Von Würmern und Firewalls

Warum technische Lösungen keine sind

Heutzutage reicht es nicht aus, viel Hardware zu besitzen, um einen Krieg zu gewinnen. Auf dem modernen Schlachtfeld sind Kommunikation sowie die Überwachung derselben lebenswichtig. Bewaffnete unbemannte Überwachungsflugzeuge werden per Fernsteuerung aus Kontrollzentren auf der anderen Seite des Globus gesteuert. Dafür braucht man Software, die wiederum für Viren, Trojaner und Würmer anfällig ist. Somit kommt eine neue Ebene in der Kriegsführung zur Geltung: Cyberwar.

Aber Cyberwar ist nicht nur auf ein reales Schlachtfeld beschränkt. Neulich berichtete die New York Times über ein Novum: Es bestehe der Verdacht, dass Israel und die USA mit Hilfe eines Schadprogramms (Malware) die Computersteuerung einer iranischen Atomanlage gestört haben. Iran bestätigte im September 2010 eine Cyberattacke mit dem „Stuxnet"-Virus auf über 30.000 Rechner in iranischen Industrieanlagen, die auch Teile des Atomprogramms beschädigte. Der Computerwurm soll speziell für eine Computersteuerung der Firma Siemens gebaut worden sein. Er wurde weltweit in Computersystemen gefunden, allerdings hauptsächlich im Iran. Die US-Firma Symantec, ein Hersteller von Anti-Viren-Software, hat den Code des Schadprogramms entschlüsselt. Dieser bewirkt, dass in der Computersteuerung eingebaute Befehle Frequenzumwandler aussenden, die die Rotationsgeschwindigkeit von Gas-Ultrazentrifugen zur Urananreicherung verändern. Der Bericht in der New York Times behauptet zudem, dass das Programm Informationen über den Normalbetrieb in der Anlage aufnahm und diese Bilder auf Kontrollbildschirme zurück spielte, so dass der Schaden zunächst unbemerkt blieb.

Der scheidende Chef des Mossad, Meir Dagan, kündigte am 7. Januar 2011 an, dass der Iran nun erst 2015 in der Lage sein könnte, Atomwaffen zu bauen. Hinter geschlossenen Türen wurde gejubelt. Man hatte das Atomprogramm der Iraner verzögert, ohne den unpopulären Einsatz von Bomben. Aber ist diese Art von Kriegsführung wirklich harmlos?

Gary Sick, ehemaliger Berater im Nationalen Sicherheitsrat der USA unter Jimmy Carter und Iran-Kenner, schreibt in seinem Blog „Gary's Choices" über die möglichen Auswirkungen dieser Attacke auf das iranische Atomprogramm. Er ist der Meinung, dass die Anwendung von „Stuxnet" mehr Schaden anrichtet, als nur in iranischen Zentrifugen. Es gibt folgende mögliche Auswirkungen:

1. Das Einschleusen des Wurms war wahrscheinlich die erste staatlich finanzierte und gezielte Cyberattacke in der Geschichte. Geheime Kriegsführung unter Anwendung von Cyberwaffen wurde damit salonfähig.

2. Darüber hinaus wurde deutlich, dass die USA und Israel sehr viel Informationen über die Urananreicherungsanlage bekommen hatten, wahrscheinlich durch die Internationale Atomenergiebehörde IAEA. Folglich wird Iran die Zusammenarbeit mit der IAEA vermutlich reduzieren, wenn nicht ganz einstellen. Ohne solche Inspektionen wird es jedoch schwer zu prüfen, was tatsächlich im Atomprogramm läuft und wie bisher festzustellen, dass Iran kein Atomwaffenprogramm durchführt.

3. Iran wird nach diesem „Erstschlag" viel defensiver werden, vor allem in den Verhandlungen über sein Atomprogramm. Warum sollte das Land jetzt kompromissbereiter sein, wenn das Gegenüber sich aggressiv verhält?

4. Das Risiko steigt, dass der Iran zurück schlägt. In den USA, Israel oder überall, wo es US-amerikanische Interessen gibt, stehen viele mögliche Ziele, seien es Staudämme, Kraftwerke, Raffinerien, Wasser-, Gas- und Stromversorgungswerke oder Atomanlagen. Zwar sind die USA in konventioneller Kriegsführung dem Iran überlegen, aber bei Cyberwar sind die Verhältnisse eher gleich.

5. Wenn man davon ausgeht, dass der Iran bisher kein Atomwaffenprogramm hat, sondern höchstens die künftige Option auf Atomwaffen durch Urananreicherung erwerben will, könnte sich diese Politik durch „Stuxnet" geändert haben. Die Hardliner, die für das Bauen von Atomwaffen argumentieren, werden gestärkt und Reformer im Land geschwächt.

Cyberwar:
Ist die neue Art der Kriegsführung wirklich harmlos?

© BuridansEsel_flickr

6. Die Cyberattacke sowie das Töten von iranischen Atomwissenschaftlern hat direkte Folgen auf die Menschenrechtslage im Lande. Die Regierung kann keinem vertrauen, es herrscht mehr Paranoia und Repression als zuvor.

Der Vorschlag, man solle das iranische Atomprogramm lieber sabotieren als bombardieren, soll laut Wikileaks und der britischen Zeitung The Guardian von Volker Perthes von der Stiftung Wissenschaft und Politik stammen. Dennoch ist die Idee der Sabotage gewiss viel älter als dieser Rat vom Nahostexperten Perthes. Bereits im Januar 2009 berichtete die New York Times von einem heimlichen Programm unter der Bush-Regierung, als Alternative zu einer Bombardierung die Computersysteme in Natans zu sabotieren. Israel hatte seinerzeit massiven Druck auf die USA ausgeübt, Militärschläge gegen die Anreicherungsanlage zu bewilligen. Die USA haben dies laut NYT entschieden abgelehnt. Präsident Obama soll von diesem Programm bei seinem Amtsantritt gewusst und seine Entwicklung beschleunigt haben.

Auch kursieren Berichte, dass der „Stuxnet"-Wurm einen Unfall im iranischen Bushehr-Reaktor auslösen könnte, der im Sommer 2011 in Betrieb gehen soll. US-Wissenschaftlerin Cheryl Rofer schreibt in ihrem Blog, dass ein von den Russen befürchtetes „iranisches Tschernobyl" wegen des Stahlsicherheitsbehälters über Bushehr zwar nicht möglich sei, aber eine Kernschmelze vom Typ „Three-Mile-Island" schon.

Immer häufiger wird versucht, Sicherheitsproblemen mit technischen Lösungen zu begegnen, statt mit Verhandlungen oder Vertrauensbildung. Beispiel Raketenabwehr: Seit Reagans SDI (Strategic Defense Initiative, auch als „Star Wars" bekannt) in den 80er Jahre sehnen sich die US-Amerikaner nach einem Garant der Unverletzbarkeit, den es gar nicht geben kann. 1986 in Reykjavik torpedierte SDI die Idee der gemeinsamen Sicherheit, die Gorbatschow von Olaf Palme, Egon Bahr und Willy Brandt übernommen hatte. Er wollte die Abschaffung aller Atomwaffen (jetzt „Global Zero" genannt) bis zum Jahr 2000 mit Reagan vereinbaren. Aber Reagan bestand auf seiner „Firewall". Ähnliches ist bei den jetzigen START-Verhandlungen mit Russland über strategische Atomwaffen geschehen. Als Obama ins Amt kam, hielten es alle für ein Kinderspiel, die Zahl der Atomwaffen auf den Ist-Stand (je 1550 stationierte Atomwaffen langer Reichweite) in einem Vertrag festzulegen. Und dennoch kam die Raketenabwehr dazwischen.

Trotz der Uneinigkeiten über Größe und Reichweite eines Raketenabwehrsystems in Europa wurde der START-Vertrag inzwischen von beiden Parlamenten ratifiziert. Das ist sehr wichtig, denn er schreibt Kontrollmechanismen fest, die für die weitere Abrüstung notwendig sind. Und es soll weitere Abrüstung geben, sagen alle. Nur die Frage der Raketenabwehr und die konventionelle Überlegenheit der USA stehen noch im Weg.

Unsere Fixierung auf technische Lösungen für unsere Sicherheitsprobleme ist hausgemacht. Es gibt keine Industrie, die von Verhandlungen und Vertrauensbildung einen Gewinn erzielt. Raketenabwehr und Cyberwaffen bringen aber mächtig viel Gewinn, ohne das ursprüngliche Problem zu lösen. Man braucht immer mehr Updates. Sie funktionieren nicht zu 100 %, d.h. die Raketenabwehr kann – wenn überhaupt – nur einen Teil der angreifenden Raketen stoppen. Und der Computerwurm erzeugt zwar einen Schaden, kann aber das Atomprogramm nicht ganz zerstören. Daher braucht man immer noch Waffen und Trägersysteme und, falls sie das Problem nicht lösen können, als „letzte Option" auch die Atomwaffen. Kurz gesagt: Cyberwar und Raketenabwehr sind nur weitere Stufen in einer Gewaltspirale. Letztendlich müssen wir unsere Sicherheit anders gewährleisten.

Xanthe Hall
ist Referentin
für Atomwaffen
und Internationale
Kampagnen
der IPPNW.