Aleksandra Sowa

Stern des Krieges

Wie die Digitalisierung die moderne Kriegsführung verändert

Hinter dem vielzitierten sogenannten »Cyberkrieg« verbirgt sich heute zweierlei: einerseits die Hoffnung der Menschen, einen Krieg ohne menschliche Verluste führen und gewinnen zu können, und andererseits die Angst, dass, wer auch immer die Waffensysteme in die kalten Hände von Robotern legte, die Menschheit einem unkalkulierbaren Risiko aussetzen würde.

Auch wenn der Einsatz von humanoiden Robotern als Soldatenersatz eher noch in weiter Ferne zu liegen scheint, funktionieren heute fast alle Waffensystem mit internetbasierter Technologie. Ohne das Netz wären die meisten von ihnen genauso wenig funktionsfähig wie Google oder Facebook. »Die Vernetzung der modernen Militärtechnik ist zugleich die Achillesferse moderner Hightech-Rüstung«, schreiben Stefan Aust und Thomas Ammann in ihrem Buch *Digitale Diktatur.*

Manchmal reichen schon einige interessierte Hacker, um eine Waffe außer Betrieb zu nehmen. Auf der Konferenz *Black Hat USA 2015* präsentierte ein Hackerpaar, wie man über die Netzverbindung die gesamte Zielautomatik eines smarten Scharfschützengewehrs der Firma TrackingPoint dauerhaft unbrauchbar machen kann. Die Hacker konnten sich als Superuser in die Linux-Software einwählen und Zugriff auf die Funktionen der Waffe erlangen. Es gelang ihnen u.a., das Zielfernrohr zu deaktivieren, die Feuersperre zu lösen, das Gewicht der Munition oder die Windstärke zu manipulieren. Das Einzige, was den Hackern nicht gelang, war das Auslösen eines Schusses. Dazu braucht auch ein smartes Gewehr einen Schützen, der den Abzug manuell betätigt. Noch, jedenfalls.

Die Sicherheitslücke, die es den beiden Hackern ermöglichte, in die Funktionen der Waffe einzudringen, lag in der WLAN-Verbindung, die aktiviert wurde, um beispielsweise Bilddaten eines Schusses auf einen Computer zu übertragen. Diese nutzte ein Standardpasswort für den Verbindungsaufbau. Das reichte den Hackern, um in das System einzudringen und die Waffe in ihre Gewalt zu bringen.

Doch die Nutzer der TP 750, wie diese moderne, netzfähige Waffe heißt, hatten Glück. Die Hacker haben nicht nur ihre Ergebnisse veröffentlicht und TrackingPoint darüber in Kenntnis gesetzt, sie arbeiteten auch gemeinsam mit dem Hersteller an einem Update, mit dem die Sicherheitslücke geschlossen werden sollte.

»Ich selbst hacke heute nur noch legal«, bekannte sich kürzlich der Hackerkönig John Draper alias Captain Crunch. Der heute 72-Jährige verdankt seinen Namen dem spektakulären »Hack« aus den späten 60er Jahren. Mithilfe einer Plastikpfeife, die damals jeder Packung der Cap'n Crunch Frühstücksflocken beilag, und mit einer Frequenz von 2.600 MHz, mit der er in die Telefonhörer pfiff, trickste er die Telefonsysteme aus und konnte so unbegrenzte Gratis-Gespräche führen.

Als sein Hack aufflog, musste er ins Gefängnis, obwohl er indirekt den Telefongesellschaften geholfen hatte, die Schwachstellen in ihren Systemen aufzudecken und die Systeme sicherer zu machen. Deswegen hacken heute viele wie Captain Crunch nur noch legal, nicht selten nur noch geschäftsmäßig. Auch das legendäre Hackerkollektiv Anonymous wurde in den vergangenen Jahren durch Festnahmen seiner besten Hacker stark geschwächt. Ein großer Teil der frühen Hacker-Elite darf sich aufgrund

von Verurteilungen und laufenden Ermittlungen dem Rechner bis auf Weiteres nicht nähern. Viele Hacker sind aus dem Untergrund aufgetaucht und betreiben nun kommerzielle Firmen, die im Auftrag der Unternehmen oder Behörden gezielte Attacken simulieren und Stresstests durchführen. Wie beispielsweise die professioneller und geschäftsmäßiger auftretende Ghost Security Group, die sich von der aus Anonymous-Aktivisten hervorgegangenen Gruppe Ghost Security (GhostSec) abgespalten hatte.

Krisen, wie die Terroranschläge in Paris, ebnen Wege für überraschende quasilegale Allianzen. Anonymous, einst der Staatsfeind Nummer eins der US-Behörden, arbeitet nun im Kampf gegen die Terrororganisation Islamischer Staat der Bundespolizei FBI und den Geheimdiensten zu. »Anonymous erklärt dem Islamstaat den Krieg« – so kommentierten die Medien das kurz nach den Anschlägen in Paris von der Hackergruppe Anonymous auf YouTube veröffentlichte Video. Darin kündigt ein mit Guy-Fawkes-Maske verhülltes Gesicht an, gezielte Angriffe auf islamistische Websites und die elektronische Kommunikation mit islamistischen Inhalten zu starten.

Mit den Operationen unter den Hashtags #OpParis und #OpISIS kündigte Anonymous an, die Internetplattformen mit islamistischen Inhalten aufzuspüren und systematisch zu zerstören. Dabei sollen die Betreiber und Nutzer von Seiten, hinter denen Mitglieder oder Sympathisanten des IS vermutet werden, entlarvt und veröffentlicht werden. Auch die Propagandavideos im Internet sind das Ziel der Aktivisten. Die Mitglieder von Anonymous sammeln außerdem Namen von Twitter-Accounts mit islamistischen Inhalten und übergeben sie den US-Behörden. Mehrere Tausende dieser Accounts sollen inzwischen von den Betreibern oder von der Polizei vom Netz genommen worden sein.

Das YouTube-Video und die Begleitung auf Twitter unter #OpParis und #OpISIS gelten als Aufruf an die Hacker-Gemeinde, sich an den Attacken auf die islamistischen Inhalte im Netz zu beteiligen. Jeder, der weiß, wie es geht, kann mitmachen. Es gibt des Weiteren passende Anleitungen im Netz: »The Noob Guide« für Anfänger, in denen die Nutzung von TOR (einem Netzwerk zur Verschlüsselung von Verbindungsdaten) und die Grundlagen der DDoS-Attacken (Distributed Denial of Service – Verweigerung des Dienstes) erläutert werden (nicht anwenden ohne vorherige Anleitung!), »Twatter Reporter« hilft, die IDs der ISIS-Twitter-Accounts zu identifizieren, und »Search Terms« findet Websites mit ISIS-Inhalten. Mit den Anleitungen kann man üben. Doch von der eigenständigen Durchführung von DDoS-Attacken wird den jungen Adepten der Hacker-Kunst abgeraten. Der Grund liegt auf der Hand: Es sind viele in der Lage, in die Systeme einzubrechen – aber nur wenige wissen, wie man seine Spuren nach dem Hack verwischt und eine Zurückverfolgung unmöglich macht.

Hacken gegen den IS

Oder wie man, völlig unbeobachtet, eine »Cyberbombe« im System des Feindes platziert, die dann bei Bedarf aktiviert werden kann, oder die ihren Weg auf der Suche nach dem vorgegebenen Ziel durch die Netze, durch zufällig ausgesuchte Computer und Datenträger nimmt. »Viren und Würmer«, schreiben Aust und Ammann in *Digitale Diktatur,* »können im Kampf David gegen Goliath zu gefährlichen Waffen werden«.

Das Beispiel des den US-amerikanischen und israelischen Geheimdiensten zugeschriebenen Computerwurms Stuxnet, der zur Manipulation der iranischen Urananreicherungsanlagen eingesetzt wurde, zeigt nicht nur, wie sich eine zum Cyberangriff konzipierte Software der Kontrolle ihrer Schöpfer entziehen und sich »verselbstständigen« kann. Es zeigt auch, dass Erstschläge mit Cyberwaffen unvorhergesehene Reaktionen provozieren können. So warnte der ehemalige US-Verteidigungsminister

Leon Panetta vor einem »Cyber-Pearl-Harbor«, einem Überraschungsangriff also, der zu Zerstörung und zum Verlust von Menschenleben führen könne.

Die Vision des sauberen, weißen Computerkrieges – oder »Softkrieges«, wie ihn einer der berühmtesten deutschen Hacker der 80er Jahre, Karl Koch, nannte –, der nur mit Viren und Würmern, von der Konsole eines Rechners aus, mit einer Drohne oder einer Waffe gesteuert wird, scheint nicht ganz in Erfüllung zu gehen. Heute ist es klar, dass im Falle eines Cyberkrieges die Staaten am besten dastehen, die eine vom Netz unabhängige, antiquiert-analoge Infrastruktur und kinetische Waffen haben und daher nicht mittels Cyberbomben angegriffen werden können, aber in der Lage sind, selbst solche Angriffe auszuführen. Netzkriegskompetenz wird daher auch in den Staaten ausgebaut, die selbst noch nicht so stark vom Internet abhängig sind wie die USA, nämlich in Nordkorea, Russland oder China. »Chinesische Hacker seien ins amerikanische Stromnetz eingedrungen und hätten dort Schaltmechanismen deponiert, mit denen ein Blackout ausgelöst werden könne«, zitieren Aust und Ammann in ihrem Buch einen Geheimdienstler. Bei Bedarf könne man diese dann scharfschalten, im ganzen Land den Strom abschalten und alle ins Chaos stürzen.

Ausbau der Netzkriegskompetenz

Ein Computerwurm wie Stuxnet unterscheidet nicht zwischen Guten und Bösen, zwischen Soldaten und Zivilisten. Das größte Opfer trägt im Fall eines solchen Cyberangriffs dann doch die Zivilbevölkerung. Die US-Geheimdienste erklärten deswegen die Gefahr der Cyberangriffe zu einer schlimmeren Gefahr als den Terrorismus. Je mehr die Staaten ihre Militärtechnik digitalisieren, desto besser müssen sie diese vor den Erstangriffen schützen. Je mehr sie für den Cyberkrieg aufrüsten, desto mehr machen sie sich von den vernetzten Maschinen abhängig.

In Deutschland wurde bereits im Jahr 2007 eine Cyberkriegseinheit ins Leben gerufen. »Die Hacker in Olivgrün«, wie Aust und Amman die Gruppe »Computer Netzwerk Operationen« innerhalb des Kommandos Strategische Aufklärung in Rheinbach nahe Bonn nennen, sind u. a. für die Sicherung des Bundeswehrnetzes zuständig. Aber auch das »Auskundschaften, Manipulieren und Sabotieren von fremden Netzwerken« soll zu ihrem Repertoire gehören, des Weiteren das Wissen darüber, wie man »mit Würmern und anderen Sabotageprogrammen gegnerische Computer lahmlegt«.

Über die Kooperationen mit den deutschen Hackergruppen ist noch nichts bekannt. Obwohl diese, sollte man der Meinung von Captain Crunch Glauben schenken, in der Szene offenbar einen hervorragenden Ruf genießen. Auch Killerroboter sind bis auf Weiteres nicht in Sicht. Doch, wie Lars Klingbeil auf der #DigiKon2015 der Friedrich-Ebert-Stiftung ankündigte, sollte zu Beginn des Jahres 2016 dem Verteidigungsausschuss im Bundestag ein neuer Vorschlag des Verteidigungsministeriums zur Einrichtung eines Cyberkommandos vorgelegt werden. Es soll sich auch bei der Bundeswehr inzwischen herumgesprochen haben, dass durch die Digitalisierung und weltweite Vernetzung ganz neue Möglichkeiten der Kriegsführung entstanden sind.

Aleksandra Sowa

leitete zusammen mit dem deutschen Kryptologen Hans Dobbertin das Horst-Görtz-Institut für Sicherheit in der Informationstechnik. Sie ist Autorin zahlreicher Fachpublikationen und in einem großen Telekommunikationskonzern tätig. Kürzlich erschien bei Springer Vieweg: *IT-Revision, IT-Audit und IT-Compliance.*