz der kritischen Energieinfrastruktur (Critical Energy Infrastructure Protection, CEIP) muss durch EU, NATO, die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), die G8 und andere internationale Organisationen ausgedehnt und vertieft werden.

Darüber hinaus bleiben die finanziellen und personellen Ressourcen der Betreiber zum Schutz ihrer Infrastruktursysteme begrenzt. Deshalb ist es wichtig, alle zugänglichen Kräfte effizient und effektiv zu nutzen, indem Eventualitäten abgewogen und entsprechende Prioritäten für ein adäquates Risikomanagement definiert werden. In den meisten Fällen können sich Unternehmen bereits mit bescheidenem Aufwand gegen Cyberkriminalität wappnen. Allein 90 Prozent aller gegenwärtigen Datenlecks könnten durch regelmäßige Aktualisierungen ihrer Software verhindert werden. Telekommunikationsunternehmen wie die Deutsche Telekom setzen inzwischen auch so genannte

Honeypot-Systeme ein, mit denen Hacker auf Webseiten gelockt werden, auf denen für Eindringlinge nichts zu holen ist. Damit können Hacker und ihre neuesten Techniken sowie Angriffsmethoden, aber auch Sicherheitslücken in den eigenen Netzwerken untersucht werden, mit denen bzw. durch die sich Computerkriminelle Zugang zu IT und Kommunikationsnetzen verschaffen.

Zwar bleibt es unmöglich, öffentliche Versorgungseinrichtungen und kritische Infrastrukturen vor physischen Attacken oder Cyberangriffen zu 100 Prozent zu schützen. Dennoch müssen die Gefahren dringend minimiert werden, ohne dass die Produktivität und der normale Geschäftsbetrieb allzu negativ beeinflusst wird. Eine professionelle Einschätzung von Sicherheit und Risiko muss physische sowie Cybersicherheit als auch SCADA und Distributed Control Systems (DCS), Kommunikationssicherheit, Netzsicherheit, Verteilungssicherheit, Erzeugungssicherheit und biologische/chemische Fragen berücksichtigen.

Die größte Sicherheitsherausforderung für die Firmen und für staatliche Schutzkonzepte für kritische Infrastrukturen, die größtenteils in privater Hand sind, liegt jedoch in einem grundsätzlichen Umdenken und der Entwicklung einer neuen Sicherheitskultur in den Unternehmen. Als erster Schritt muss hierbei die tradierte „Kultur des Schweigens" aufgebrochen werden. Inzwischen lassen sich Firmen nach erfolgreichen Angriffen immer häufiger erpressen und zahlen Schweigegeld an Cyberkriminelle, um ihre geschäftliche Reputation nicht zu verlieren. Fast die Hälfte der befragten Unternehmen gab bei einer Umfrage des deutschen IT-Branchenverbandes Bitkom an, keinen Notfallplan für das Verhalten nach Angriffen zu haben. Jedes vierte Unternehmen gab sogar zu, die Zusammenarbeit mit der Polizei lieber zu vermeiden, wenn es Ziel einer Attacke sei oder ein Datenleck feststelle.[64]

Unternehmen lassen sich nach Cyberangriffen immer häufiger erpressen. Sie zahlen Schweigegeld, um ihre geschäftliche Reputation nicht zu verlieren.

Erschwert wird die Situation in Deutschland auch dadurch, dass Unternehmen bislang nur in Ausnahmefällen verpflichtet sind, die Angriffe öffentlich zu machen. Ob eine gesetzliche Meldestelle wie in einigen anderen Ländern wirklich

64 | Vgl. Florian Eder, „EU verschärft Kampf gegen Hacker", *Die Welt*, 27.03.2012, 11.

zielführend ist, bleibt ebenso abzuwarten wie der Versuch, mittels einer „Allianz für Cybersicherheit“ eine zentrale freiwillige Meldestelle für Cyberangriffe einzurichten, um so einen anonymen Informations- und Wissensaustausch zu fördern. Demgegenüber sollen die Unternehmen nach Auffassung der Europäischen Kommission künftig ihre Daten nicht nur besser schützen müssen, sondern es soll auch eine Anzeigepflicht über das Ausmaß der Cyberattacken eingeführt werden. Wichtige Richtschnur für unternehmerisches und staatliches Denken sollte bei der Analyse der künftigen Cybersicherheitsherausforderungen mehr denn je die Aufforderung sein, „das Undenkbare zu denken“ und notfalls ausgetretene Pfade, Konzepte und Organisationsstrukturen zu verlassen.