MANFRED KLOIBER, JAN RÄHM, PETER WELCHERING

Bits und Bomben

Cyberwar: Konzepte, Strategien und reale digitale Kontroversen

AVM

Bits und Bomben

Manfred Kloiber, Jan Rähm, Peter Welchering

Bits und Bomben

Cyberwar: Konzepte, Strategien und reale digitale Kontroversen

AVM

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

e-ISBN (ePDF) 978-3-96091-215-6
ISBN (Print) 978-3-86924-325-2

Verlagsverzeichnis schickt gern:
AVM – Akademische Verlagsgemeinschaft München
Schwanthalerstr. 81
D-80336 München

www.avm-verlag.de

Inhalt

Vorbemerkung

World Wide War, Cyberwar, das Internet als digitales Schlachtfeld – Politiker, Militärs und selbsternannte Sicherheitsexperten fordern die massive Nachrüstung in Sachen Computerwaffen. Die Bedrohung kommt wahlweise als China, Russland oder Nordkorea, seit neuestem auch aus dem Iran. Vor dem digitalen Erstschlag auf die sogenannten kritischen Infrastrukturen wird gewarnt, aber es wird nicht über eine Defensivstrategie nachgedacht, sondern über Angriffsszenarien. Wenn mit Computerwaffen die Stromversorgung in Westeuropa ausgeknipst würde, wenn unser Finanz- und Bankensystem dank eines feindlichen Computervirus gecrasht ist, wenn Industrieanlagen in die Luft fliegen, weil logische Bomben gezündet wurden, dann steht tatsächlich das Leben von vielen Millionen Menschen auf dem Spiel.

Die Gefahr eines digitalen Anschlags ist real. Das bezweifelt selbst der paläokonservativste Sicherheitspolitiker nicht mehr. Monat für Monat erfolgen mehrere Dutzend ernst zu nehmende digitale Angriffe auf die Lebensadern unserer modernen Gesellschaft. Die Täter sind in der Regel nicht auszumachen. Nur selten werden diese Angriffe konsequent zurückverfolgt. Im Falle von Stuxnet hat der amerikanische Journalist David E. Sanger zwei Jahre gebraucht, um die amerikanisch-israelische Urheberschaft dieser Waffe nachzurecherchieren. Die Konsequenz: Regierungsstellen in den USA versuchen nun, derartige Recherchen mit winkeladvokatorischen Tricks zu unterbinden, nachdem auch im Falle Sanger die Geheimdienste versagt haben. Es wird also auf der politisch-administrativen Ebene alles getan, um den Einsatz digitaler Waffen zu vertuschen. Häufig tarnen sich die Täter mit aufwändigen technischen Mitteln. Der amerikanische Sicherheitsexperte Richard Clarke fordert deshalb neue Offensivstrategien, weil die bloße Verteidigung gegen Cyberangriffe nicht mehr ausreiche, um einer digitalen Gesellschaft das Überleben zu sichern. Innerhalb der NATO wird darüber nachgedacht, digitale Angriffe mit konventionellen Luftschlägen und dem Einsatz von Kampfpanzern zu beantworten. Und im bundesrepublikanischen Verteidigungsministerium geben sich die Lobbyisten der digitalen Waffenindustrie die Klinke in die Hand, um ihre Cyberwaffensysteme an den Mann zu bringen.

Die Nachrichtendienste machen da gern mit und stimmen in den Chor der Kassandrarufe mit ein. Lassen sich doch auf diese Weise zumindest die vom Vermerk „künftig wegfallend“ bedrohten Planstellen sichern, wenn nicht sogar neue Abteilungen mit klingenden Namen, wie zum Beispiel „digitale Proliferation“, aufbauen. Darin sieht insbesondere der seit dem NSU-Skandal noch unglücklicher als sonst agierende Bundesnachrichtendienst eine Überlebensstrategie. Nachdem Militärs und Geheimdiensten mit dem Ende des Kalten Krieges der Feind abhanden gekommen war, die Rüstungsindustrie ihre satten Zuwachsraten im Geschäft mit den eigenen Militärs ein wenig „downsizen“ musste, und der militärisch-industrielle Komplex sich schon zumindest so bedroht sah wie den Juchtenkäfer im Stuttgarter Schlossgarten, bringt der Cyberwar neue Hoffnung. Endlich ist wieder ein Feindbild verfügbar, das man kommunizieren kann. Zwar bleibt der feindliche Cyberkrieger noch ein wenig unscharf und blass. Aber dann muss die Regierung eben ein wenig Geld in die Hand nehmen, um dieses Feindbild zu schärfen. Bundesnachrichtendienst und Militärischer Abschirmdienst verfügen über ausreichend Analytiker, die seit dem Ende des Kalten Krieges ihre tägliche Zeitungslektüre nicht mehr ausreichend verkauft bekamen und die hier eine OSINT-Operation starteten, um den Cyberfeind genauer beschreiben zu können. Das Kürzel „OSINT“ steht dabei übrigens für „Open Source Intelligence“ und umfasst die Auswertung von öffentlich zugänglichen digitalen Quellen, vorzugsweise die Recherche in sozialen Netzwerken, in die bundesdeutsche Nachrichtendienste im Jahr 2010 rund 180 Millionen Euro investierten.[1]

Ein nicht unerheblicher Teil dieses Geldes fließt an Informanten, die spannende Web-Adressen zuliefern, Sicherheitsberater, die den Mitarbeitern der Dienste zeigen, wie man Software für den File Transfer bedient und welche Sicherheits-Plugins der jeweilig benutzte

[1] Zahlen für das Jahr 2011 sind noch nicht vollständig recherchierbar. Die Zahl für das Jahr 2010 wurde auf der gemeinsamen Tagung der Sicherheitsbevollmächtigten der Landesämter für Verfassungsschutz in Baden-Württemberg und Bayern am 5. und 6. April 2011 in Friedrichshafen genannt. Der diese Zahl Vortragende darf aus rechtlichen Gründen nicht identifizierbar genannt werden. Siehe auch Bundestags-Drucksache 17/10077, hier sind die im Bereich des Bundesministeriums des Inneren verwendeten Mittel für Nachrichtendienste genannt, teilweise bis in das Jahr 2002 zurückgehend.

Browser benötigt, sowie nicht näher bezeichnete „Quellen“, die ihren nachrichtendienstlichen Aufklärer und mitunter Führungsoffizier in einer Person auch im unübersichtlichen sozialen Netzwerk an den Ort des spannenden Geschehens bringen.

Entsprechend bunt wird dann auch das konkrete Feindbild. Denn wenn zur umfassenden digitalen Ausforschung der „Yahoo Boys aus Nigeria“ schon satte 19.000 Euro an diverse Quellen fließen, dann müssen die Jungs auch in digitaler Hinsicht ausreichend feindlich sein. So wird zumindest für die Schlapphüte der Cyberkrieger dann doch nur wieder zum bösen schwarzen Mann. Aber: Vorsicht! Hinter den Yahoo-Boys aus Nigeria steht natürlich wahlweise der Russe oder Chinese, und wenn es politisch gar nicht anders geht, auch schon einmal der Nordkoreaner.

Auch der Innenpolitik tut das neue Feindbild des Cyberkriegers gut. Denn hier mutiert der Digitalkrieger rasch zum Cyber-Terroristen mit entsprechender Unterstützung durch virtuelle und andere Sympathisanten, die dann den Einsatz des Bundes-Trojaners, Vorratsdatenspeicherung und verdeckte Sonderermittler in sozialen Netzwerken nötig machen.

Der Cyberkrieg mit seinen zivilen Abwandlungen sorgt also im gesamten Sicherheitsbereich für Konjunktur. Positiv daran muss man sehen, dass so mancher ehemalige Stasi-Mitarbeiter und die unfähigsten der Verfassungsschützer durch diese Entwicklung von der Straße weg sind und dort keinen Unfug mehr anrichten können. Allerdings trägt diese Entwicklung kaum dazu bei, dass den wirklich großen Gefahren von Angriffen auf unsere Infrastrukturen etwas entgegen gesetzt wird. Eine durchdachte Strategie fehlt völlig und wird sogar verhindert, wenn Militärs und Nachrichtendienste ihre Interessen dadurch bedroht sehen.

Digitale Angriffsprogramme nutzen Sicherheitslücken in den Betriebssystemen, in Anwendungsprogrammen und in den verwendeten Protokollen aus. Um sich gegen solche Angriffsprogramme zu verteidigen, hilft nur eines: Sicherheitslücken, so gut es eben geht, aufspüren und öffentlich machen, damit sie geschlossen werden können. Das aber verhindern Militärs, Nachrichtendienste und Sicherheitsbehörden in seltener Eintracht. „Glauben Sie, ich lasse die Sicherheitslücke schließen, die wir ausnutzen, um den digitalen Torpedo zu entwickeln“ fragte in rhetorischer Absicht ein Offizier der in Rheinbach bei Bonn ansässigen Cybereinheit der Bundeswehr die Autoren nach einem Vortrag über Sicherheitslücken. Und wir mussten zugeben, in projekttaktischer Hinsicht können wir diesen Offizier verstehen. Denn er will die Planstellen und Budgets für das Projekt „digitaler Torpedo“ möglichst für die nächsten zwei Jahre absichern. Dafür muss er Erfolge bei der Entwicklung vorzeigen. Diese Erfolge werden zunichte gemacht, wenn die Basis seines digitalen Torpedos, nämlich die von dieser Angriffssoftware ausgenutzte Sicherheitslücke geschlossen würde. Hier herrscht noch ein altes sicherheitspolitisches Paradigma vor, das allerdings in Zeiten digitaler Angriffe zu einem echten Sicherheitsrisiko wird. Und weil auf dieser Basis auch Projekte wie die heimliche Online-Durchsuchung beruhen, setzt der Sicherheitskomplex in dieser Republik alles daran, um zu verhindern, dass Sicherheitslücken nachhaltig aufgedeckt, veröffentlicht und somit geschlossen werden. Eine zweite Entwicklung spielt diesem Unsicherheitsfaktor in die Hände. Weder das Transport Control Protocol noch andere Mitglieder der Internet-Protokollfamilie waren jemals für Einsätze in sicherheitskritischen Bereichen ausgelegt. Wenn aber nun Lastverteilungsrechner des Stromnetzes am Internet hängen, Fabrikanlagen über das Internet ferngewartet werden und die Versorgung ganzer Staaten von Internetverbindungen ohne ausreichende Redundanzen und ohne ausreichende Sicherheitssysteme abhängig ist, schaffen wir einen Hochrisikobereich, den wir nicht mehr beherrschen können.[2]

[2] Siehe z.B. Bundestags-Drucksache 17/5672, 17. Wahlperiode 27. 04. 2011, Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung Technikfolgenabschätzung (TA), TA-Projekt: Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung.

So tritt neben die Forderung zur Systemtransparenz, um Sicherheitslücken rasch erkennen und schließen zu können, die Forderung nach Entnetzung von kritischen Infrastrukturen. Natürlich können wir uns nicht mehr den schon seit Jahrzehnten wegrationalisierten Wartungsfahrer in einer Raffinerie einfach zurückwünschen, damit die Fernwartung mit ihren Risiken entfallen könnte. Wir können und müssen uns aber die Frage stellen, ob die Fernwartung einer Pipeline unbedingt über das hochgradig unsichere und für derartige Anwendungen nicht vorgesehene Internet laufen muss, oder ob dafür nicht der Aufbau einer internetunabhängigen Infrastruktur mit jeweils eigenen Sicherheitsvorkehrungen empfehlenswert ist.

Entnetzung ist sicherlich kein Allheilmittel, aber Entnetzung vom Internet meint die Diversifizierung von Netzstrukturen, damit Sicherheitsrisiken ausgeschaltet werden können, die eine zu stark eindimensional ausgerichtete Vernetzungsidee mit sich bringt. Zumindest sollte einmal vorurteilsfrei geprüft werden, ob eine derartig ausgerichtete Sicherheitsstrategie nicht der vor allen Dingen von amerikanischer Seite zunehmend geforderten Offensivstrategie der Vernetzung von konventionellem Krieg und digitalem Erstschlag überlegen ist. Sie ist zugegebenermaßen ziviler und deshalb viel weniger martialisch. Das vermögen wir aber als Nachteil noch nicht so richtig zu erkennen.

Allerdings können wir einem Argument, das ein Mitarbeiter des amerikanischen Denkfabrik Brookings Institution uns in einer Diskussion über sicherheitspolitische Paradigmen mitgab, nichts entgegensetzen. Dieser brillante Analytiker fragte: „Was sollen dann die ganzen Thinktank-Mitarbeiter machen, die bisher ihr Geld mit dem Verfertigen von Strategien für den digitalen Erstschlag und das Gleichgewicht des Cyber-Drohpotentials verdient haben? Die würden doch wieder beschäftigungslos wie Anfang der 1990er-Jahre“.

Da hat der Mann einfach Recht. Und er hat auch Recht, dass viele arbeitslose Analytiker der Denkfabriken und der Geheim- und Nachrichtendienste in dieser Zeit Unterschlupf in der organisierten Kriminalität fanden. Doch bei Licht besehen, hat die organisierte Kriminalität darunter mehr gelitten als profitiert. Dieser sicherheitspolitische Aspekt ist meines Erachtens bisher überhaupt noch nicht bedacht

worden. Nicht bedacht worden ist auch, dass sich mittlerweile nicht nur eine ganze Industrie etabliert hat, die von tatsächlichen oder nur als Szenario erdachten Cyberattacken sehr gut lebt, sondern, dass die Gefahr, die von Cyberattacken ausgeht, auch immer stärker in der politischen Diskussion genutzt wird, um Grundrechte teilweise außer Kraft zu setzen und Freiheitsrechte der Bürger zu beschneiden.

Weil inzwischen sehr viele Interessen mit dem Geschäft um Bits und Bomben verwoben sind, zahlreiche politisch-ideologische Bewegungen dahinter stehen, gute Geschäfte mit Cyberattacken gemacht werden, ist eine Gemengelage entstanden, die eine internationale digitale Rüstungskontrolle wirkungsvoll verhindert. Verhindert wird auch eine durchdachte Sicherheitsstrategie. Die damit befassten Behörden auf Bundes-, Landes- und regionaler Ebene fürchten, dass bei einer transparenten Diskussion der informationstechnischen Sicherheitslage ihre völlige Unfähigkeit in Sachen Bevölkerungsschutz und Daseinsvorsorge dokumentiert wird. Die politischen Eliten zahlreicher Länder sehen in den digitalen Waffen ein wirkungsvolles Instrument politischer Machtausübung. Und Militärs haben schon immer gern mit neuen Waffen herumgespielt – einfach weil sie es können.

Die Situation ist also bedrückend bis gefährlich. Vor allen Dingen muss hier für Aufklärung gesorgt werden. Wie digitale Waffen funktionieren, welche Szenarien im Cyberkrieg es gibt und welche Spieler hier welche – auch politischen – Spielchen spielen, ist oftmals einfach nicht bekannt. Vielleicht können wir mit „Bits und Bomben“ einen kleinen Beitrag dazu leisten.

1. Der Digitale Erstschlag und die Folgen

Solange die Option des atomaren Erstschlags die Sicherheitsdoktrin der USA wie Russlands beherrschte, war für die Militärstrategen in Ost und West die Welt in Ordnung. Denn den atomaren Erstschlag konnte man durch ein ausreichend aufgefächertes Drohszenario verhindern. Solange dem Staat, der den Erstschlag auslöste, die weitgehende Vernichtung durch einen rechtzeitig eingeleiteten Gegenschlag drohte, sorgte eine Art Gleichgewicht des Schreckens für eine gewisse Stabilität. Dieses Szenario möchten die führenden Sicherheitsstrategen gern auf den Cyberkrieg übertragen und müssen dabei voller Entsetzen feststellen, dass die gegenseitige Neutralisierungsstrategie hier nicht funktioniert. Der digitale Erstschlag findet immer in einem asymmetrischen Bedrohungsszenario statt. Es gibt in der Regel keine Vorwarnzeiten und die Angreifer haben sich in der Vergangenheit nicht zu erkennen gegeben, sondern vielmehr alles daran gesetzt, um zu verschleiern, woher der digitale Angriff kam.

Ein solcher digitaler Erstschlag hat zum Beispiel im Jahr 1982 stattgefunden. In Russland explodierte eine Verdichtungsstation an der Chelyabinsk-Pipeline. Der damalige KGB-Mitarbeiter Alexej Momot wurde mit einem Team von vier Softwareexperten, die allesamt am Moskauer Institut für Strahlenphysik, der damaligen Elite-Schmiede für Programmierer, ausgebildet worden waren, zwei Tage nach dem Unglück mit der Untersuchung der Unglücksursache beauftragt.[1]

Zu dieser Zeit stand fest, dass die Explosion in der Verdichtungsstation nicht durch konventionellen Sprengstoff ausgelöst worden war. Man vermutete vielmehr einen Softwarefehler. Momot forderte aus Prag zwei weitere Experten für das „Reverse Engineering“ an. Unter

[1] Hintergrundgespräche mit Peter Welchering am 11.12.1989 in Moskau. Die Informationen von Momot sind in zahlreichen Beiträgen für den Norddeutschen Rundfunk verarbeitet worden. Alexej Momot alias Oleg Levner ist nicht zu verwechseln mit Alexander Momot, dem Geschäftsführer des Herstellers Intercomputer, der in den 90er Jahren in den Hack der Hannover-Connection hineingezogen wurde. Die damals geäußerten Anschuldigungen konnten nicht erhärtet werden.