

eine Einzelkämpferin, die keinen Teamgeist in der CDU herstelle.

Merkel weiß, dass viele Christdemokraten so denken wie Schlarmann, das ist für sie die eigentliche Gefahr. So ein einzelner Schlarmann ist kein Problem, aber wenn die Methode Schlarmann Schule macht, dann frisst das am Fundament ihrer Macht. Eine Partei, die ohne Tabus diskutiert, erlaubt sich schnell mal die Frage, ob sie noch die richtige Vorsitzende hat.

Ein paar Tage nach seiner Rede im Weinkeller sitzt Schlarmann in seiner Hamburger Kanzlei und redet über seine Sicht auf die Merkel-CDU. Er habe den Glauben daran verloren, dass es in einem Parteiensystem demokratisch zugehe, sagt er. Es ist später Nachmittag, von seinem Büro hat man einen herrlichen Blick auf die Binnenalster. Von hier aus gesehen erscheint ihm die Berliner Politik noch immer wie ein Paralleluniversum.

Schlarmann ist seit gut drei Jahren in der großen Politik, aber er hat schnell gelernt, welch merkwürdige Geschöpfe sie gebiert. Als er vor kurzem von Merkel im CDU-Vorstand abgebürstet wurde, klopfen die anderen Mitglieder der Parteispitze so heftig auf den Tisch, dass die Kaffeetaschen klapperten. Jeder wollte im Angesicht der Chefin größtmögliche Abscheu über Schlarmanns Worte demonstrieren.

Dann aber kommen wieder die klandestinen Anrufe von Merkels Rivalen, die Schlarmann ermutigen, bei seiner Linie zu bleiben. Sie teilen nicht immer seine Meinung, aber finden es ganz gut, wenn er die Kanzlerin ärgert. Mit dem nordrhein-westfälischen Regierungschef Jürgen Rüttgers darf er sich inzwischen duzen.

Das wiederum schmeichelt Schlarmann. Er genießt die Wonnen seiner medialen Alterskarriere als Deutschlands führender Kanzlerkritiker, ganz uneigennützig ist natürlich auch er nicht. Der Beruf als Anwalt und Wirtschaftsprüfer hat ihn wohlhabend gemacht, aber nicht bekannt. Jetzt gibt es sogar Homestorys über ihn.

Es ist dunkel geworden über der Binnenalster und Schlarmann beim Grundsätzlichen angelangt, der Frage, ob er mit seiner Radikalopposition etwas ausrichten kann. „Wenn Frau Merkel eine Wutrede auf mich hält, dann ist das positiv für mich“, sagt er. Aber stimmt das? Merkels Große Koalition hat den Gesundheitsfonds beschlossen, Mindestlöhne für acht Branchen, auch das Konjunkturpaket wird wohl ohne größere Korrekturen durchlaufen. Aller Schlarmannscher Furor nutzt da nichts.

Doch wahrscheinlich kommt es darauf gar nicht an. Man kann Schlarmanns Kritik an Merkel für überzogen halten. Aber was mit einem wie ihm erhalten bleibt, ist der Glaube, dass Politik aus mehr besteht als den Erfordernissen des Moments. Das ist ab und zu eine Kanzlerexplosion wert.

RENÉ PFISTER

VERTEIDIGUNG

Krieg der Zukunft

Weltweit rüsten Staaten auf, um sich für Cyber-Konflikte vorzubereiten. Auch die Bundeswehr trainiert Hacker in Uniform.



Nato-Cyber-Verteidigungszentrum im belgischen Mons: „Angriffe in einer Grauzone“

So also sieht ein amtlich bestellter Hacker aus: ein Herr mit grauen Haaren, Schnauzbart, Besoldungsgruppe B 6 und blauer Luftwaffenuniform. Friedrich Wilhelm Kriesel heißt der Mann, er ist 60, Brigadegeneral und Leiter des Kommandos Strategische Aufklärung.

Kriesel ist an einem Frontabschnitt eingesetzt, der erst in jüngster Zeit ins Visier der Bundeswehr geraten ist. Der General soll den Krieg der Zukunft vorbereiten, und der könnte in Teilen im weltweiten Netz stattfinden. Kriesel scheint der richtige Mann für diese Aufgabe zu sein. Knapp 6000 Soldaten unterstehen seinem Kommando, sein Verband funktioniert schon jetzt wie ein Geheimdienst.

Streng abgeschottet von der Öffentlichkeit tüfteln mittlerweile 76 seiner Leute in der Tomburg-Kaserne im beschaulichen Fachwerkstädtchen Rheinbach bei Bonn an den neuesten Methoden, um in fremde Netzwerke einzudringen, sie auszukundschaften, zu manipulieren – oder zu zerstören. Was im internen Behördengebrauch unter der harmlosen Bezeichnung „Abteilung Informations- und Computernetzwerkoperationen“ firmiert, ist eine Einheit, die sich für den elektronischen Ernstfall vorbereitet, digi-

tale Angriffe auf fremde Server und Netze inklusive.

Die uniformierten Hacker aus Rheinbach sind Deutschlands Antwort auf eine Bedrohung, die mittlerweile Regierungen, Geheimdienste und Militärs in aller Welt alarmiert. Seit Computer praktisch alle Lebensbereiche durchdringen, ist die Anfälligkeit für Angriffe aus dem Netz massiv gestiegen. In den USA warnen Experten schon seit Jahren vor einem „elektronischen Pearl Harbor“, einem „digitalen 11. September“ oder einem „Cybergeddon“.

Estland war der erste Nato-Staat, der Opfer einer solchen Digital-Attacke wurde. Im Frühjahr 2007 gerieten Banken, Behörden und Parteien für drei Wochen unter massives elektronisches Sperrfeuer. Die Baltenrepublik war zeitweise so gut wie offline und galt damit als Austragungsort des ersten „Cyber-Kriegs“, denn sie vermutete den Nachbarn Russland hinter dem Angriff, mit dem es damals gerade gravierende diplomatische Querelen gab.

Der Begriff „Krieg“ war dabei zu Recht von Anfang an umstritten – immerhin gab es keine Toten oder Verletzten. Doch dass Angriffe aus der virtuellen auch in der realen Welt desaströse Folgen haben können, ist spätestens seit der Estland-Attacke klar.

Das Internet hat sich zu einem virtuellen Schlachtfeld entwickelt, auf dem sich die Konflikte der realen Welt widerspiegeln.

In aller Stille rüsten viele Staaten deshalb massiv auf. Allein die Amerikaner wollen Milliarden US-Dollar in ein nationales Cyber-Programm investieren. Westliche Geheimdienste und Militärs sind sich sicher, dass die Feinde wie einst im Kalten Krieg vor allem im Osten stehen: in Russland und in China. Ein Bericht für den US-Kongress kam im Herbst zu dem Schluss, China baue seine Cyber-Kriegs-Kapazitäten „aggressiv“ aus und könnte bald schon „asymmetrische Vorteile“ besitzen: „In einer Konfliktsituation würde dieser Vorteil die konventionelle Überlegenheit der USA reduzieren.“

Auch die Deutschen haben in diesem Punkt schlechte Erfahrungen mit China gemacht. Vor knapp zwei Jahren informierte der Verfassungsschutz die Bundesregierung, dass Server aus der chinesischen Provinz Lanzhou mehrere Bundesministerien und das Bundeskanzleramt mit Schadprogrammen angriffen. Sie waren darauf ausgelegt, sensible Informationen abzugreifen (SPIEGEL 35/2007).

Mitte Januar verabschiedete das Bundeskabinett von der Öffentlichkeit weitgehend unbemerkt einen Gesetzesentwurf zur „Stärkung der Informationssicherheit des Bundes“, der von Wolfgang Schäubles Innenministerium vorgelegt wurde. Nun liegt der Entwurf beim Bundesrat und soll schon Anfang März in den Bundestag kommen. Die „besondere Eilbedürftigkeit“, heißt es, ergebe sich aus der „notwendigen Absicherung der Regierungskommunikation“. Das zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn soll dafür zu einer Art Datenwachturm für Behörden ausgebaut werden, mit mehr Geld, Personal und Befugnissen.

Bereits vor drei Jahren befahl Verteidigungsminister Franz Josef Jung den Aufbau einer Cyber-Truppe innerhalb der Bundeswehr. Es war die Geburtsstunde der Kriesel-Einheit.

Die 76 deutschen Netzkrieger kommen vor allem aus den Fachbereichen für Informatik an den Bundeswehruniversitäten. Stolz berichtete General Kriesel am vergangenen Dienstag dem Generalinspekteur Wolfgang Schneiderhan und den Chefs von Heer, Luftwaffe und Marine von den Erfolgen seines Kommandos, etwa bei den elektronischen Abhörmaßnahmen in

Mögliche Angriffsziele im Internet



Kernkraftwerk (Gundremmingen)



Bundeskanzleramt



Flughafen (Frankfurt am Main)

dann unauffällig an den Auftraggeber.

Noch diffiziler und exotischer ist das, was in der Abteilung Attacke auf dem Ausbildungsprogramm steht. Die Rheinbacher Soldaten müssen sich nicht mehr mit Panzern, Eurofightern oder Sturmgewehren auseinandersetzen. Ihre Waffe ist der Rechner, ihre Szenarien klingen nach Science-Fiction oder wie Importe aus der Welt der Computerspiele: Sie heißen „Denial of Service“-Angriffe oder „Botnet“-Attacken.

Beides studieren Kriesels Soldaten auch an realen Angriffswellen wie jenen auf Estland und Georgien.

In Estland war es der politische Konflikt um die Versetzung eines sowjetischen Ehrenmals, der im Frühjahr 2007 innerhalb von wenigen Stunden ins Internet überschwappte. Über Nacht hatten die Esten die Bronzestatue demontiert, um sie aus der Innenstadt von Tallinn auf einen Soldatenfriedhof zu versetzen. Was viele Esten als Symbol der Besetzung ansahen, war für die russische Minderheit das Zeichen des Triumphs über Hitler-Deutschland.

Keine 24 Stunden danach begann die erste Welle von Internet-Attacken auf die Web-Seiten des estnischen Ministerpräsidenten, des Parlaments und diverser Parteien. Hacker plazierten eine falsche Entschuldigung für die Entscheidung, die Statue umzusetzen, und verpassten dem Ministerpräsidenten auf seiner Web-Seite ein Hitler-Bärtchen.

Parallel tauchten in diversen russischen Internet-Foren Gebrauchsanweisungen auf, wie jeder einzelne Internet-Nutzer seinen Unmut über die Entscheidung ausdrücken könne.

Detailiert wurde in russischer Sprache beschrieben, wie estnische Web-Seiten und Server mit Testsignalen überflutet werden könnten. Es war die Anleitung für eine klassische Verfügbarkeits-Attacke („Denial of Service“).

Die Instruktionen wirkten schnell, der Datenverkehr auf den estnischen Netzen schwoll enorm an; zudem registrierten die Experten des estnischen „Computer Emergency Response Teams“ die orchestrierten Angriffe von über einer Million Rechner auf einzelne Ziele. Dahinter steckten „Botnets“, also gleichgeschaltete Computer, die mit einer Schad-Software infiziert sind und so ohne Wissen ihrer Eigentümer zu kriminellen Zwecken missbraucht werden können, sobald sie online sind.

Die Folgen waren spektakulär. Das estnische Parlament musste sein E-Mail-System für einen halben Tag herunterfahren,

Afghanistan, dann kam er zu seiner geheimsten Truppe. Schon im kommenden Jahr solle seine Cyber-Einheit einsatzfähig sein und das auch nachweisen – etwa durch einen simulierten Angriff auf ein reales Ziel, einen sogenannten Penetrationstest.

Die Soldaten bedienen sich dabei der gleichen Methoden, die auch Computerkriminelle anwenden. So lernen die zukünftigen Digital-Krieger etwa den Umgang mit Schadprogrammen, die ohne Wissen der Nutzer auf fremde Rechner aufgespielt werden können, sei es in einer E-Mail, über externe Medien wie eine CD-Rom oder auch nur „im Vorbeisurfen“ über eine präparierte Internet-Seite. Infizierte Rechner können dann weitere Schadprogramme nachladen, etwa eine Art Buchstaben-Recorder, der jede Tastatureingabe mitschneidet: E-Mails, Internet-Adressen, Passwörter. Die gesammelten Eingaben schickt das Programm

ALFRED BUELESBACH / VISUM (O.); JOERG HEIMANN / BILDERBERG (M.); BORIS ROESSLER / PICTURE-ALLIANCE / DPA (U.)

Internet-Provider kappten kurzzeitig sämtliche Netzverbindungen ihrer Kunden, mehrere estnische Banken waren für längere Zeit im Netz nicht erreichbar.

Ein estnischer Netzanbieter zählte danach insgesamt 128 Attacken, darunter 36 auf die Web-Seiten von Regierung und Parlament, 35 auf die estnische Polizei und weitere 35 auf das Finanzministerium.

Estland gilt bei Militärs und Geheimdiensten in aller Welt als Präzedenzfall mit beunruhigender Botschaft. So heißt es in einer schwedischen Studie, das estnische Beispiel beweise endgültig, „dass ein einzelner Angreifer oder eine Gruppe ohne größere Probleme das normale Geschäft von Behörden und das Wirtschaftsleben in einem anderen Land erheblich stören – und ihre Beteiligung erfolgreich verheimlichen“ können. Tatsächlich stehen die Verantwortlichkeiten bis heute nicht fest. Sicher ist nur, dass einige der beteiligten Bot-Netze auch schon den Netzauftritt einer russischen Oppositionspartei angriffen.

Ähnlich verliefen im vergangenen Sommer die Attacken auf Georgien, die in diesem Fall allerdings den Einmarsch russischer Truppen und damit einen realen Krieg flankierten. Wieder waren es zu-



General Kriesel, Minister Jung: Digitale Guerilla

deswehr beispielsweise einen einmal identifizierten Kontrollserver eines Bot-Netztes unschädlich machen, braucht sie am Ende selbst ein Computer-Heer?

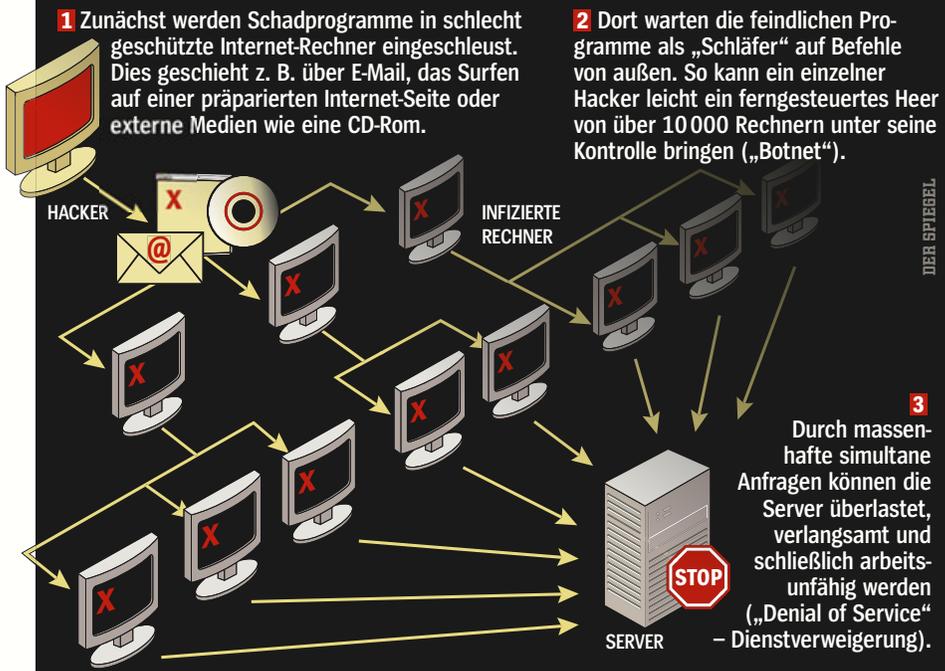
Seit dem estnischen Fall gibt es über diese Fragen heftige Debatten zwischen Militärs und Diplomaten. Auf dem Natogipfel im vergangenen Jahr in Bukarest beschlossen die Staatschefs ein

gemeinsames Konzept für die Cyber-Verteidigung und verstärkten die Sicherheitsvorkehrungen für die eigenen Netze, für die eine Nato-Agentur im belgischen Mons zuständig ist. Zusätzlich richtete das Bündnis in Tallinn ein „Exzellenzcenter für Cyber-Verteidigung“ ein. Das neue Institut legte bereits eine Analyse der Attacken auf Georgien vor, in der es von „Angriffen in einer Grauzone“ spricht: „Die aktuelle Frage, ob Cyber-Attacken wie bewaffnete Angriffe gewertet werden sollten, bleibt ungelöst.“ Es werde „Zeit brauchen, um über die rechtlichen Fragen der Cyber-Verteidigung auf der internationalen Bühne Übereinstimmung zu erzielen“.

Zumindest was die Verteidigung der eigenen Behörden-Netze angeht, will die Bundesregierung so lange offenbar nicht warten. Der Gesetzesentwurf aus dem Innenministerium, über den der Bundestag nun beraten soll, sieht vor, das BSI zu einer Art ziviler Cyber-Verteidigungs-Agentur aufzuwerten. Es soll künftig automatisiert die Datenströme etwa des Bundeskanzleramts und der Ministerien überwachen, um Auffälligkeiten schneller erkennen und bekämpfen zu können. Zudem soll die kleine Bonner Behörde widerstrebenden Bundeseinrichtungen nicht nur wie bisher Empfehlungen aussprechen, sondern konkrete „Vorgaben“ machen können, etwa die Zahl der offenen Zugänge ins Internet zu reduzieren.

In ihrem bislang unveröffentlichten Bericht zur Lage der IT-Sicherheit in Deutschland 2009 warnen die Sicherheitsexperten, dass nicht nur die Zahl der Angriffe, sondern auch ihre Professionalität stark steigt. Sie prognostizieren nicht nur eine wachsende Gefährdung durch Botnet-Attacken, aber auch durch Angriffe auf große Steuersysteme kritischer Infrastrukturen, etwa von Kernkraftwerken oder Verkehrsleitsystemen.

Virtuelles Schlachtfeld Wie Hacker ganze Datendienste lahmlegen



nächst russischsprachige Internet-Foren, die zur Attacke bliesen und gleich eine Liste von lohnenden georgischen Zielen mitlieferten. Auf der eigens eingerichteten Seite „stopgeorgia.ru“ konnten Nutzer gar ein Schadprogramm namens „war.bat“ herunterladen, das für den Angriff auf die georgischen Netze zugeschnitten war.

Als Folge der Attacken musste die Web-Seite des georgischen Präsidenten für einen Tag vom Netz genommen werden, auf

ges zwischen zwei Nationen ins Internet? Oder handelt es sich um weitere neue Formen „asymmetrischer Auseinandersetzungen“, bei denen Staaten von digitalen Guerilla-Gruppen angegriffen werden?

Sind solche als Verstoß gegen das „Übereinkommen über Computerkriminalität“ des Europarates zu werten, das bislang 23 Staaten ratifiziert haben? Oder als militärischer Angriff, der Vergeltungsschläge oder Gegenangriffe rechtfertigt? Dürfte die Bun-

Die Rheinbacher Netzsoldaten der Bundeswehr haben derweil mit einem besonders tückischen Gegner zu kämpfen: dem deutschen Strafrecht, das eigentlich seit 2007 schon die Vorbereitung von Computersabotage verbietet. Sollten die deutschen Cyber-Krieger tatsächlich Versuchsangriffe auf fremde Netze starten, stünden sie strenggenommen mit einem Bein im Gefängnis. Auf schwere Computersabotage stehen bis zu zehn Jahren Haft.

JOHN GOETZ, MARCEL ROSENBACH, ALEXANDER SZANDAR