AUSGABE 89
März 2011

ANALYSEN & ARGUMENTE

Cyber-Sicherheit

Die Sicherheitsstrategie der Bundesregierung

Klaus-Dieter Fritsche (ext.)

Am 23. Februar 2011 hat die Bundesregierung die von dem damaligen Bundesinnenminister Dr. Thomas de Maizière vorgelegte „Cyber-Sicherheitsstrategie für Deutschland" beschlossen. Hier erklärt Staatssekretär Klaus-Dieter Fritsche die Hintergründe dieser Strategie: Welche Gefahrenpotentiale birgt der Cyberspace und warum nimmt die Bedeutung der Cyber-Sicherheit für Deutschland immer stärker zu? Welche Maßnahmen hat die Bundesregierung ergriffen und wie sehen die nächsten Schritte in der internationalen Zusammenarbeit aus? Und wie lässt sich im Umgang mit den Cyber-Risiken das Verhältnis zwischen zivilen und militärischen Instrumenten sinnvoll gestalten?

Ansprechpartner

Dr. Patrick Keller
Koordinator Außen- und Sicherheitspolitik
Hauptabteilung Europäische und Internationale Zusammenarbeit
Telefon: +49(0)30 2 69 96-35 10
E-Mail: patrick.keller@kas.de

Postanschrift
Konrad-Adenauer-Stiftung, 10907 Berlin

www.kas.de

publikationen@kas.de

ISBN 978-3-942775-14-4

Konrad Adenauer Stiftung

INHALT

NEUE UND KOMPLEXERE BEDROHUNGEN IN DER GLOBALISIERTEN WELT

In einer globalen Studie erklären 73% aller befragten Unternehmen, dass sie im Jahr 2009 Opfer von Internetangriffen wurden. Ein Drittel dieser Angriffe war erfolgreich. Mit Estland und Georgien gibt es mittlerweile zwei Staaten, die sich als Opfer von Cyber-Attacken im Rahmen eines „Cyber War" sehen. Es gibt Indizien, dass der Industrieanlagen sabotierende Computerwurm „Stuxnet" von einem staatlichen Akteur entwickelt worden ist und gezielt auf Atomanlagen im Iran angesetzt wurde. Die US-Regierung richtete jüngst ein „Cyberspace-Kommando" gegen Computerangriffe auf die eigenen sicherheitsrelevanten Computernetzwerke ein. Dieses soll auch selbsttätig im Cyberspace operieren.

Vor diesem Hintergrund haben in jüngster Zeit eine Reihe nationaler Sicherheitsstrategien (USA, Indien, Großbritannien, Australien) und auch die neue NATO-Strategie von 2010 mögliche Angriffe auf die Informationssicherheit ihrer Länder als eine der Hauptbedrohungen der kommenden Jahrzehnte definiert. Waren noch vor wenigen Jahren so gut wie alle Cyber-Attacken nachweisbar kriminellen Ursprungs, häuften sich zuletzt Angriffe, die als Spionage oder Sabotageversuch mit politisch-strategischem Hintergrund deutbar sind.

Sicherheitspolitisch wird hier Neuland betreten. Wie bei anderen modernen Bedrohungsformen (Terrorismus, Piraterie, asymmetrische Kriege und *failing states*) verliert das Territorialprinzip und damit die Grenzverteidigung ihre Relevanz. Innere und äußere Sicherheit verschmelzen. Der Angreifer kann nicht mehr identifiziert werden – Kriminalität, Terrorismus, asymmetrische bzw. verdeckte Kriegführung und Spionage fließen ineinander.

Die Bedrohung erfordert eine starke Beteiligung der Bürger im Sinne des Selbstschutzes und der Subsidiarität, eine enge Sicherheitspartnerschaft zwischen Staat und Wirtschaft, eine ressortübergreifende Kooperation im Sinne der „vernetzten Sicherheit" und v.a. eine intensive internationale Kooperation. Sicherheitspolitik im Feld der Schlüsseltechnologie der sich herausbildenden globalen „digitalen Gesellschaft" muss zudem kompatibel sein zu Wirtschaftsinteressen und strengen Datenschutzforderungen im sensiblen Feld des Informationsaustauschs.

CYBER SECURITY – KONKRETE BEISPIELE DER BEDROHUNG

Der Cyberspace, also der mit dem Internet verbundene Raum aller Informations- und Kommunikationstechniken, ist für moderne Informationsgesellschaften auch durch die Abhängigkeiten weiterer kritischer Infrastrukturen (u.a. Stromversorger, Banken, Versicherungen, Transport) zu einer kritischen Schlüsselinfrastruktur geworden.

Die Angriffe auf die Informationssysteme aus dem In- und Ausland sind in den letzten Jahren immer zahlreicher und komplexer geworden. 2009 hat die CIA ca. 500.000 gegen sie gerichtete Angriffe registriert – aus China, Russland, dem Iran oder durch private „Hacker". Dass die Angriffe auch aus den eigenen Reihen kommen können, zeigt der kürzliche illegale Abfluss vertraulicher Regierungskommunikation (Botschaftsberichte) in den USA (Wikileaks-Affäre). Täglich werden weltweit fünfzehn Lücken in Softwareprodukten entdeckt, auf deren Basis jede zweite Sekunde ein neues Schadprogramm entwickelt wird. Diese werden über manipulierte Webseiten im Internet verbreitet. Derzeit werden täglich 40.000 Webseiten im Internet mit Schadprogrammen infiziert. Durch die zunehmende Komplexität moderner Informationstechnik sowie den Aufwuchs krimineller, terroristischer und nachrichtendienstlicher bzw. militärischer Angriffsfähigkeiten ist mit einer weiteren Verschärfung der IT-Sicherheitslage zu rechnen.

Beispiele der Bedrohung:

- Cyber-Spionage: Seit 2005 werden zielgerichtete Angriffe auf Bundesbehörden und Industrie mittels Spionage-Trojaner beobachtet. In E-Mails enthaltene Schadsoftware wird auch zur Wirtschafts- und Industriespionage genutzt. Nur einer von 10.000 Fällen der Cyber-Spionage wird erkannt.

- Bot-Netze erlauben eine Fernsteuerung von Millionen von PCs. Deutschland ist hinsichtlich infizierter Rechner unter den TOP 5 weltweit und in Europa auf Platz 1. Von ihnen gehen Angriffe auf die Verfügbarkeit von Netzwerken und Dienstleistungen durch *Distributed Denial of Service*-Angriffe aus.

- Cyber-Sabotage: 2007 wurden Server der estnischen Regierung, von Banken, Zeitungen und vereinzelten Unternehmen Ziel konzertierter *Denial of Service*-Angriffe. Estland war massiv gelähmt und technisch wie organisatorisch nicht in der Lage, die Angriffe abzuwehren. Ähnliche Angriffe erfolgten auf Malta (2004) und Georgien (2008).

- Stuxnet: Das im Juli 2010 bekannt gewordene Schadprogramm Stuxnet richtete sich gegen Software-basierte Steuerung industrieller Produktionsprozesse. Ein nachrichtendienstlicher Hintergrund mit dem Ziel der Spionage oder Sabotage ist wahrscheinlich – die Offensivfähigkeiten im militärischen bzw. nachrichtendienstlichen Bereich wachsen.

- Cyber-Angriffe auf kritische Infrastruktur: Besondere Sorge macht die zunehmende Verletzbarkeit durch Angriffe über das Internet auf kritische Infrastrukturen. Ein längerer Ausfall hätte in Zeiten moderner Produktionsmethoden erhebliches ökonomisches Schadenspotential. Kriminelle und Terroristen könnten dieses z.B. zu Erpressungsversuchen nutzen.

- Cyber-War: Im Fall kriegerischer Auseinandersetzungen spielt die elektronische Kampfführung über den virtuellen Raum mit Mitteln der Informationstechnik heute eine Schlüsselrolle. Die hochtechnisierten Formen des Krieges im Informationszeitalter basieren auf einer weitgehenden Computerisierung, Digitalisierung und Vernetzung fast aller militärischen Fähigkeiten. Eine Begrenzung der Kriegsführung auf das Gefechtsfeld kriegführender Nationen ist unter Globalisierungsbedingungen eher unwahrscheinlich.

- Cyber-Kriminalität: Der Schaden aus Betrugsstraftaten im Zusammenhang mit Online-Banking, Identitätsdiebstahl und Kreditkarten steigt. Die Schadenssumme bei letzterem erreichte 2010 in Deutschland in etwa die Höhe der aus dem Kreditkartengeschäft erwirtschafteten Gewinne (dreistelliger Millionenbereich).

MASSNAHMEN IM FELD DER CYBER SECURITY

Die Bundesregierung hat 2005 den „Nationalen Plan zum Schutz der IT-Infrastrukturen" als Dachstrategie für die IT- und Internetsicherheit beschlossen. Im September 2007 wurde der daraus abgeleitete Umsetzungsplan für die Bundesverwaltung verabschiedet, der Mindeststandards und ein IT-Sicherheitsmanagement für Bundesbehörden festlegt. Ebenfalls im September 2007 hat das BMI mit der Wirtschaft eine Konkretisierung des „Nationalen Plans für die kritischen Infrastrukturen" vereinbart, den „Umsetzungsplan für Kritische Infrastrukturen".

Im Rahmen des 2008 aufgesetzten Projektes „Netze des Bundes" wird derzeit ein neues Regierungsnetz aufgebaut. Hierfür werden ca. 360 Millionen Euro für Investitionen und laufende Betriebskosten aufgewendet. Dieses Netz soll künftig auch die Grundlage für die Kommunikation zwischen Bund und Ländern bilden. Wesentliche Anforderung für dieses Nachfolgenetz des derzeitigen Regierungskommunikationsnetzes IVBB ist eine erhöhte Sicherheit und Krisenfestigkeit.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erhielt durch die im Sommer 2009 erfolgte Novellierung des BSI-Gesetzes neue Befugnisse zum Schutz der Cyber-Sicherheit.

Schwerpunkt des IT-Investitionsprogramms (220 Millionen Euro) ist die IT-Sicherheit.

Zentraler Träger von internetbasierten Angriffen sind sogenannte Bot-Netze. Mit der vom Branchenverband eco und dem BSI im Sommer 2010 initiierten Anti-Bot-Netz-Initiative erhalten betroffene Internetnutzer Hilfestellungen, um Schadsoftware von ihren PCs zu entfernen und damit die Bot-Verbreitung zu verringern.

Die 2010 durch die Innenministerkonferenz gebilligte Strategie zur Bekämpfung der Cyber-Kriminalität enthält Handlungsempfehlungen zur Erreichung der strategischen Zielsetzungen (Optimierung des Informationsaustauschs zwischen öffentlichen Dienststellen und privaten Akteuren, wirksame Kriminalitätskontrolle im Bereich Cybercrime, Stärkung des Verantwortungsbewusstseins bei Anbietern und Entwicklern sowie Stärkung der Kompetenz von privaten und professionellen Anwendern).

Übungen wie die Lükex 2011 und die Teilnahme Deutschlands an der US-Übung Cyberstorm 2010 oder der Eurocybex 2010 stellen die Cyber Security ins Zentrum der nationalen Sicherheitsüberlegungen.

Der Koalitionsvertrag von CDU/CSU und FDP enthält konkrete Vorgaben für die Stärkung der Cyber-Sicherheit. Hierzu gehören die Stärkung des BSI und dessen Ausbau zur zentralen Cyber-Sicherheitsbehörde sowie die Bündelung von Kompetenzen innerhalb der Bundesregierung bei der Beauftragten der Bundesregierung für Informationstechnik (BfIT).

Im Februar 2011 hat die Bundesregierung zudem eine Cyber-Sicherheitsstrategie verabschiedet. Wesentliche Kernpunkte der Strategie sind u.a.:

- Schutz kritischer Infrastrukturen
- Sichere Computer und Internetzugänge für Bürgerinnen und Bürger sowie für kleine und mittlere Unternehmen
- Stärkung der IT-Sicherheit in der öffentlichen Verwaltung
- Aufbau eines Nationalen Cyber-Abwehrzentrums (NCAZ)

INTERNATIONALE KOOPERATION IM BEREICH DER CYBER SECURITY

Die Pflege von Partnerschaften mit anderen Staaten und Organisationen ist künftig unverzichtbarer Teil einer vorausschauenden Cyber-Sicherheitsstrategie. Die NATO könnte bei einem „vernetzten" Ansatz von militärischen und zivilen Anstrengungen auch als ein Organisator von gemeinsamen Anstrengungen im Feld der Cyber Security fungieren. Dies würde die wichtige transatlantische Klammer zum wohl stärksten Partner hinsichtlich der Ressourcen machen.

In der NATO hatte man sich 2008 – noch unter dem Eindruck des Cyber-Angriffs auf Estland 2007 – verpflichtet, das Thema Cyber Security stärker in den Mittelpunkt der Aufmerksamkeit zu stellen. Seither wurde das *Center of Excellence* in Tallinn eingerichtet, das sich der Verbesserung der Abwehrfähigkeiten verschrieben hat. Eine Zelle für systematische Planung prüft die Frage, wie mit dem Thema innerhalb der NATO umgegangen werden soll.

Die US-Administration hat, nicht zuletzt durch Präsident Obama selbst, das Thema Cyber Security zu einer Priorität ihrer Verteidigungs- und Heimatschutzpolitik gemacht. Cyber Security ist einer der Schwerpunkte in der neuen Nationalen Sicherheitsstrategie der USA. Insbesondere im militärischen Bereich arbeitet man seit der Einrichtung des Cyber Command im Mai 2010 intensiv an Strategien zur Sicherung vor Cyberbedrohungen. Die Gesamtkoordination obliegt dem Cyber Czar Howard Schmidt im Weißen Haus.

Forciert wird die internationale Kooperation von den USA derzeit auf allen denkbaren Ebenen: Bilateral, regional, in Gruppen Gleichgesinnter, in internationalen Organisationen und in Regierungskonsultationen. Aus Sicht einiger US-Think Tanks greifen traditionelle rüstungskontrollpolitische Instrumente nicht. Auch einer Verrechtlichung durch Verträge, die darauf zielt, den Handlungsspielraum von Regierungen einzuschränken, stehen manche Beobachter in Washington zum jetzigen Zeitpunkt skeptisch gegenüber.

Die USA setzen vor Schaffung rechtlicher und institutioneller Instrumentarien auf internationalen Dialog über Verhaltensnormen und vertrauensbildende Maßnahmen, die wie im humanitären Völkerrecht später kodifiziert werden könnten. Internationale Vertragskonstrukte – z.B. ein „Cyber War Limitation Treaty" nach Vorbild der Rüstungskontrolle im Nuklearwaffenbereich („no first use" etc.) – gelten als zu starr, zu wenig verifizierbar und zu sehr auf staatliches Handeln fokussiert, um gegen asymmetrische Cyber-Bedrohungen effektiv wirken zu können. Lediglich im Bereich der Strafverfolgung sieht man gemeinsame Normen als sinnvoll an. Daher zeigen sich die USA entschlossen, den in den VN angestoßenen Dialog über Verhaltensnormen und vertrauensbildende Maßnahmen weiter voranzutreiben.

Ein geeignetes Instrument wäre bei den Vereinten Nationen die *Group of Government Experts*. Auch die International Telecommunication Union (ITU) versucht sich als Forum für internationale Zusammenarbeit im Bereich Cyber Security zu etablieren – v.a. im Bereich der technischen Standardisierung. Private Akteure gilt es in den inter-staatlichen Dialog mit aufzunehmen. Angestrebt wird eine gemeinsame Sicherheitskultur durch vertrauensbildende Maßnahmen (strategischer Dialog auch mit Russland, China und Indien). Frühwarnsysteme in Form automatischer Sensorennetzwerke und Hotlines zwischen Staaten sollen ausgebaut werden. Deutschland wird sich mit einer abgestimmten Cyber-Außenpolitik aktiv in diesen Diskussionsprozess einbringen.

Deutlich wird in der NATO, dass v.a. Russland näher an das Bündnis herangeführt und ihm dabei auf Augenhöhe begegnet werden soll. Russlands Präsident Medwedjew war auf Einladung Kanzlerin Merkels und des französischen Präsidenten Sarkozy persönlich beim NATO-Russland-Rat in Lissabon erschienen. Aus den USA hören wir jedenfalls die feste Absicht, Russland stärker in die Kooperation im Bereich der Cyber Security – wie ja auch der Raketenabwehr – einzubinden.

Ziel der NATO-Strategie ist es, gemeinsam mit Russland (v.a. im NATO-Russland-Rat) so viel Sicherheit wie möglich zu organisieren. Die NATO-Staaten betonen ausdrücklich, dass Russland nicht als Bedrohung angesehen wird. Gemeinsam mit Moskau soll eine Euro-Atlantische Sicherheitsarchitektur erarbeitet werden. Die Einbindung Russlands in Raketenabwehr und Cyber Security könnte Teil einer Heranführungsstrategie an das Bündnis werden.

In den USA hofft man, dass auch andere Staaten eine zentrale Stelle wie die des „Cyber Czar" im *National Security Council* einrichten. Für Deutschland ist dies Frau Staatssekretärin Rogall-Grothe als Bundesbeauftragte für Informationstechnik.

Ohne internationale Abstimmung von Strategien können nationale Maßnahmen allenfalls Teilerfolge erzielen – Deutschland hat zu wenig Ressourcen. Ob der sich abzeichnende „Rüstungswettlauf" der Militärs und Nachrichtendienste im Bereich offensiver „Cyber War"-Fähigkeiten nicht doch frühzeitige kollektive Vertragskonstrukte erfordert, muss nach den Erfahrungen mit dem Rüstungswettlauf im Nuklearwaffenbereich zumindest intensiv erörtert werden.

ZIVIL-MILITÄRISCHES KRISENMANAGEMENT IM FELD DER CYBER SECURITY

Zusätzlich zur jüngst beschlossenen Cyber-Sicherheitsstrategie der Bundesregierung läuft bereits eine internationale Initiative im Kampf gegen Netzkriminalität. Aktivitäten erfolgten bislang auch von militärischer Seite (*Center of Excellence* in Estland gegründet, Bundeswehr integriert). In den USA kooperiert die Bundeswehr mit Cyber Command, das zur Abwehr von Cyber-Angriffen auf Militärnetze zuständig ist und in Fort Meade bei der NSA angesiedelt ist. Für IT-Sicherheit der Gesamtgesellschaft ist in den USA das US-Heimatschutzministerium (DHS) zuständig, mit dem das Bundesministerium des Innern eng kooperiert.

Eine Reihe von Nationalstaaten sind zuletzt dazu übergegangen, Sicherheitsstrategien der Innenbehörden zu entwickeln bzw. bereits vorhandene Strategien aktiv weiterzuentwickeln (zuletzt die USA mit dem *Quadrennial Homeland Security Review* 2009). Das Ziel jedoch sind transnationale Sicherheitsstrategien, die global einsetzbare zivile Interventionsmittel bereitstellen (Gendarmerien, Ausbildungseinheiten, GSG-9, THW, OK-Experten, Finanzpolizeien, Cyber-Abwehr-Strukturen, Nachrichtendienste) und helfen, diese zu koordinieren. Die Entwicklung einer deutschen Cyber-Sicherheitsstrategie muss sich in diesen sicherheitspolitischen Gesamtrahmen einbinden. Das Bekenntnis zu „vernetzter Sicherheit" und einem „comprehensive approach" wird sich gerade im Feld der Cyber Security bewähren müssen.

DER AUTOR

Klaus-Dieter Fritsche, von 1993 bis 1996 Büroleiter des bayerischen Innenministers Günther Beckstein, von Oktober 1996 bis November 2005 Vizepräsident des Bundesamtes für Verfassungsschutz, von Dezember 2005 bis zum Dezember 2009 Geheimdienstkoordinator im Bundeskanzleramt, ist seit Dezember 2009 Staatssekretär im Bundesministerium des Innern, Berlin.