DIE SCHWEIZ WAPPNET SICH

Bis Ende Jahr soll das Budget für die Cyber-Armee des Bundes stehen – damit beginnen die Herausforderungen aber erst

VON BARNABY SKINNER (TEXT), BRUNO MUFF (ILLUSTRATION)

Braucht ein Staat offensive Fähigkeiten, um sich gegen Bedrohungen im Internet zu wehren? Die Antwort von Ehud Barak im Plenum des europäischen Cyber-Security-Gipfels vergangene Woche in Bonn kam wie aus der Pistole geschossen: «Natürlich», sagte der ehemalige Ministerpräsident und Verteidigungsminister Israels. Nur wenn eine Armee die Möglichkeit habe, sich in die Computersysteme seiner Gegner zu hacken, könne sie im Web die Landesinteressen wahren.

Das Zusammengehen der digitalen mit der realen Kriegsführung ist generell zu beobachten, nicht nur im Falle Israels. Das US-Sicherheitsunternehmen Fire Eye schreibt in einer globalen Analyse: «Jedes Land spricht die eigene Sprache, hat die eigenen politischen Gesetze, die eigene Geschichte und Kultur.» Dies und die geopolitische Lage prägten die Cyber-Angriffs- und Verteidigungsstrategie des jeweiligen Landes.

So setzt China zum Beispiel auf grossflächige Cyber-Attacken, vergleichbar damit, wie die Armeeführung während des Koreakriegs 1953 Hunderttausende Fusssoldaten mit jeweils nur ein paar Patronen in den Kampf schickte. Am anderen Ende des Spektrums sind die USA, die mit dem technisch fortschrittlichsten Spionageapparat die ganze Welt aushorchen, um gezielt Attacken zu lancieren.

Das Stromnetz und die Banken sind mögliche Angriffsziele

Worin sich alle Nationen einig sind: Eine Cyberwar- und Cyberdefense-Strategie sind unverzichtbar. Die Vorteile des Onlinekriegs sind vielfältig: Er ist billiger als ein realer Kriege und fordert, zumindest bis jetzt, kein Blutvergiessen (mit Ausnahme von Drohnenangriffen). Vor allem kann er vollkommen verdeckt durchgeführt werden. Der Ursprung einer Langstreckenrakete ist einfach zu eruieren. Wer hingegen mithilfe eines Trojaners das Nuklearkraftwerk eines fremden Landes kontrolliert, der bleibt anonym. Hätten sich die USA nicht selber zum Anschlag auf ein iranisches Kernkraftwerk im Jahr 2010 bekannt, wir hätten wohl nie erfahren, wer dahintersteckte.

Auch die Schweiz hat die Cyber-Gefahr erkannt. So warnt das bisher umfangreichste, öffentlich zugängliche Papier «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken» vor allem vor einem Angriff auf den Bankensektor. Ein anderes Horrorszenario besteht darin, dass Hacker dereinst das Stromnetz der Schweiz lahmlegen könnten.

Und ab Ende Jahr wird auch die Schweizer Armee offiziell eine Cyber-Armee haben – zumindest soll bis dahin das interne Armeebudget dafür stehen. Wie gross diese Streitkräfte sein werden und welche Kompetenzen sie haben werden, macht das Verteidigungsdepartement (VBS) nicht bekannt. So wie kein Land bisher öffentlich über die Grösse ihrer virtuellen Streitmacht spricht. Fest steht nur, dass diese moderne Kriegsführung für die Schweiz zur Herausforderung wird. Der Cyber-Krieg kennt keine Landesgrenzen oder Berge, die Schutz bieten.

Wenn Ehud Barak recht damit hat, dass im Web Angriff die beste Verteidigung ist, muss die Schweiz über kurz oder lang mit einem Prinzip brechen, das seit der Schlacht bei Marignano die Schweizer Identität geprägt hat: dem Prinzip der Neutralität.

SCHWEIZ

Die Schweiz ist im Internet nur mit Verteidigung beschäftigt. Besonders leidet sie unter Attacken, die Schweizer Websites vom Netz zwingen, indem sie millionenfach aufgerufen werden. Ob sich die defensive Haltung mit den neuen Mitteln der Cyber-Armee ändert, ist unklar (siehe Text links). Der Ausbau des Nachrichtendienstgesetzes ist aber ein Hinweis darauf, dass der Bund gewillt ist, im Cyber-Krieg eine aktivere Rolle einzunehmen.

0,6 | 5 | 8

EU

Brüssel hält sich mit Cyber-Angriffen zurück. So gibt es, mit Ausnahme der von Snowden publik gemachten Abhöraktionen der Briten, keine Cyber-Spionage oder Cyber-Angriffe, die auf einen EU-Mitgliedsstaat zurückgeführt werden können.

Den schlimmsten Angriff auf die Militärinfrastruktur erlebte Frankreich im Jahre 2009. Ein Conficker-Wurm zwang eine Militärflugzeugflotte zum Grounding. Im Jahre 2011 wurden zehn Öl- und Sicherheitsfirmen in Norwegen gehackt.

16,5 | 286 | 505

RUSSLAND

Das Land hat eine Cyber-Armee mit 10 000 Soldaten. Doch nur selten wird Russland für internationale Angriffe verantwortlich gemacht. Die Sicherheitsfirma Kaspersky vermutet, dass Russland seine Energie darauf konzentriert, die eigene Bevölkerung zu überwachen. Vielleicht aber ist die russische Cyber-Armee nur äusserst geschickt und bleibt deshalb unentdeckt.

2 | 91 | 143

NORDKOREA

Die unbekannte Grösse. Im Vergleich zum Nachbarn Südkorea, mit Download von über 100 Megabit vorn dabei, befindet sich der Norden mit seinen Dial-up-Verbindungen eigentlich in der digitalen Steinzeit. Dennoch verfügt die Diktatur bereits seit 2009 über eine schlagkräftige Cyber-Armee, die sich immer wieder in südkoreanische Websites hackt, um zum Beispiel Nutzerdaten zu stehlen.

0,04 | 10 | 24

USA

«Big Brother» im Cyber-Krieg, der jeden ausspioniert, und mit der fortschrittlichsten Technologie alle in die Knie zwingen kann. Neben dem Stuxnet-Virus (siehe unten) sollen die ebenfalls für die Infrastruktur gefährlichen Viren Duqu und Flame aus US-Labors stammen. Gleichzeitig ist das Land selber für Angriffe anfällig, nicht nur auf Websites. So hat die CIA bereits Stromausfälle in Grossstädten mit Cyber-Angriffen in Verbindung gebracht.

15,6 | 683 | 317

ISRAEL

Wie in der realen Welt besitzen die Israelis auch in der Virtualität im Vergleich zum restlichen Nahen Osten den mit Abstand fortschrittlichsten Cyber-Kriegsapparat. Dennoch zeigt sich Israel immer wieder verwundbar gegenüber Angriffen. Denn die Abwehr kann noch so gut sein, es ist eine Eigenart des Cyber-Krieges, dass ein Angreifer auch mit primitiven Mitteln eine wichtige Website oder einen Onlinedienst lahmlegen kann.

0,2 | 15 | 8

SYRIEN

Im Vergleich zum Westen besitzt Syrien im Web nur geringe Schlagkraft. Die «Syrian Electronic Army», die Cyber-Armee von Bashar al-Assad, nutzt kreative Tricks, um Schädlinge in Umlauf zu bringen, z. B. sind sie in Onlinegames versteckt.

0,07 | 2 | 21

IRAN

Seit dem Angriff auf ein Kernkraftwerk (siehe unten) experimentiert der Iran mit eigenen Cyber-Angriffen. 2012 löschte die iranische Gruppe «Cutting Sword of Justice» aus der Ferne drei Viertel aller PC-Laufwerke der Saudi-Ölfirma Aramco.

0,5 | 9 | 77

PAKISTAN

Die «Pakistani Cyber Army» hat nur Indien im Visier. Laut der Onlinepublikation Register zwangen Hacker letztes Jahr während drei Monaten 112 indische Regierungs-Websites immer wieder mit sogenannten Dental-of-Service-Attacken in die Knie. Die Inder reagierten mit «Operation Hang Over» (siehe rechts).

0,2 | 6 | 184

INDIEN

Seit Jahren ist es an der Grenze zwischen Indien und Pakistan still. Im Web bekämpfen sich die Staaten umso heftiger. Die von der Firma Symantec bekannt gemachte und bisher grösste Aktion der Inder war «Operation Hang over», welche die Webdienste diverser pakistanischer IT-, Auto- und Detailhändler zerstörte.

1,8 | 46 | 1236

CHINA

Kümmert sich nicht darum, die Angriffsspuren der 100 000-köpfigen Cyber-Armee zu verwischen. Die meisten der Attacken richten sich gegen die USA. Erst kürzlich soll China laut Presseberichten die Pläne des F35 gestohlen haben, des neusten US-Kampfjets. Anfang Jahr hackten sie sich gemäss dem US-Magazin «Christian Science Monitors» in die Systeme von 23 Gasfirmen.

8,2 | 166 | 1360

Internet-Abdeckung

Gegen 100% | 80% | 60% | 40% | 20%

Über 7,2 Milliarden Menschen leben auf der Welt. Gerade mal 2,4 Milliarden haben Zugriff aufs Internet. Vor allem in Afrika gibts vergleichsweise wenige Benutzer. Dementsprechend spielt der Kontinent wie auch Südamerika im Cyber-Krieg beinahe keine Rolle.

BIP – Das Bruttoinlandprodukt in Trilliarden US-Dollar. Der Gesamtwert aller Güter ist in der EU am grössten. Dennoch ist das Armeebudget nur die Hälfte des US-amerikanischen. Am krassesten ist der Vergleich zwischen BIP und Militärausgaben bei Nordkorea: Es ist nur viermal grösser als das Militärbudget.

Ausgaben – Militärbudget in Milliarden US-Dollar. Die USA haben das grösste Budget und deshalb wohl am meisten Geld für die Cyber-Armee. Wie viel genau, ist unbekannt. Experten schätzen, dass die Cyberarmee bis zu 30 000 gut ausgebildete Hacker unterhält. China hat 100 000 Cyber-Soldaten.

Einwohner – Anzahl Einwohner in Millionen. Wie Menschen sind auch IP-Adressen weltweit ungleich verteilt. IP-Adressen sind wie die Seriennummer jedes Gerätes, das mit dem Internet verbunden ist. In den USA kommen auf jeden Bürger 4,9 IPs, in der Schweiz sind es 2,7. In Nordkorea nur noch 0,0004.

Botnetze sind PCs von ahnungslosen Privatnutzern, die für Cyber-Angriffe ferngesteuert werden. Am meisten hat es laut Sicherheitsfirma Trend-Micro in 1. Australien (32%) 2. Südkorea (15) 3. Deutschland (9) 4. Japan (7) 5. Italien (6) 6. Taiwan (5) 7. Indien (4) 8. USA (3) 9. Vietnam (2) und 10. Holland (2).

WORLD WAR C – TIMELINE DER WICHTIGSTEN CYBER-WAR-EREIGNISSE DER LETZTEN JAHRE

2003 Der irakische Diktator Saddam Hussein setzt während der Invasion durch die US-Amerikaner erstmals im grossen Stil das Internet als Waffe ein, um Militär-Server lahmzulegen.

2006 Israel heuert Hacker an, die zur Informationsbeschaffung in Hizbollah-Server eindringen. Viele Länder beginnen im selben Jahr mit der Entwicklung einer Cyber-Verteidigungsstrategie.

2007 Russische Hacker greifen Estland an und legen Websites von Banken, Ministerien etc. lahm. Israel fliegt gegen Syrien Angriffe und zerstört das Radarsystem mit einer Hackerattacke.

2008 Im südossetischen Krieg zwischen Russland und Georgien zwingen beide Parteien die Regierungs-Sites der Gegner in die Knie. Es wurde keine kritische Infrastruktur beschädigt.

2009 Die Regierungen der USA und von Südkorea sehen sich immer wieder Angriffen aus China ausgesetzt, bei der Websites millionenfach aufgerufen und damit in die Knie gezwungen werden.

2010 Die USA greifen mit dem Stuxnet-Wurm im Iran 1000 der 5000 zur Urananreicherung eingesetzten Zentrifugen an. Erstmals ist kritische Infrastruktur von Cyber-Angriffen betroffen.

Anfang 2011 Die Sicherheitsfirma McAfee macht Angriffe publik, die seit 2006 Sportverbänden gelten, allen voran dem Olympischen Komitee, und Computer fernsteuern. Herkunft der Angriffe: China.

Ende 2011 Die US-Armee stellt fest, dass grosse Teile der Drohnenflotte keylogged sind. Das heisst, jemand wusste schon bei Eingabe eines Befehls, was das Ziel einer Drohne ist.

2012 Mike McConnell, der frühere Direktor des US-Geheimdienstes National Security Agency (NSA) gibt erstmals zu, dass die USA Cyber-Angriffe auf andere Staaten lanciert hat.

2013 Edward Snowden macht publik, dass die NSA systematisch Millionen Menschen ausspioniert, unter anderem, um Infos zu Webbedrohungen zu sammeln, um selber Cyber-Angriffe zu lancieren.