Keith B. Alexander / Emily Goldman / Michael Warner

Defending America in Cyberspace

In: The National Interest, Nr. 1, 28,
November/Dezember 2013, S. 18–25

Im Artikel von Keith B. Alexander, dem Direktor der National Security Agency (NSA), sowie seinen Co-Autoren Emily Goldman und Michael Warner, werden eingangs veröffentlichte Aussagen vom Präsidenten der USA, seines ehemaligen Verteidigungsministers Leon Panetta und von zwei Staatssekretären für Verteidigung zitiert, in denen auf die digitale Verwundbarkeit der USA und ihrer Streitkräfte mit sehr einprägsamen Metaphern wie »Pre-9/11 Moment« und »Cyber Pearl Harbour« hingewiesen wird. Die USA begegnen den Angriffen aus dem Cyberraum mit einem breit gefächerten Sortiment an Fähigkeiten, die innerhalb von zwei Dekaden mittels der Methode »Versuch und Irrtum« (trial and error) entwickelt wurden und sehr stark von den Ergebnissen aus der Verlinkung strategischer nachrichtendienstlicher Fernmeldeaufklärung und Informationsbereitstellung profitieren.

In einem historischen Abriss wird auf die Bedeutung der zeitlichen Synchronisation von logistischen und operativen Abläufen hingewiesen, die ein Garant für eine funktionierende moderne Gesellschaft, Wirtschaft und Armee sind. Am Beispiel Großbritanniens und seines internationalen Überseehandels wird veranschaulicht, wie ausgesetzt und verwundbar zusammenhängende und vernetzte Systeme bereits am Beginn des 20. Jahrhunderts waren. Eine auch nur kurzweilige Unterbrechung des britischen Überseehandels durch französische Kriegsschiffe hätte zu einem Kollaps der gesamten britischen Wirtschaft führen können. Die Briten haben damals ihr Wissen über die Sensibilität und Störanfälligkeit des globalen Wirtschaftssystems in einer von Nicholas Lambert so treffend bezeichneten »Armageddon«-Strategie (Weltuntergangsstrategie) zusammengefasst, mit der sie erheblichen Druck auf andere Staaten, wie z.B. Deutschland, ausüben hätten können. Zur Identifizierung der Schwachstellen wurde von den Briten in dieser Zeit die strategische Fernmeldeaufklärung entwickelt, die von den USA übernommen und dort zu einer kryptologischen Plattform weiterentwickelt wurde. Diese Plattform stellt heute noch einen der Grundpfeiler der militärischen Cyberarchitektur der USA dar, in der die NSA zuerst für das Pentagon und später dann auf gesamtstaatlicher Ebene den Schutz der Computer und Informationssysteme übernommen hat. Interessant erscheint in dem Artikel die aufgezeigte historische Parallele zwischen den von Planern der Royal Navy 1905 identifizierten Verwundbarkeiten globaler interdependenter Systeme und deren Anwendungsmöglichkeit auf den heutigen digitalen Systemverbund.

In dem Bericht setzen sich die Autoren auch mit der großen Angst der USA vor einer Lahmlegung oder Zerstörung ihrer kritischen Infrastrukturen auseinander. Derartig massiven Bedrohungen aus dem Cyberraum soll mit einem gesamtstaatlichen Wirkverbund begegnet werden, der mit Ressourcen und Fähigkeiten der Ministerien und unter Einbindung der Privatwirtschaft aufgebaut werden soll. Das Herzstück dieses Systems bilden die Nachrichtendienste, die mit weitreichenden Befugnissen ausgestattet wurden und deren »Teamarbeit« vom Direktor der NSA, der zugleich Chef des USCYBERCOMMAND ist, koordiniert wird. Durch diesen organisatorischen Schulterschluss wurde für das »Departement of Defence« der Grundstein für ein verstärktes Engagement für die nationale Cybersicherheit gelegt. Die Privatsphäre der Menschen und die Rechte der Bürger sollen durch zahlreiche Kontrollmechanismen gewahrt bleiben.

Sehr kritisch wird in dem Artikel auf den schleichenden Verlust der digitalen Dominanz der USA eingegangen, woraufhin jene mit zahlreichen Initiativen versuchen, dieser Entwicklung entgegenzusteuern.

Cybersicherheit im militärischen Bereich soll durch eine Reduktion der Netzwerke und durch das Bereitstellen einer kodifizierten C3-Struktur (Command, Control and Communication) für die Streitkräfte erreicht werden. Im Bereich »Cyber« sollen Kapazitäten entwickelt werden, aufgrund derer man in der Lage sein soll, die Nation im Cyberraum zu verteidigen, das Informationsnetzwerk des »Department of Defence« zu schützen und Operationen direkt zu unterstützen. Von diesen Kräften wird weiters verlangt, dass sie einen sicheren digitalen Zufluchtsort (safe haven) bereitstellen, von dem aus die USA auch operieren können, während diese angegriffen werden.

Für die USA mutiert der Cyberraum immer mehr zum Kriegsschauplatz, auf dem sich Feinde tummeln, deren Fähigkeiten sich schneller entwickeln als jene der USA. Zum Schutz vor strategischen Überraschungen aus dieser Domain bedarf es des Poolings gesamtstaatlicher Ressourcen in einem »Unternehmen«, das über den Handlungsrahmen und die Zuständigkeiten des »US Department of Defence« hinausgeht. Die Ausgestaltung dieses »Unternehmens« ist unverzichtbar für die Fähigkeit, Feinde aus dem Cyberraum abzuschrecken und abzuwehren, damit diese die Sicherheit, den Wohlstand und das tägliche Leben der US-Bürger nicht bedrohen.

Der Artikel ist sehr informativ und stellt die Angreifbarkeit hoch vernetzter digitaler Systeme dar, die in letzter Konsequenz auf nationaler Ebene nur durch ein gesamtstaatliches, koordiniertes Zusammenwirken aller Akteure geschützt werden können. Die Schwäche und Verwundbarkeit der USA im Bereich »Cyber« wird etwas übertrieben dargestellt. Vermutlich wurde diese Darstellung gewählt, um die weit reichenden Befugnisse der NSA damit ein Stück weit zu rechtfertigen.

Wolfgang Manzl