Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 179 (2013)

Heft: 11

Artikel: Cyberwar heute

Autor: Schlomann, Friedrich-Wilhelm

DOI: https://doi.org/10.5169/seals-358192

Cyberwar heute

Dass Cyberwar zum wichtigsten Thema beim ersten Gipfeltreffen zwischen US-Präsident Obama und dem chinesischen Präsidenten und Parteichef Xi Jinping Anfang Juni 2013 in Südkalifornien werden würde, war vorauszusehen – befürchten doch die USA auf diesem Weg eine Verschiebung der Militär-strategischen Balance.

Friedrich-Wilhelm Schlomann

Schon kurz zuvor warf der neue Jahresbericht des Pentagons der Volksrepublik in bisher unbekannter Deutlichkeit gezielte Cyber-Spionage gegen Computernetzwerke des US Militärs vor. Ende Mai 2013 drangen deren Hacker in diese ein, mit Bauplänen für zwei Dutzend Waffensysteme der Bereiche Raketenabwehr, Kampfflugzeuge und Kriegsschiffe. Bereits zu diesem Zeitpunkt erachteten CIA-Experten erstmals Cyberwarfare als eine grössere Bedrohung als Al-Qaeda oder den Terrorismus. Geheimdienstdirektor Clapper stufte diese sogar als die grösste Gefahr weltweit ein. Inzwischen hat der US-Präsident bei unmittelbar bevorstehenden Cyber-Attacken sogar die Möglichkeit militärischer Präventivschläge seitens der USA befürwortet. Schon vor zwei Jahren waren deren Regierungsstellen täglich millionenfach das Ziel, allein auf die Rechner des Verteidigungsministeriums zählte man pro Stunde 250 000 Angriffe.

Investitionen trotz Budgetkürzungen

Bei allen Kürzungen im Militärhaushalt will Obama in den nächsten Jahren 18 Mia US Dollar in Cyber-Abwehr investieren. Die Anzahl der wirklich qualifizierten Spezialisten in Cyber-Sicherheit der USA beträgt rund 1000, benötigt werden aber 20 000 – 30 000! Unlängst gestand ein früherer CIA-Chef ein, «wenn wir uns heute im Cyberwar befänden, würden wir ihn verlieren». Ein solcher ist kein Krieg im herkömmlichen Sinn, kann indes die gleiche Wirkung haben, bis hin zur existenzbedrohenden Gefährdung eines Staates. Er kennt keine Kriegserklärung, keinerlei Verletzung einer territorialen Integrität, selbst ein Schusswechsel ist nicht erforderlich. Es gibt keinen offenen Kampf, eher Guerilla-style Angriffe. Diese können von überall erfolgen, Entfernungen sind bedeutungslos. Der Angreifer will möglichst verborgen bleiben. NSA behauptet, sie könne ihn stets aufspüren, doch dürfte das nicht immer zutreffen; man kann eine solche Schadsoftware zudem über sehr viele Umwege versenden. Die Frage ist, ob man ein derartiges Vorgehen als Krieg ansehen kann und dann das Kriegsrecht im Sinne der § 33, 41 und 51 der UNO-Charta gilt. Darüber herrscht keine einheitliche Auffassung. Bejaht wird es von den USA und Russland bei Verletzungen der kritischen Infrastrukturen (Energieversorgungen, Telekommunikationsnetze, Kernkraftwerk), kurz die Lebensadern eines Staates. China, aber auch viele europäische Staaten weichen einer direkten Antwort aus.

China, Russland, Iran

Die häufigsten Attacken erfolgen von der VR China, die schon recht früh deren Bedeutung erkannt hatte. Ihren Militärpublikationen waren bereits vor etwa 20 Jahren Sätze zu entnehmen wie «Hacker könnten die Helden des nächsten Krieges» sein. Die III. Abt. des Verteidigungsministeriums in Beijing ist dafür verantwortlich, sie soll 6000 Experten umfassen; die Gesamtzahl der Cyberwar-Soldaten wird auf 200 000 geschätzt. Zumeist arbeiten diese über Beijing, Shanghai und Quanzhou. Vor wenigen Monaten enttarnte ein US-Computersicherheitsunternehmen deren «Einheit 61 398» in einem Hochhaus am Stadtrand von Shanghai. Einem deutschen Verfassungsschutzbericht zufolge haben deren Ausspähungsaktivitäten inzwischen qualitativ ein Niveau erreicht, wie es vor kurzem noch undenkbar war.

Moskauer Akademie der Wissenschaften. Bild: Wikipedia

Weniger aktiv, aber raffinierter erscheint die russische Cyber-Strategie. Nach aussen trat dabei früher oft die Moskauer Akademie der Wissenschaften auf, heute sind die Hacker im Dienst der Auslandspionage als Privatfirmen getarnt. Deutsche Regierungsstellen registrieren in jüngster Zeit drei bis fünf Attacken pro Tag.

Seit Herbst 2012 spüren primär die USA ebenfalls Cyber-Angriffe des Irans. Diese legten Online-Angebote wichtiger Banken teilweise für Tage lahm und verschafften sich Zugang zu Software, mit der sie amerikanische Öl- und Erdgasleitungen manipulieren könnten.

Sabotage, Spionage

Je technisch entwickelter ein Staat ist, umso verwundbarer ist er zugleich. Wer in Computer eindringt, kann mit Sabotageprogrammen den Absturz aller elektronischen Systeme herbeiführen. In der Nähe von Frankfurt am Main befindet sich eine Einrichtung der Deutschen Bahn; eine Sabotage würde zum sofortigen Stillstand sämtlicher in Deutschland fahrenden Züge führen. In ähnlicher Weise würde ein Anschlag auf den Bahnhof Olten eine Lähmung des Bahnverkehrs bewirken. Im Juni 2010 infiltrierte der Cyber-Wurm Stuxnet die Uran-Anreicherungsanlage im iranischen Natanz und warf das gesamte Atomprogramm Teherans um Jahre zurück. In den Niederlanden lähmte ein Computervirus unbekannter Herkunft vergangenen Sommer das Alltagsleben. Die grösste Sorge dabei war, die Täter könnten ebenfalls Zugriff auf die Schleusen-, Brücken- und Deichsteuerungen bekommen; in diesem Fall wären sie in der Lage, Schleusen zu öffnen und ganze Landstriche Hollands zu überfluten.

Überaus gefährlich sind Schläferviren, die erst zu einem im Voraus bestimmbaren späteren Zeitpunkt ihre Zerstörungskraft entfalten. Stellt ihr Ziel etwa die wichtigsten Bahnhöfe eines Landes dar und sind alle auf eine bestimmte Stunde eingestellt, wird sich ein Chaos kaum vermeiden lassen. Sabotage soll zerstören, den Angegriffenen militärisch oder wirtschaftlich schwächen. Derartige Aktionen sollen indes Panik, eine psychologische Lähmung erzeugen. Sollten sie durch weitere Attacken – wie 2007 gegen Estland – für Wochen anhalten, wird die Widerstandskraft bei vielen Menschen nur noch recht minimal sein.

Gefährliche Cyber-Spionage

Inzwischen hat sich die Cyber-Spionage als viel gefährlichere Waffe erwiesen. Wirkungsvoller Virus scheint gegenwärtig «Flame» zu sein, der drei Jahre lang völlig unerkannt arbeitete und erst 2012 entdeckt wurde. Er ist ein Autospion, sucht nach einem Mikro auf dem infizierten Rechner, schaltet es ein und zeichnet alle Gespräche im Raum auf. Primär für Beijing dürfte generell das Ausspähen von Industrieanlagen und Produktionsprozessen speziell in der Informationstechnologie sein. Es geht um geistiges Eigentum, Patente und Baupläne. In Deutschland tauchten chinesische Spionageprogramme sogar im Bundeskanzleramt auf. Anonyme Hacker drangen in Fahndungscomputer der dortigen Bundespolizei ein, die als die sichersten der Welt gelten! Teile des Regierungsnetzes Kanadas waren letztes Jahr das Ziel solcher Attacken. Erfolglos blieb der Angriff auf eine Firma in Toronto, die Blaupausen für mehr als die Hälfte aller Öl- und Gaspipelines in Nord- und Südamerika verwaltet. Australiens Regierung warnte vor Versuchen Beijings, die Rohstoffquellen des Kontinents auszuspionieren. Ende Mai gelang es einem Hacker, Kopien der Baupläne für die neue Zentrale des Abwehr-Geheimdienstes zu erlangen.

Der Cyber-Krieg umfasst heutzutage nahezu den gesamten Erdball. Viele Angriffe werden nicht bemerkt. Extrem hoch schätzen die Experten die Dunkelziffer bei Wirtschaft und Technik, welche aus Imagegründen die Öffentlichkeit scheuen, sowie bei Staaten, die derartige Vorkommnisse aus Geheimhaltungsmotiven verschweigen. Das ist die Welt, in der wir heute leben; ob wir die Fakten sehen oder auch nicht zur Kenntnis nehmen wollen, bleibt ohne Belang. Es ist die Realität! Deutschland registrierte letztes Jahr fast

Fort Meade, Zentrale des US Cyber Command. Bild: NSA

1100 digitale Angriffe allein auf seine Bundesregierung. Gegenwärtig erfolgen von russischer Seite pro Tag drei bis fünf Attacken auf Bundesstellen. Der Schaden deutscher Unternehmen allein durch Hacker Beijings soll jährlich rund 50 Mia Euro betragen. Führend in der Abwehr ist das Bundesamt für Sicherheit in der Informationstechnik mit seinen 550 Mitarbeitern; ob man auf ernste Cyber-Schläge genügend vorbereitet ist, muss eher bezweifelt werden. Die Bundeswehr mit ihrer Spezialabteilung CNO ist angeblich auch zu Gegenangriffen auf feindliche Netzwerke in der Lage. Österreichs jüngster Jahresbericht des Verfassungsschutzes beklagt, Cyber-Angriffe mit politisch-strategischem Hintergrund hätten sich gehäuft, sie seien heute komplexer denn je. Bei der Internationalen Atomenergiebehörde in Wien wurden Kontaktdaten von Wissenschaftlern gestohlen und über das Internet mit Erpressungen gedroht. Im August 2012 wurden 30000 Computer staatlicher saudi-arabischer Ölfirmen von einer Gruppe «Cutting Sword of Justice» zerstört, deren Formulierung auf den Iran hindeutet. Wenige Monate danach legten dortige Hacker die Rechner der israelischen Polizei lahm.

Indien und Korea

Neuerdings versucht ebenfalls Indien durch Cyber-Ausspähbemühungen im Westen seinen Technologiestand zu verbessern. Für die eigenen Cyber-Sicherheit, besonders gegenüber China aber auch Pakistan bildet es zusammen mit der Privatwirtschaft 500000 Fachleute aus.

Nordkorea begann seinen elektronischen Krieg gegen den Südteil des Landes bereits 1998 mit der Abt. 121, welche dem militärischen Geheimdienst Pjöngjangs untersteht. Die Zahl der Hacker wird auf 3000 geschätzt; insgesamt sollen derartige Einheiten etwa 12000 Soldaten umfassen. Während der jüngsten Jahre attackierten sie mehrfach die Webseite des südkoreanischen Präsidenten sowie diejenige der wichtigsten Ministerien. Ebenso erfolgten Einbrüche in das Netzwerk der Armeecomputer sowie in die Webseiten des US-Militärs. Im März 2013 wurden mehrere Fernsehsender und Banken lahmgelegt und dabei 48700 Computer und Bancomaten beschädigt. Nach Mitteilung des Seouler Abwehrdienstes beläuft sich die Durchschnittszahl der Versuche, im Süden militärische Informationen zu hacken, auf täglich über 93000.

Aufgrund immer neuer technischer Entwicklungen gibt es im heutigen Cyberwar keine vollständige Sicherheit. Auch Firewalls können Angriffe letztlich nur erschweren, zudem müssen sie stets auf den neuesten Stand eingestellt sein. Seit kurzem bauen die USA das Utah Data Center aus. Es soll das Land in die Lage versetzen, weltumspannende Informationsoperationen zur Abwehr von Cyber-Attacken durchführen zu können. Ebenfalls arbeiten die USA an einem Quantencomputer, von dem man sich grösste Sicherheit verspricht.

Bestrebungen, der rasanten Entwicklung auf diesem Gebiet Einhalt zu gebieten – durch die Errichtung einer weltweiten Cyber-Behörde – blieben bisher ohne konkrete Erfolge. Wohl gibt es zahlreiche Versuche, im Rahmen der UNO Gespräche zu führen, doch ist kein Land bereit, auf seinen tatsächlichen oder auch nur un-

terstellten Vorsprung zu verzichten. Angesichts des beträchtlichen Misstrauens zwischen den führenden Cyber-Mächten kommt bei Vorstössen gegen geschlossene Verträge die sehr bedeutsame Problematik der notwendigen Kontrollmöglichkeiten, welche bis dato überaus unsicher erscheinen sowie diejenige von wirksamen Gegenmassnahmen. Der Vorschlag Moskaus nach einem totalen Verbot der militärischen Nutzung des Weltraums erscheint angesichts der in der Zwischenzeit eingetretenen Situation längst realitätsfremd.

Elektronisches Pearl Harbor?

Umfragen in 64 Ländern aus jüngster Zeit ergeben bei 84 % der Befragten eine mangelhafte Informationssicherung. Lediglich bei rund der Hälfte der Firmen zeigte deren Führungsebene überhaupt Interesse an einer Datensicherung. Aber auch bei Behörden sowie im Militär sind oftmals die Probleme der konkreten Zuständigkeit und der Koordinierung nicht genügend festgelegt.

In der Schweiz erfolgen nach Auskunft Berner Sicherheitsstellen solche Cyber-

Cyberwar Einheit 61 398 in Shanghai.
Bild: NY Times.com

Anschläge täglich. Markante Beispiele sind die Hacker-Attacken vor Jahren auf die Webseite der Bundesverwaltung und 2010 auf das EDA. Zwei Jahre lang konnte ein Trojanisches Pferd die UNO-Verwaltung in Genf ausspionieren. Der folgenreiche Angriff auf einen in der Schweiz ansässigen Anti-Spam-Dienst im April 2013, welcher zeitweilig Auswirkungen auf das gesamte Internet hatte, kam von russischen Hackern. Es gibt selbst in der Schweiz Unternehmen die für das WC-Papier ihrer Belegschaft mehr bezahlen, als für die Sicherheit ihres Betriebes! Es fehlt sehr häufig an einem tieferen Verständnis für die für jedes Land bestehenden Gefahren und damit ein Gefühl für die Notwendigkeit von Sicherheitsmassnahmen. Vielleicht ist es ebenfalls ein Generationenproblem? In demokratischen Staaten, in denen generell Offenheit und Sorglosigkeit herrschen, wird ein verändertes Verhalten nicht leicht zu erreichen sein. Im jetzigen Zeitalter von Hackern, Würmern und Trojanern ist indes schon bei geringsten Merkwürdigkeiten im Internet stets Misstrauen angebracht! Im Gegensatz zu früheren Jahren hat die Bevölkerung der USA die Situation erkannt, in Europa fehlt es nicht selten an einer öffentlichen Aufklärung. Muss erst ein elektronisches Pearl Harbor wie 1941 geschehen, um Politik, Militär und Wirtschaft wachzurütteln? Für viele wäre es dann – wie damals – zu spät … ■

Friedrich-Wilhelm
Schlomann
Dr. iur utriusque
D-53639 Königswinter