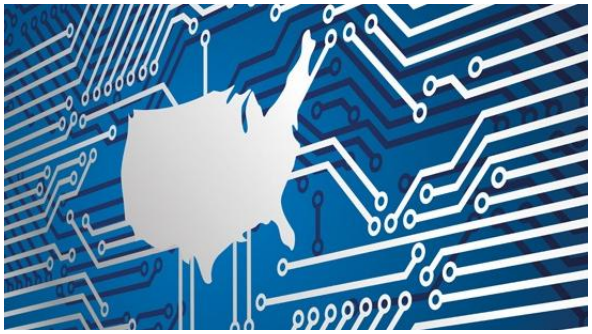
Cyber-Weltkrieg: Die USA rüsten sich gegen die digitale Apokalypse

von Andreas von Rétyi

Quelle: KOPP online vom 14.08.2016



Der nächste Weltkrieg soll im Weltall beginnen.

Er wird digital geführt werden und verheerende Folgen haben. Auf der Erde werden zugleich die Stromnetze angegriffen.

Dann bleiben nur noch wenige Tage Zeit, bis das totale Chaos ausbricht.

Zu Beginn des lahres 2016 warnte Keith Alexander, der ehemalige Chef der *National SecurityAgency,* eindringlich vor dem wachsenden Risiko, dem die industrialisierte Welt durch einen Cyber-Angriff auf die Energieinfrastruktur ausgesetzt sei. Später äußerte sich dann auch US-Präsident Obama zur Bekämpfung solcher digitaler Angriffe. Anschließend gab das Pentagon bekannt, einen Plan gegen diese Gefahr zu haben, die auf der Erde und auch im Weltraum drohe. Das Szenario lautet in Frageform:

Beginnt der Dritte Weltkrieg mit einem Stromausfall? Die Vernetzung der Welt lässt zumindest Gefahren der Art koordinierter digitaler Angriffe gegen die Infrastruktur eines Landes wahrscheinlicher werden. Hacker könnten die Energieversorgung zum Stillstand bringen und die gesamte Nation lähmen, fürchtet auch der frühere NSA-Chef Keith Alexander.

► Die neue Dimension des Terrors

Schon einmal haben die USA eine präzis koordinierte Terrorattacke erlebt, die sich zuvor wohl niemand hätte vorstellen können. Die Weltmacht wurde damals direkt im Herzen getroffen. Und seit jenem 11. September 2001 lebt die Nation in ständiger Angst, wieder Opfer eines vergleichbar folgenschweren Ereignisses oder eines gar noch umfassenderen gezielten Angriffs zu werden. Die neue Dimension des Terrors hat die Welt seither nicht mehr losgelassen. Sie hat dem 21. Jahrhundert einen charakteristischen Stempel des Schreckens aufgeprägt und vor allem die globale Überwachung im erklärten Krieg gegen den Terror eingeläutet. Gefährlich ist auch die zunehmende Komplexität der Vernetzung, eine regelrechte Technologie-proliferation mit gleichzeitig massiv steigender Verletzbarkeit. Die DARPA als avantgardistische Forschungsabteilung des US-Verteidigungsministerium hat ein Programm gestartet, um Sicherheitsbedrohungen durch digitale Angriffe wirksam zu begegnen. Dal5ei geht es um Maßnahmen gegen Bedrohungen, die auch alle Energie liefernden Systeme schlagartig zum Erliegen bringen können.

Vorrangig soll jene Infrastruktur geschützt werden, die für Missionen des US-Verteidigungsministeriums existenziell notwendig ist. Das neue DARPA-Programm

RADICS umfasst *Rapid ,4ttack Detection, Isolation aM Choracterization Systems* und somit Systeme zur Entdeckung, Isolierung und Charakterisierung von Angriffen.

► Eine Woche oder mehr ohne Strom?

Dabei geht es vor allem um die Entwicklung eines automatischen Systems, das nach einem großen Angriff Ausfälle bewältigen und die Energieversorgung möglichst schnell wieder herstellen kann. Ingenieure sollen die Infrastruktur dann innerhalb einer Woche wieder zum Laufen bringen. Das wäre in etwa die kritische Spanne, während derer noch eine behelfsmäßige Überbrückung einer Katastrophensituation möglich scheint, ohne ins vollständige, irreversible Chaos zu gleiten. DARPA-Programm-Manage Dr. John Everett stellt fest:

- *»Würde sich heute eine koordinierte Cyber-Attacke auf das nationale Stromnetz ereignen, dann würde die Zeit bis zu dessen Wiederherstellung erschreckende Herausforderungen an die nationale Sicherheit stellen«*.

Abgesehen von den massiven Auswirkungen auf Wirtschaft und Bevölkerung, würde ein auf längere Zeit unterbrochenes Stromnetz die militärische Mobilisierung und Logistik in erhebliche Schwierigkeiten bringen und die Fähigkeit der Regierung schwächen, Lösungen bei internationalen Krisen zu verfolgen und Stärke zu zeigen. Was Everett hier euphemistisch umschreibt, läuft doch letztlich auf den Verlust der militärischen Handlungsfähigkeit und die Vorherrschaft in Kriegssituationen hinaus. Es scheint klar, dass eine wirklich umfassende Cyber-Attacle zum Verlust der US-Vormachtstellung führen würde, und nichts bereitet dem Pentagon offenbar mehr Kopfzerbrechen. Daher will man dort alles daransetzen, ein entsprechendes Frühwarnsystem zu installieren, mit möglichst hoher Empfindlichkeit und dennoch niedriger Quote an Fehlalarmen.

► Darauf sind wir nicht vorbereitet

Sofern der Ernstfall bereits eingetreten ist, sollen Energieversorger in einem Notfallnetzwerk verbunden werden, jedoch unter Isolierung betroffener Einrichtungen vom Internet, sodass es nicht zu einer weiteren Überwachung und Interferenz durch gegnerische Kräfte kommen kann. RADICS soll auch weitreichende Suchsysteme einbinden, die schädliche Software lokalisieren und charakterisieren. General Keith Alexander sieht das größte Angriffsrisiko in einem katastrophalen Angriff auf die Infrastruktur der Energieversorger. *»Darauf sind wir nicht vorbereitet*«, sagte er Anfang des Jahres.

In Deutschland wäre das nicht anders. Im schlimmsten Szenario Alexanders könnten Hacker Ölraffinerien, Kraftwerke und das Stromnetz übernehmen. Auch das Zahlungsgeflecht der großen Banken könne ins Chaos gestürzt werden, warnte der General. Daher sei eine Art integriertes *»Luftverteidigungssystem«* für den gesamten Energiesektor nötig. Einer Studie zufolge sind auch die Kernkraftwerke der Welt nicht auf CyberAngriffe vorbereitet. Daher bestehe die Gefahr, selbst mit relativ kleinen Attacken den Austritt radioaktiver Strahlung auslösen zu können. Cyber-Kriminelle könnten sogar einen Zwischenfall von Fukushima-Dimerision künstlich herbeiführen.