Vorschlag für ein „Digitales Hilfswerk“

von Gerold Reichenbach, MdB

Der Bericht der EU-Kommission über den Schutz kritischer Infrastrukturen (KOM (2009) 149 endgültig vom 30.3. 2009) zitiert Schätzungen des Weltwirtschaftsforums aus dem Jahre 2008, das davon ausgeht, dass in den kommenden zehn Jahren ein größerer kritischer Informationsinfrastruktur-Ausfall mit einer Wahrscheinlichkeit von 10-20% eintreten wird, der für die Weltwirtschaft Kosten von ca. 250 Milliarden US-Dollar verursachen könnte. Der 2012 Norton Cyber Crime Report konstatiert bereits jetzt ein weltweites Schadenspotenzial von 110 Milliarden US-Dollar (ca. 88 Milliarden Euro) durch Cyber-Kriminalität und Cyber-Attacken. Durchaus sinnvollerweise, konzentrieren sich die bisherigen Anstrengungen im Bereich der IT-Sicherheit und Sicherheit kritischer Informationsinfrastruktur zunächst auf Präventions- und Abwehrmechanismen. Das Schwergewicht liegt dabei auf der Erhöhung der Sicherheitsstandards, wie dies etwa mit der Gründung des Bundesamtes für Sicherheit in der Informationstechnik, und der Verbesserung der Informations-und Abwehrmechanismen, wie dies in der Gründung des deutschen Cyberabwehrzentrums zum Ausdruck kommt. Neben den staatlichen Stellen sind die privaten Betreiber kritischer Informationsinfrastrukturen zur Verbesserung der Abwehrmechanismen und der internen Sicherheitsstandards aufgefordert. Dabei hat man bislang eher auf Eigenvorsorge, Information und die Schaffung von Gefährdungsbewusstsein, denn auf regulative Eingriffe gesetzt. Inwieweit dies ausreichend ist, wäre in einem eigenen Diskurs zu klären. Zunehmend wächst auch das Bewusstsein, dass wir bezüglich der Vernetzungen und möglicher Kaskadeneffekte noch erheblichen Informations- und Forschungsbedarf haben. Dies gilt insbesondere für die wechselseitige Beeinflussung zwischen anderen kritischen Infrastrukturen und der Informationsinfrastruktur. Gleichzeitig wissen wir nur wenig über die Kaskadenpotenziale ausgelagerter Dienstleistung und Produktion für die kritische Informationsinfrastruktur. Die Auswirkungen der Hochwasserflut 2011 in Thailand auf die internationale IT-Produktion haben ein Schlaglicht auf die Weite dieses Feldes geworfen. Gleichwohl konzentriert sich das zivile Forschungsrahmen-Programm der Bundesregierung bisher stärker auf den instrumentell operativen Bereich, denn auf die Schließung von Forschung- und Informationslücken bei den oben genannten Themen. Allein durch das bisher Beschriebene wird überdeutlich, dass die Steigerung der Sicherheit und Prävention nicht ausreichen werden, um den wachsenden Gefahren des Cyberzeitalters zu begegnen. So formuliert Symantec in seinen Keyfindings des CIP-Reports 2011 für Deutschland „emphasize that security is not enough to stay resilient in the face of today‘s cyber attacks“ (Betonen, dass Sicherheit nicht ausreichend ist, um gegenüber den heutigen Cyber-Attacken resilient zu bleiben, G.R.).Als die Weimarer Reichsregierung Ende 1919 auf Anregung des Freikorpspionieroffiziers Otto Lumitzsch die Technische Nothilfe, die Vorläuferorganisation des heutigen THW, ins Leben rief, war das zwar zunächst dem Bemühen geschuldet, wilde Streiks abzuwehren, es stellte sich jedoch nach dem Abflauen der Revolutionswirren viel deutlicher heraus, dass der Organisationsgedanke der technischen Nothilfe, nämlich in der Zivilgesellschaft Freiwillige mit hoher technischer und beruflicher Qualifikation, wie Ingenieure, Facharbeiter und Handwerksmeister, als Freiwillige zu rekrutieren und organisatorisch so zusammenzubinden, dass sie Noterhaltungs- und Instandsetzungsmaßnahmen in einer sich durch die Industrialisierung rasant technisierenden Welt durchführen konnten, eine adäquate Antwort auf die wachsenden Gefahren- und Schadenspotenziale im hochindustrialisierten Deutschland boten. Zumal die damaligen freiwilligen und wenigen Berufsfeuerwehren sich noch im Wesentlichen auf den Brandschutz oder regionale Naturkatastrophen konzentrierten und ihnen in der Mehrzahl außerhalb des

Brandschutzes das fachliche Know-how fehlte, adäquat auf die Gefährdung von und durch die Industrie und die Infrastruktur zu reagieren. Gleiches gilt übrigens ähnlich für die Gründung des Arbeitersamariterbundes als Hilfsorganisation für die von Industrieunfällen in großen Massen betroffenen Arbeitnehmer. Inzwischen hat sich in der Bundesrepublik Deutschland daraus, einhergehend mit der Erweiterung des Aufgabenbereichs der Feuerwehren, ein hoch ausdifferenziertes System der Gefahrenabwehr etabliert, das im Grundsatz vorzüglich geeignet ist auf die bisherigen Gefahren zu reagieren. Und so stellte Prof. Dr. Wolf Dombrowsky 2007 bei seinem Impulsreferat anlässlich der Gründung des vom Autor initiierten Zukunftsforum für Öffentliche Sicherheit treffend fest, „dass die Katastrophen des konventionellen (newtonschen) Bereichs in modernen Gesellschaften so stark umhegt sind, dass ihr Schadenspotenzial zumeist durch die Bündelung der Ressourcen bewältigt werden kann“ . Er führte weiter aus, „für die problematischen Schadenspotenziale des nach-newtonschen Zeitalters gibt das bestehende Katastrophenschutzsystem so gut wie keine geeigneten Antworten“ . Und so ist es auch nicht verwunderlich, dass die strategische Krisenmanagement-Übung Lükex 11, die die Störung kritischer IT-Systeme und ihre Auswirkungen zum Gegenstand hatte, sich im Wesentlichen auf die Bekämpfung und Behebung der mittelbaren Folgen des Ausfalls von IT - und Kommunikationstechnologien, konzentrierte. Denn lediglich für diesen „newtonschen“ Bereich der Katastrophe stehen erhebliche Potenziale zur Reaktion und Bewältigung zur Verfügung. Im Gegensatz dazu stehen für den digitalen „nach- newtonschen“ Katastrophenablauf kaum zusätzliche Ressourcen zur Notfallbewältigung bereit. Bei der Abwehr und Eindämmung müssen die Betreiber im Wesentlichen auf die für den Normalbetrieb und Normalstörung vorgehaltenen eigenen Ressourcen zurückgreifen. Das notfallmäßige Unterstützungspotential durch andere privatwirtschaftliche Unternehmen und den bereits bestehenden Einrichtungen wie BSI und CERT ist begrenzt. Im „newtonschen“ Katastrophenschutz stehen uns dagegen zur Abwehr und Bekämpfung der Folgen von Natur- und Industriegefahren zusätzlich die breite Personal- und Know-how-Ressource der Zivilgesellschaft zur Verfügung, die von den Hilfsorganisationen und Feuerwehren rekrutiert, organisatorisch eingebunden, zusätzlich ausgebildet und auf den Einsatz in Notfall-Situationen vorbereitet werden. Aber so wie die Industriegesellschaft mit den in ihr Beschäftigten gleichzeitig die personellen und instrumentellen Ressourcen sowie organisatorischen Voraussetzungen generierte, um den aus ihr entstehenden Gefahren und Herausforderungen zu begegnen, so geschieht dies auch in der digitalisierten Postindustriellen Gesellschaft. Der entscheidende Unterschied jedoch ist, dass im Gegensatz zur „traditionellen Gefahren- und Katastrophenabwehr“ uns bislang die organisatorischen Strukturen fehlen, um diese Ressourcen zu heben und auch in einer digitalen Gesellschaft zur Gefahrenabwehr und Bekämpfung einzusetzen. Was also läge näher, als den Gründungsgedanken, aus dem das heutige Technische Hilfswerk und die modernen Hilfsorganisationen und Feuerwehren entstanden, auf die digitale Gesellschaft zu übertragen. Mit anderen Worten: ich schlage die Gründung eines digitalen Hilfswerkes vor. Dieser Vorschlag muss sich mit dem Einwand auseinandersetzen, das ausgerechnet in Zeiten, in denen die Feuerwehren und Hilfsorganisationen aufgrund des demographischen Wandels und den Veränderungen in der Arbeitswelt mit Rekrutierungsproblemen zu kämpfen haben, eine weitere Konkurrenz geschaffen werden soll.Bei genauerem Hinsehen ist jedoch das Gegenteil der Fall. Ein digitales Hilfswerk böte die Chance, zusätzliches ehrenamtliches Potential aus der Zivilgesellschaft zu schöpfen, das den traditionellen Hilfsorganisationen aufgrund ihrer Aufgabenstellung und der daran ausgerichteten Organisationsstruktur gar nicht zur Verfügung steht. Denn auch die Grundlage der Organisationsstruktur, des traditionellen ehrenamtlichen Katastrophen- und Bevölkerungsschutzes, die auf räumlicher und örtlicher Gleichzeitigkeit beruht, fußt auf einem Ergebnis der Industrialisierung. Nämlich der Normierung von Arbeitszeit und Freizeit. Erst durch diese weitgehende Normierung war es möglich gemeinsame Übungen, gemeinsame

Ausbildungen und Vorbereitungen zu organisieren, so dass im Einsatzfalle, aus den Betrieben, Handwerksunternehmen und der Landwirtwirtschaft aus der räumlichen Umgebung die Einsatzkräfte alarmieren und in den Einsatz bringen konnte. Genau diese verlässlichen, zeitlichen und örtlichen Rahmenbedingungen schrumpfen im Zuge der zunehmenden Flexibilisierung von Arbeitszeiten und Lebensarbeitsbiografien, die die post-industrielle Gesellschaft gegenüber der Industrie-Gesellschaft prägen. Dies ist neben der Demographie einer, wenn nicht sogar der entscheidende Grund, für die zunehmenden Rekrutierungsschwierigkeiten der klassischen Hilfsorganisationen. Um die Helfer ausbilden oder in den Einsatz bringen zu können, muss ich sie zur gleichen Zeit an einem Ort versammeln können. Lässt sich zumindest die theoretische Ausbildung durch Hilfe moderner Medien und Kommunikationsmechanismen zeitlich und räumlich entzerren, so gilt das für den größten Teil der praktischen Ausbildung und das Einsatzgeschehen auf keinen Fall. Genau dieser Umstand, der in vielen Regionen dazu führt, dass es vielen Feuerwehren trotz eigentlich ausreichender freiwilliger Mitglieder in den Einsatzabteilungen, nur noch schwer oder kaum gelingt ausreichende Tageseinsatzstärken herzustellen. In der digitalen Welt ist dies anders. Eine der qualitativen Errungenschaften der digitalisierten Welt ist, neben der Fähigkeit zu massenhafter Datenverarbeitung, die teilweise Unabhängigkeit von Ort und Zeit. Dies hat nicht nur zu neuen Formen der Kommunikation, der Information und von Dienstleistungen geführt, sondern dies führt auch dazu, dass Menschen über Räume und Zeitschienen hinweg in Netzen interagieren können. Und genau hier liegt die Chance. Um sich zu organisieren, miteinander zu kommunizieren, Informationen auszutauschen, sich aus- und weiterzubilden, und zu trainieren, müssen die Mitglieder eines digitalen Hilfswerks sich nicht regelmäßig am gleichen Ort treffen und sind auch zeitlich viel flexibler. Und dies gilt sogar für mögliche Einsätze. Um etwa Administrationsforen bei der Abwehr von Abgriffen oder der Analyse von Schadsoftware zu unterstützen, um Analyse und CERT-Teams aufzubauen, ist es nicht mehr notwendig, dass sich die Helfer an „der“ Einsatzstelle zusammenfinden. Sondern dies kann auch remote geschehen, teilweise sogar wenn die entsprechende Infrastruktur zur Verfügung steht ohne den eigenen Arbeitsplatz räumlich verlassen zu müssen. Dies hat auch die positive Auswirkung, dass hier die Veränderung der Arbeitswelt im Gegensatz zu den traditionellen Einsatzbereichen des Bevölkerungs- und Katastrophenschutzes, die Verfügbarkeit sogar wieder erhöhen können. Und genau deswegen lassen sich ehrenamtliche Engagementbereitschaft und in der Ausbildung und im Berufsleben erworbene Qualifikationen von Bürgern in der Zivilgesellschaft ansprechen, die für die klassischen Hilfsorganisationen gar nicht zur Verfügung stehen können. Auch wenn die Strukturen und die räumliche Organisation aus diesem Grunde sich von den bestehenden Hilfsorganisationen grundlegend unterscheiden kann und wird die Gründung eines solchen digitalen Hilfswerks ähnlich der Bundesanstalt des technischen Hilfswerks erfolgen. Dabei sind auch die Vor- und Nachteile einer Angliederung an dieses abzuwägen. Aber ähnlich wie beim THW können Einsatz- und Fachgruppen gebildet, regionale und zentrale Aus- und Weiterbildungen organisiert, sowie Einsatzszenarien identifiziert und Einsatzstrukturen gebildet und geübt werden. Allerdings mit dem Vorteil gegenüber den bereits bestehenden ehrenamtlichen Strukturen, dass man nicht grundsätzlich Orts-, bzw. Zeitgebunden ist. Die zentrale Aufgabe eines digitalen Hilfswerks würde dann sein, Krisen und Notfall, etwa bei erheblichen Angriffen auf kritische Informations- und Kommunikationsstrukturen, die betroffenen Einrichtungen durch Personal und Expertise zu unterstützen. Gerade bei mittelständischen Firmen, die gleichwohl Teil kritischer Infrastrukturen sein können, kann nicht dauerhaft ausreichendes Personal vorgehalten werden, um solche Krisen oder Angriffe adäquat abarbeiten zu könnenNeben der Ausbildung und Vorbereitung auf Einsatzszenarien, kann das Digitale Hilfswerk Aufgaben in der Prävention übernehmen. Es kann in Zusammenarbeit und Abstimmung mit dem BSI Sicherheitslücken bei zentralen Infrastrukturen suchen und identifizieren, diese analysieren und an das BSI

melden. Gerade bei der Prävention kann es Unterstützung für Unternehmen und Behörden bieten, die kritische Infrastrukturen bereitstellen. Eine mögliche Konkurrenz privater Anbieter muss dabei jedoch vermieden und könnte durch ähnliche Regelungen wie sie auch beim Technischen Hilfswerk gelten, sichergestellt werden. Darüber hinaus könnte es für eine gegenseitige Fort- und Weiterbildung sorgen sowie mit Aktionen und Veranstaltungen einen Beitrag zur Sensibilisierung und zur Aufklärung der Bürger zu Sicherheitsfragen im Netz leisten. Im Gegensatz zur estnischen Cyber Defense League sollte das Digitale Hilfswerk analog zu den Aufgabenstellungen des Technischen Hilfswerkes zivil ausgerichtet sein. Gerade im Bereich der Cybersicherheit ist es nicht entscheidend, ob der Angriff oder die Schädigung aus privaten oder staatlichen Strukturen entspringt.

Der Beitrag ist auch erschienen in Homeland Security (2014), 3, S. 29 - 32.