Sicherheitspolitische Information

Oktober 2012

Cyber Defence:

Wie gut ist die Schweiz gerüstet?

Herausgegeben vom Verein Sicherheitspolitik und Wehrwissenschaft (VSWW)
Postfach 65, 8024 Zürich (Postkonto 80-500-4)
Präsident: Dr. Günter Heuberger
Redaktion: Dr. Daniel Heller und Andreas Heizmann

www.vsww.ch

Inhalt

Vorwort

Der technische Fortschritt hat sich in der Menschheitsgeschichte bereits verschiedentlich als Segen und Fluch erwiesen. Die Informations- und Kommunikationstechniken bilden dabei keine Ausnahme. Sie haben uns im zivilen und im militärischen Bereich ganz neue Möglichkeiten eröffnet. Vor etwas mehr als 20 Jahren entwickelt, sind sie heute aus unserem täglichen Leben kaum mehr wegzudenken. Es gibt wohl keine technischen Bereiche, in denen grundlegende Steuerungs- und Überwachungsaufgaben für eine rationellere und sichere Bewirtschaftung nicht den vernetzten Informations- und Kommunikationssystemen anvertraut worden sind. Damit haben wir uns in den vergangenen Jahren in eine zunehmende Abhängigkeit dieser Technologien gebracht. Diese Abhängigkeit birgt grosse Gefahren: Attacken, die auf unsere Kommunikationsnetzwerke abzielen, sind real und bedrohen unsere Infrastruktur und damit unsere staatliche Stabilität von innen.

Angriffe aus dem Cyberspace sind eine reale Bedrohung – davon zeugen unter anderem die verschiedenen dokumentierten Attacken, die in den letzten Jahren auf schweizerische oder ausländische Einrichtungen stattgefunden haben. Wir müssen uns heute überlegen, wie wir uns gegen Attacken aus dem Cyberspace verteidigen und schützen können.
Im Vergleich mit ausländischen Staaten muss die Schweiz ihre Anstrengungen verstärken. Der Bundesrat hat zu diesem Zweck am 19. Juni 2012 die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken verabschiedet. Die Strategie des Bundesrates stellt einen wichtigen Schritt dar. Eine Analyse der geplanten Vorkehrungen zeigt rasch, dass für diesen essenziellen Bereich wohl mehr Mittel gesprochen und die Kräfte stärker koordiniert werden müssen.

Die Schweiz muss sich auf den Cyberwar vorbereiten. Deshalb heisst es heute einmal mehr: Si vis pacem, para bellum – Wer den Frieden will, der bereite den Krieg vor.

Dr. Günter Heuberger, Präsident

1. 1 Technologische Errungenschaften und ihre Chancen und Risiken

1.1 Chancen: Die technologische Entwicklung als Treiber des Fortschritts

Historisch gesehen, brachte jede technische Revolution tiefe gesellschaftliche und politische Veränderungen mit sich. Die Theorie der langen Wellen von Kondratjew, der als Ausgangspunkt für die Zyklen Paradigmenwechsel und die damit verbundenen innovationsinduzierten Investitionen sieht, geht davon aus, dass massenhaft in eine neue Technik investiert und damit ein Aufschwung hervorgerufen wird. Hat sich die Innovation allgemein durchgesetzt, verringern sich die damit verbundenen Investitionen drastisch und es kommt zu einem Abschwung. In der Zeit des Abschwungs wird aber schon an einem neuen Paradigma gearbeitet. Es lassen sich folgende Zyklen und Effekte ableiten:

1. Periode (ca. 1780–1849): Frühmechanisierung; Beginn der Industrialisierung in Europa; Epoche der Dampfmaschinen. Die arbeitsteilige Gesellschaft entsteht durch Herausbildung eines zweiten Sektors neben der Landwirtschaft.

2. Periode (ca. 1840–1890): Zweite industrielle Revolution («Transportation Revolution»); Epoche der Eisenbahn (Bessemerstahl und Dampfschiffe). In Mitteleuropa Gründerzeit genannt. So dividierte die Industria-

lisierung die Gesellschaft in Bürgertum und Arbeiterklasse, ermöglichte aber langfristig durch die gesteigerte Wertschöpfung die Bildung eines breiten Mittelstandes und somit eine grössere politische Partizipation.

3. Periode (ca. 1890–1940): Epoche der Elektrotechnik- und Schwermaschinen (auch Chemie). Zusammen mit der Elektrifizierung hielten die Maschinen auch in den Haushalt Einzug. Durch die Effizienzsteigerung in der Hausarbeit wurde Freizeit möglich, was früher nur der Oberschicht, die sich Bedienstete leisten konnte, vorbehalten war. Die Elektrifizierung liess mit den ersten transatlantischen Telegrafenkabeln die neue und alte Welt enger zusammenrücken. Der Informationsfluss wurde massiv beschleunigt. Sukzessive ermöglichte später der Anschluss ans Telefonnetz auch der Bevölkerung, rasch und unkompliziert kommunizieren zu können.

Kriege und Konflikte waren immer auch ein Abbild der verfügbaren Technologien.

4. Periode (ca. 1940–1990): Epoche der Einzweck-Automatisierung (Basisinnovationen: integrierter Schaltkreis, Kernenergie, Transistor, Computer und das Automobil). Die Herausbildung einer breiten Mittelschicht mit Zugang zu Konsumgütern und das Wirtschaftswunder im Nachgang zum Zweiten Weltkrieg führen zur modernen Massenkonsumgesellschaft des ausgehenden 20. Jahrhunderts.

5. Periode (ab 1990): Epoche der Informations- und Kommunikationstechnik (globale wirtschaftliche Entwicklung). Der letzte grosse Schritt brachte die elektronische Datenverarbeitung durch Computer. Damit ist die Digitalisierung der Information möglich geworden. Durch die stetig fortschreitende Vernetzung hat der Bürger heute die Gelegenheit, sich unabhängig von Standort und Zeit zu informieren und auszutauschen. Die Kontradjew-Zyklen sind als Konjunkturmuster in der Makroökonomie umstritten. Jedoch veranschaulichen sie ohne Anspruch auf statistische Überprüfbarkeit den epochalen Einfluss technologischer Entwicklungen.

Auch die Wirtschaft hat sich aufgrund der modernen Informationstechnologien enorm weiterentwickelt. Die Vernetzung hat den Handlungsspielraum von Unternehmen erweitert und gleichzeitig Prozesse beschleunigt und globalisiert. Durch die neuen Informations- und Kommunikationstechnologien kann ein Unternehmen heute wesentlich einfacher und schneller global agieren. Die wirtschaftlichen Entwicklungen haben dadurch neue Sphären erreicht.

1.2 Risiken: Verletzliche Infrastrukturen der Informationsgesellschaft

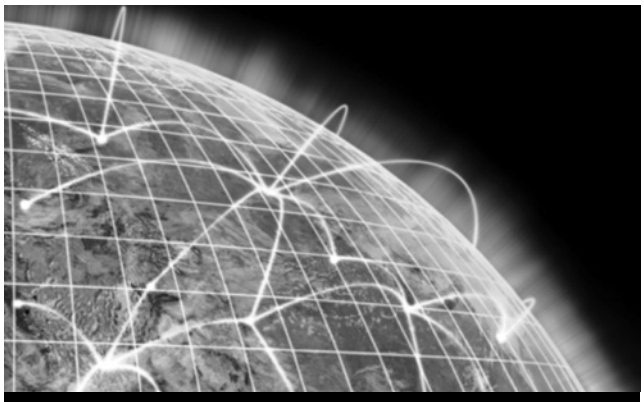
Im Vergleich zu einem Maschinenpark eines Unternehmens anfangs des 20. Jahrhunderts ist aufgrund der Vernetzung nicht mehr nur mit physischen oder finanziellen Risiken zu rechnen. Die Risiken haben sich wesentlich potenziert und sind mittelbarer geworden.

Die Informationsrevolution hat in der Gesellschaft tiefe Spuren hinterlassen. Mobile Kommunikationsgeräte erlauben den Kontakt zu jeder Zeit und an jedem beliebigen Ort. Die starke Verbreitung hat die Informationsinfrastruktur gleichsam zu einer Art Nervensystem unserer hoch entwickelten Gesellschaft gemacht.

Das Internet beschleunigt und globalisiert zwar Prozesse, doch mit zunehmender Komplexität nimmt auch die Verwundbarkeit zu. Wirtschaft, staatliche Institutionen wie auch die Gesellschaft sind gleichermassen betroffen. Unternehmen und Individuen werden vor neue, unbekannte Herausforderungen gestellt. Diese Chancen und Risiken sind bei genauer Betrachtung der Technikgeschichte erst das Morgenrot einer neuen Epoche.

Die erste Ebene der Konfrontation dreht sich deshalb um die Verfügbarkeit und Intaktheit der Technologien. Darum drehen sich viele Formen des Cyberwar – der Kriegsführung im virtuellen Raum. Im Umfeld moderner Konflikte kam und kommt es zu gezielten Attacken über das Internet. Das Internet ist ein wesentlicher Teil der Infrastruktur jedes modernen Staates. Neben dem Internet ist das Satellitensystem eine weitere kritische Infrastruktur. Die Bandbreite möglicher Angriffe reicht von physischen Attacken auf Satelliten-Bodenstationen und das Eindringen von Hackern in sensible Netzwerke zur Satellitensteuerung über das Blenden des Sensoriums oder der Kamera der Satelliten bis hin zu deren Ausspionierung mittels Mikro- oder Nanosatelliten.

Die wesentlichen Versorgungsnetze sind durch elektromagnetische Waffen auf besondere Weise bedroht. Aufgrund der Vorteile, welche überlegene Informationsstrukturen im Kriegsfall mit sich bringen, ist es naheliegend, dass viele Staaten an der Entwicklung von elektromagnetischen Waffen arbeiten, die alle elektronischen Geräte im Umkreis von Kilometern unbrauchbar machen. Am weitesten fortgeschritten ist die Entwicklung in den USA. Im jüngsten Irakkrieg setzten die Amerikaner zum ersten Mal elektromagnetische Waffen ein. Die modernste Entwicklung im US-Waffenarsenal ist eine «High Power Microwave»-Bombe, die durch einen starken elektromagnetischen Impuls im Umkreis von Hunderten Metern alle elektronischen Geräte, Telefone und Funkgeräte unbrauchbar macht. Computerfestplatten werden gelöscht, Autos bleiben stehen und Flugzeuge am Boden.



Gefährdete lebenswichtige Infrastrukturen.

Der Einsatz elektromagnetischer Waffen ist auch in zivilem Kontext denkbar und könne sich mittelfristig zu einer reellen Gefahr für die hoch entwickelten westlichen Gesellschaften entwickeln. Deren hohe Abhängigkeit von elektrischen und elektronischen Systemen führt dazu,

Was ist Cyber Defence?
Im Zuge dieser Analyse drängt es sich auf, die wichtigsten Begriffe kurz zusammenzufassen und zu definieren.

Cyberspace
Cyberspace ist ein Operationsraum, in welchem Daten erfasst, gespeichert, verarbeitet, geordnet, kodiert, dargestellt und in physische Aktionen umgewandelt werden.

Cyberkriminalität
Cyberkriminalität bezeichnet strafbare Handlungen, welche Informatik als Gegenstand (Angriffsobjekt) oder Werkzeug (Medium) zur Ausführung strafbarer Handlungen benutzen.
Gemäss dem Eidgenössischen Justiz- und Polizeidepartement fallen unter Cyberkriminalität Straftaten wie Computerbetrug, Datendiebstahl, Fälschung von Dokumenten mithilfe eines Computers oder das Eindringen in ein geschütztes Computersystem.
Die Schweiz hat die European Convention on Cybercrime unterzeichnet, die seit dem 1. Januar 2012 in Kraft ist.

Cyberwar
Cyberwar meint Kriegsformen im virtuellen Raum. Er stellt eine hoch technisierte Form des Krieges dar, die auf einer Computerisierung, Elektronisierung und Vernetzung militärischer Bereiche und Belange basiert. Dabei ist die Abgrenzung zwischen Cyberkriminalität und Cyberwar sehr schwammig. So lässt sich nicht immer leicht unterscheiden, ob ein Vorfall/Angriff unter Cyberkriminalität fällt oder ob es sich bereits um einen gezielten «militärischen» Angriff handelt, der dem Cyberwar zuzuordnen ist.

dass Störungen der wesentlichen Versorgungsnetze (Strom, Wasser, Telekommunikation, öffentlicher Verkehr etc.) grosse Schäden verursachen können.

Um sich die Folgen solcher Anschläge auf die öffentliche Infrastruktur vorzustellen, braucht es nicht viel Fantasie: Zusammenbruch des öffentlichen Verkehrs, lückenhafte oder gänzlich ausfallende Versorgung der Bevölkerung mit Wasser, Strom und Lebensmitteln. Im wirtschaftlichen Sektor würde besonders der Finanzplatz Schweiz durch den ausser Kraft gesetzten elektronischen Finanzverkehr Schaden erleiden.

1.3 Cyberspace: Tummelraum für Kriminelle, Saboteure, Terroristen und Spione

Moderne Cyber-Angriffe werden auf Computer, Netzwerke und Daten ausgeführt mit dem Ziel, Daten auszuspionieren und/oder die Funktionsweise von Infrastrukturen und Datenverarbeitungssystemen zu beeinträchtigen. Dabei kommen oftmals Methoden zur Anwendung, die auch bei der Spionage verwendet werden.

Nicht nur die Art der Täter, sondern auch die Werkzeuge, die für Angriffe verwendet werden, sind sehr unterschiedlich. Mit Installation von Schadprogrammen auf fremden Computern, die zu fehlerhaften Funktionen von ungenügend geschützten Computern führen, lassen sich infizierte Computer durch Dritte kontrollieren. Die Computer lassen sich so fernsteuern, dass Täter weitere Schadprogramme installieren können, um auf Daten zuzugreifen, diese zu kopieren, zu löschen oder zu verändern. Täter nutzen auch Schwächen in der IT-Infrastruktur von Unternehmen, um in deren System einzudringen. Im Cyber-Bereich geniessen die Täter insbesondere Anonymität, räumliche Distanz und physische Integrität. Das Verwischen ihrer Spuren lässt sich umso einfacher bewerkstelligen, da viele Regierungen in der Strafverfolgung alles andere als kooperativ sind.

Als Täter können Einzelpersonen, Firmen, Gruppen, aber auch Behörden von Staaten infrage kommen. Sie unterscheiden sich insbesondere in ihren Motiven und Absichten als auch in ihren handwerklichen und finanziellen Möglichkeiten. In letzter Zeit ist auch oft von sogenannten «Hacktivisten» die Rede. Hacktivisten sind nichtstaatliche, einzeln oder in Gruppen agierende Akteure, die Webseiten von Unternehmen oder auch staatlichen Institutionen angreifen, um dadurch öffentliche Aufmerksamkeit für ihr Anliegen zu erlangen (vgl. «Anonymous»).

Auch Terroristen nutzen vermehrt den Cyberspace für propagandistische Zwecke, die Planung von Aktionen und die Kommunikation untereinander. Dabei könnten sie in Zukunft insbesondere darauf abzielen, Cyber-Angriffe gegen kritische Infrastrukturen eines Staates auszuüben. Beispielsweise könnten sie versuchen, die Stromversorgung lahmzulegen oder den Finanzmarkt zu stören, um so die entsprechende Regierung zu schwächen.

Lahmlegung ganzer Netze und kritischer Infrastrukturen.

1.4 Beispiele gezielter Angriffe lassen Potenzial erahnen

Cyber-Angriffe und Cyber Defence sind keine neuen Erscheinungen und Begriffe. Bereits in den 80er- und 90er-Jahren des 20. Jahrhunderts hat sich herausgestellt, dass mit fortschreitender Entwicklung der Informationstechnologien und deren Vernetzung eine erhöhte Bedrohung der Sicherheit einhergeht. So wurden schon damals Computerviren und Würmer in Umlauf gesetzt, die Schaden anrichten konnten. Im Laufe der letzten Jahre fand eine Professionalisierung auf diesem Gebiet statt. Die Angriffe wurden gezielter und richteten sich vermehrt auf die Infrastruktur eines Landes, was sie zu einer sicherheitspolitischen Gefährdung macht. In den letzten zehn Jahren haben mehrere Mächte mit globalen Ambitionen begonnen, den Cyberspace in ihre Verteidigungsstrategie zu integrieren. Anders als im Bereich der Nuklearwaffen lässt sich sowohl die Herstellung, das

Testen wie auch die «Lagerung» von Cyberwaffen optimal verbergen. Sogar im Falle eines Angriffs ist es ungemein schwierig, die Urheberschaft nachzuweisen.

Die Schweiz wurde bereits mehrmals Opfer kleinerer Cyber-Angriffe. 2007 wurden das Aussendepartement (EDA) wie auch das Staatssekretariat für Wirtschaft (SECO) angegriffen. Der Angriff ging von einer afrikanischen IP-Adresse aus. Zwei Jahre später, im Oktober 2009, wurde das EDA erneut Opfer einer professionellen Virenattacke aus China. Diesmal handelte es sich jedoch um einen koordinierten ersten Cyber-Angriff. Mithilfe einer speziellen Software gelang es den unbekannten Tätern, in die IT-Infrastruktur des EDA einzubrechen und sich Daten zu beschaffen (Tagesschau 27.05.2012). Das EDA hat sich nie dazu geäussert, welche Daten genau kopiert wurden. Wie bei jeder Angriffsplanung ist davon auszugehen, dass die Angreifer den militärischen Endzustand und damit die eigentlichen Angriffsziele im Vorfeld definiert hatten. Was die Angreifer wollten, konnten sie sich aller Wahrscheinlichkeit nach beschaffen: Offensichtlich liess der zu erwartende Ertrag die Risiken und den Aufwand als tragbar erscheinen. Ein Jahr später kam es erneut zu einem Vorfall. Wiederum war das EDA betroffen.

Im zweiten Irakkrieg überschwemmte der US-Geheimdienst CIA schon Wochen vor Kriegsbeginn die politische und militärische Elite Iraks mit E-Mails. Das irakische Regime wehrte sich gegen die Mail-Flut durch Filter, die alle Nachrichten mit amerikanischem Absender abblockte. Die CIA umging diese Sperre wiederum, indem sie E-Mail-Provider aus Europa oder Nahost einsetzte. 2010 ist mit dem hoch entwickelten Computerwurm Stuxnet ein Cyber-Angriff auf iranische Atomanlagen ausgeführt worden. Dieser Computervirus hatte das Atomprogramm des Irans beinahe zum Erliegen gebracht. Angeblich wurde das Programm der Iraner um drei Jahre zurückgeworfen. Gemäss der Medienberichterstattung vom Januar 2011 war Stuxnet so konstruiert, dass er lediglich für diese einen Zentrifugen in den Urananreicherungsanlagen schädlich wirkte und andere von Siemens-Produkten gesteuerte Anlagen nicht tangierte. Stuxnet stellt insofern ein Risiko dar, da der Computerwurm als Vorlage für einen Angriff auf westliche Industrieanlagen dienen könnte.

Vor allem in Kombination mit konventionellen Bedrohungsformen eröffnen Mittel des Cyberwar beängstigende neuartige Bedrohungsperspektiven.

Als weiteres Beispiel ist der Angriff auf Estland zu erwähnen. 2007 erfolgte eine schwere Cyber-Attacke, die drei Wochen die Server des Parlaments, der Ministerien, der Banken und Medien massiv gestört oder gar lahmgelegt hat. Ein erheblicher Schaden soll entstanden sein. Nicht nur in finanzieller Hinsicht, da Regierung, Wirtschaft und andere Akteure während Stunden handlungsunfähig gewesen sind. Dieser Vorfall gilt als eine der bisher massivsten Cyber-Attacken. Erschwerend kommt hinzu, dass die Urheberschaft von Cyber-Attacken leicht verdeckt und somit gefälscht werden kann. Wer hinter einer solchen Attacke steckt, lässt sich kaum verlässlich bestimmen. Beim Angriff gegen Estland wurde teilweise der russische Staat, beim Angriff auf die iranische Atomanlage Israel als Urheber der Attacken vermutet. Bewiesen ist das allerdings bis heute nicht, es sind auch andere Angreifer denkbar.

Auch private Unternehmen sind täglich den Gefahren des Internets ausgesetzt und demnach auch von Cyber-Angriffen betroffen. Insbesondere Firmen äussern sich indes nicht gerne zu solchen Angriffen und deren Folgen, befürchten sie doch einen Imageschaden. Der Nachrichtendienst des Bundes spricht von Angriffen auf die Schweizer Rüstungsindustrie.[1] Die öffentlich bekannten Beispiele von Cyber-Angriffen stellen indes nur die Spitze des Eisberges dar. Es kann davon ausgegangen werden, dass die Angriffe in Zukunft immer komplexer, technisch raffinierter und schädlicher werden.

1 Sicherheit Schweiz, Lagebericht des Nachrichtendienstes des Bundes, Bern 2012.

2 Cyber Defence: Strategische Herausforderungen für die Schweiz

2.1 Die Risiken werden erkannt

Aufgrund der zunehmenden Vernetzung sind die Netzwerke einer exponentiell steigenden Zahl an Bedrohungen ausgesetzt, die darauf abzielen, bestehende Sicherheitslücken anzugreifen. Es stellt sich daher die Frage, wie diesen Risiken adäquat begegnet werden kann. In der westlichen, freiheitlichen Gesellschaft öffnet sich hier ein Spannungsfeld: Wo beginnt und, vor allem, wo hört die Kontrolle auf, um genügend Sicherheit zu generieren. Stichworte dazu sind: Big brother is watching you – oder wie es der römische Satiriker Juvenal ausdrückte: Quis custodiet ipsos custodes – Wer überwacht die Wächter?

Das Schlagwort zur Begegnung der modernen Gefahren und Risiken der Informationsgesellschaft lautet heute Cyber Defence. Auf nationaler wie auch auf internationaler Ebene stellt Cyber Defence eine neue sicherheitspolitische Herausforderung dar. So nennt der CdA, Korpskommandant André Blattmann, den Krieg im Internet als die aktuell gefährlichste Bedrohung. Diese zugespitzte Äusserung beschreibt weniger eine Akzentverschiebung in der Bedrohungsanalyse für die Schweiz als die Tatsache, dass durch moderne Formen der Cyberkriminalität der Schweizer Wirtschaft und dem Bund täglich Schaden in unbekannter Höhe zugefügt wird. Der Schaden des täglich stattfindenden Diebstahls von Industrie-Know-how kann bis heute nicht annähernd abgeschätzt werden.

Vor diesem Hintergrund wird klar: Die Schweiz muss sich dieser Problematik/Bedrohung annehmen. Dabei gilt es nach strategischen Lösungen zu suchen, in welche alle betroffenen Akteure involviert sind.

Dafür müssen grundsätzliche Fragen gestellt werden:

– Welche Bereiche sind bedroht?
– Welche Ziele zur Cyber Defence verfolgt die Schweiz?
– Welche Bereiche sind mit welchen Mitteln wie zu schützen?
– Welche Staatsebene und welche Behörde ist für welche Vorkehrungen zuständig?
– Wie gestaltet sich die Kooperation zwischen den Behörden, der Privatwirtschaft und der Forschung aus?
– Wie sind die Kompetenzen im Einzelnen geregelt?

2.2 Blick ins Ausland: Bei den Vorkehrungen einen Schritt voraus

Bespiele aus den USA und dem Baltikum zeigen, dass man andernorts bereits aktiv wurde sowohl in der Verteidigung als auch im Aufbau eigener Angriffsfähigkeiten. In der Schweiz liegt hingegen nach wie vor keine solche verbindliche nationale Strategie vor.

In Utah in den Vereinigten Staaten entsteht das grösste Datenzentrum der Welt, das der Sicherung und Analyse fremder Daten dient. Die Sicherung und Auswertung der Daten geschieht zum einen durch die Entwicklung neuer Hardware- und Software-Technologien und zum anderen durch aktive Spionage. Ab Oktober 2013 soll es in Betrieb genommen werden. Rund 200 Mitarbeiter der National Security Agency sollen dort mit der Speicherung und Analyse von Daten aus E-Mails, Telefongesprächen, Facebook-Einträgen und jeglichen Suchanfragen sowie aus Navigations- und Transaktionsdaten beschäftigt sein.

Reichen unsere Ressourcen? (Bild: US Airforce Intelligence)

Auch der massive Vorfall in Estland blieb nicht ohne Folgen. So führte er zu einer erhöhten Sensibilisierung von Politik und Öffentlichkeit im gesamten baltischen Raum. So wurde als Antwort darauf mithilfe von Lettland und Litauen das «Cooperative Cyber Defence Centre of Excellence» (CCDCOE) mit Sitz in Tallinn gegründet. Das Zentrum gehört zu den Centres of Excellence der Nato, welchem 15 weitere Zentren angehören. In Estland bildet somit die Cyber Defence einen integralen Bestandteil einer umfassenden nationalen Sicherheitsstrategie. Auch in Lettland wurde im letzten Jahr die Strategie der nationalen Sicherheit verabschiedet, welche unter anderem einen Teil der IT-Sicherheit beinhaltet. Parallel dazu wurde die gesetzliche Grundlage geschaffen, die die Instrumente zur Umsetzung der Massnahmen im Bereich Cyber Defence beschreibt und die nationalen und lokalen Behörden wie auch private Firmen und Institutionen zur Kooperation verpflichtet. Fakt ist, dass ohne eine aktive und intensive Zusammenarbeit die baltischen Staaten einen solchen Stand im Bereich der Cyber Defence nicht erreicht hätten.

Am 23. Februar 2011 hat das Kabinett Merkel die neue Cyber-Sicherheitsstrategie für Deutschland beschlossen. Die Deutsche Cyber-Sicherheitsstrategie (Federführung: Bundesministerium des Innern) hält exemplarisch fest:

«Cyber-Sicherheit kann nur in einem umfassenden Ansatz verfolgt werden. Dies erfordert die weitere Intensivierung des Informationsaustausches und der Koordinierung. Zivile Ansätze und Massnahmen stehen bei der Cyber-Sicherheitsstrategie im Vordergrund. Sie werden ergänzt durch die Massnahmen der Bundeswehr zum Schutz ihrer eigenen Handlungsfähigkeit und im Rahmen zugrunde liegender Mandate, um auf diese Weise Cyber-Sicherheit als Teil gesamtstaatlicher Sicherheitsvorsorge zu verankern. Aufgrund der Globalität der Informations- und Kommunikationstechnik ist eine internationale Abstimmung und geeignete Vernetzung unter aussen- und sicherheitspolitischen Gesichtspunkten unverzichtbar. Hierzu gehört neben der Zusammenarbeit in den Vereinten Nationen auch die Zusammenarbeit in der EU, dem Europarat, in der NATO, im G8-Kreis, in der OSZE und anderen multinationalen Organisationen. Ziel ist es, Kohärenz und Handlungsfähigkeit der Staatengemeinschaft für den Schutz des Cyber-Raums zu erzielen.»[2]

Bundesinnenminister Dr. Thomas de Maizière und Bundeswirtschaftsminister Rainer Brüderle stellten in Berlin gemeinsam mit Vertretern der Wirtschaft sowie dem Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Michael Hange, die Cyber-Sicherheitsstrategie, die Einschätzungen der Industrie und Wirtschaft sowie die Ausgestaltung des Cyber-Abwehrzentrums der Öffentlichkeit vor. Ein nationales Cyber-Abwehrzentrum wird unter der Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) errichtet. Direkt beteiligt werden das Bundesamt für Verfassungsschutz, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Weitere Behörden werden mitwirken. Die Aufgabe des Cyber-Abwehrzentrums besteht darin, Informationen auszutauschen. Das nationale Cyber-Abwehrzentrum ermöglicht es, schnell und abgestimmt alle Informationen zu Schwachstellen in IT-Produkten oder IT-Vorfällen zu vernetzen, diese zu analysieren und Empfehlungen zum Schutz der IT-Systeme zur Verfügung zu stellen bzw. auszusprechen. Koordiniert wird die Arbeit im Rahmen der Cyber-Sicherheitsstrategie durch einen neu einzurichtenden Cyber-Sicherheitsrat unter der Verantwortung der Beauftragten der Bundesregierung für Informationstechnik.

In einem vom österreichischen Heer als geheim eingestuften Dossier, das im Mai 2011 in die Medien gelangte, wird die geplante Einrichtung eines «Cyber Defense»-Bereiches genannt, der mit rund 1600 Personen ausgestattet werden soll. Die «Cyber Defense» soll vom Abwehramt, dem Heeresnachrichtenamt, dem Führungsunterstützungszentrum und dem Führungsunterstützungsbataillon sichergestellt werden. Die Aufstellung dieses Bereichs beruht auf der neuen, von der österreichischen Regierung beschlossenen Sicherheitsstrategie. Darin heisst es: «Konventionelle Angriffe gegen Österreich sind auf absehbare Zeit unwahrscheinlich geworden. Umso mehr sind Österreich und die EU von neuen Herausforderungen, Risiken und Bedrohungen betroffen.» In der darauffolgenden Aufzählung werden dann

2 Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland. Berlin, Februar 2011.


Wer überwacht die Wächter?

auch «Angriffe auf die IT-Sicherheit» genannt. Auf Seite 8 der Sicherheitsstrategie heisst es: «Cyberkriminalität, Cyber-Angriffe oder der Missbrauch des Internets für extremistische Zwecke oder Netzwerksicherheit stellen besondere neue Herausforderungen für alle betroffenen Akteure dar und erfordern ein breites Zusammenwirken im Rahmen eines Gesamtkonzeptes.»

Der neue Bereich soll personell stärker bestückt werden, als es Abwehramt und Heeresnachrichtenamt gewesen sind. Er dürfte zwischen Abwehramt und Kommando Führungsunterstützung angesiedelt werden. Eine zentrale Rolle beim Aufbau des neuen Bereichs sollen die Gruppe C des Abwehramtes, die sich schon seit Längerem mit IKT-Sicherheit beschäftigt, und die Abteilung «Technische Aufklärung» des Heeresnachrichtenamtes einnehmen.

Diese Beispiele zeigen: Was in der Schweiz nur schleppend vorankommt, konnte sich im Ausland bereits erfolgreich durchsetzen.

2.3 Erarbeitung der Strategie des Bundes

Trotz zahlreichen parlamentarischen Vorstössen und einigen Bemühungen des Bundes in den letzten Jahren verfügte die Schweiz bis in den Sommer 2012 über keine Strategie im Bereich Cyber Defence. Zwar gibt es auch in der Schweiz seit Jahren eine steigende Anzahl von Cyber-Attacken. Immer wieder wurden in der Vergangenheit vereinzelte Massnahmen getroffen, doch vermochten sie nicht in jedem Fall die gleiche Wirkung zu zeigen. Einmal mehr verhindern unser dezentral strukturierter Ansatz und die relativ geringen Mittel effektive Lösungen auf Bundesebene unter Einbezug aller Schlüsselbereiche.

Erst im Dezember 2010 wurde das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) vom Bundesrat beauftragt, eine nationale Strategie für die Schweiz zum Schutz vor Cyber-Risiken auszuarbeiten. Diese Strategie soll über folgende Fragen Auskunft geben:

– Wie sieht die Risikolage im Cyberspace aus?
– Wie sind der Bund und die Schweiz bzw. die Betreiber der kritischen Infrastrukturen dagegen gerüstet?
– Wo liegen die erkannten Mängel?
– Wie sind diese Mängel am effektivsten und effizientesten zu beheben?

Hierzu wurde eine Arbeitsgruppe, bestehend aus Vertretern von Bund, Kantonen und Wirtschaft, ins Leben gerufen. Zum Projektleiter dieser Gruppe ernannt wurde Divisionär Kurt Nydegger, federführend war sein Stellvertreter Gerald Vernez. Nydegger leitete eine Expertengruppe von insgesamt sieben Personen, die bis Ende 2011 eine gesamtheitliche Strategie des Bundes gegen Cyber-Bedrohung ausarbeiten sollte. Da Wirtschaft, Gesellschaft und Staat den Risiken und Gefahren aus dem Cyberspace gleichermassen ausgesetzt seien, müsse eine wirksame Strategie auf einem umfassenden Ansatz basieren und möglichst alle betroffenen Akteure einbeziehen: staatliche und private. Es soll eine enge Zusammenarbeit mit den Kantonen, den wichtigsten Städten sowie den Betreibern der kritischen Infrastrukturen stattfinden. Weiter ist es wichtig, den Dialog mit internationalen Partnern und Organisationen zu führen.

Über ein Jahr lang rangen im Cyber-Defence-Projekt zwei verschiedene Denkschulen um die Meinungshoheit: Sollte einer umfassenden Dienststelle im VBS der Lead in der Koordination der Schutzmassnahmen zukommen oder sollte die Schweiz den neuen Risiken dezentral mit bereits bestehenden Ressourcen, aber dank besserer Koordination und besserem Austausch aller beteiligter Akteure begegnen? Der Bundesrat entschied sich im Frühjahr 2012 offenbar für die eher dezentrale Variante mit einer Stärkung der Rolle von MELANI. Offen ist die Durchschlagskraft einer solchen

dezentralen Lösung, Das manifestiert sich auch daran, dass die Projektleitung Cyber-Defence-Strategie nicht identisch ist mit dem Projekt «Nationale Strategie zum Schutz kritischer Infrastrukturen», welche das Bundesamt für Bevölkerungsschutz parallel dazu erarbeitet hat.

3 Die vom Bundesrat verabschiedete Nationale Strategie

Am 27. Juni 2012 hat der Bundesrat an seiner Sitzung die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken gutgeheissen (Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS: Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken. Bern 19.06.2012).

3.1 Strategische Ziele, Handlungsfelder und Massnahmen

Der Bundesrat verfolgt die folgenden strategischen Ziele[3]:

- Die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich
- Die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen
- Die wirksame Reduktion von Cyber-Risiken, insbesondere Cyberkriminalität, Cyberspionage und Cybersabotage

In erster Linie sollen die einzelnen Akteure selber für die Aufrechterhaltung und Optimierung von Schutzmassnahmen verantwortlich sein: Es sollen massgeschneiderte und branchenspezifische Lösungen gesucht und umgesetzt werden. Dies entspreche dem Subsidiaritätsprinzip der Schweiz. Erst dort, wo bereichsspezifische Massnahmen nicht wirksam oder effizient sind, soll der Staat eingreifen.

Im Folgenden wurden nachstehende Handlungsfelder und Massnahmen definiert (Bericht Seite 4/45):

Handlungsfeld 1	**Massnahmen**	
Identifikation von Risiken durch Forschung	1	Neue Risiken im Zusammenhang mit der Cyber-Problematik sollen erforscht werden
Handlungsfeld 2	**Massnahmen**	
Risiko- und Verwundbarkeitsanalyse	2	Selbstständige Überprüfung der Systeme Risikoanalysen zur Risikominimierung in Zusammenarbeit mit Behörden, den IKT-Leistungserbringern und Systemlieferanten
	3	IKT-Infrastruktur auf systemische, organisatorische und technische Verwundbarkeiten untersuchen
Handlungsfeld 3	**Massnahmen**	
Analyse der Bedrohungslage	4	Erstellung Lagebild und Lageentwicklung
	5	Nachbearbeitung von Vorfällen für die Weiterentwicklung von Massnahmen
	6	Fallübersicht und Koordination interkantonaler Fallkomplexe
Handlungsfeld 4	**Massnahmen**	
Kompetenzbildung	7	Schaffung einer Übersicht über Kompetenzbildungsangebote und Identifikation von Lücken
	8	Schliessung der Lücken bei Kompetenzbildungsangeboten und vermehrte Nutzung qualitativ hochstehender Angebote
Handlungsfeld 5	**Massnahmen**	
Internationale Beziehungen und Initiativen	9	Aktive Teilnahme der Schweiz im Bereich der Internet-Governance
	10	Kooperation auf der Ebene der internationalen Sicherheitspolitik
	11	Koordination der Akteure bei der Beteiligung an Initiativen und Best-Practices im Bereich Sicherheits- und Sicherungsprozesse
Handlungsfeld 6	**Massnahmen**	
Kontinuitäts- und Krisenmanagement	12	Stärkung und Verbesserung der Widerstandsfähigkeit (Resilienz) gegenüber Störungen und Ereignissen
	13	Koordination der Aktivitäten in erster Linie mit den direkt betroffenen Akteuren und Unterstützung der Entscheidungsfindungsprozesse mit fachlicher Expertise
	14	Aktive Massnahmen zur Identifikation der Täterschaft und allfälligen Beeinträchtigung deren Infrastruktur bei einer spezifischen Bedrohung
	15	Erarbeitung eines Konzeptes für Führungsabläufe und -prozesse zur zeitgerechten Problemlösung
Handlungsfeld 7	**Massnahmen**	
Rechtsgrundlagen	16	Überprüfung bestehender Rechtsgrundlagen aufgrund der Massnahmen und Umsetzungskonzepte und Priorisierung von unverzüglichen Anpassungen

3 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken, Bern 19.06.2012.

Die in der Strategie bezeichneten verantwortlichen Bundesstellen sollen die Massnahmen im Rahmen ihres Grundauftrags bis Ende 2017 umsetzen. In diesen Umsetzungsprozess gelte es, die Partner aus Behörden, Wirtschaft und Gesellschaft einzubeziehen.

Im EFD wird eine kleine Koordinationsstelle geschaffen. Auf ein grösseres zentrales Steuerungs- und Koordinationsorgan will man verzichten; dafür soll die bundeseigene Melde- und Analysestelle Informationssicherung MELANI[4] gestärkt werden. Die geplante «Koordinationsstelle zur Strategieumsetzung» im Eidgenössischen Finanzdepartement (EFD) «unterstützt in enger Zusammenarbeit mit den verantwortlichen Stellen die fortlaufende Umsetzung und Erfüllung der geforderten Massnahmen». Dies soll im Zeitraum von vier bis sechs Jahren erreicht werden. Die Koordinationsstelle soll eng mit bestehenden Koordinations- und Geschäftsstellen für weitere Strategien des Bundes zusammenarbeiten und Doppelspurigkeiten vermeiden.

Nach Abschluss der Umsetzung und somit der Überführung der relevanten Prozesse und Anpassungen in den regulären Betrieb ist geplant, dass die Koordinationsstelle zur Strategieumsetzung aufgelöst wird. MELANI übernimmt nach Abschluss der Umsetzungen, sofern notwendig, eine Koordinations- und Leitungsrolle.

Aufgaben der Koordinationsstelle zur Strategieumsetzung sind gemäss Strategie:

- Führt einen interdepartementalen Steuerungsausschuss zur Koordination der Umsetzungsschritte auf Stufe Bund. Dieser besteht aus Vertretern der verantwortlichen Bundesstellen. Die Departemente bezeichnen ihre Vertreter selber.
- Begleitet in Zusammenarbeit mit dem Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS) eine Fachgruppe «Cyber», bestehend aus Vertretern der Stufen Bund, Kantone und Gemeinden sowie der Infrastrukturbetreiber, der Wirtschaft und der Gesellschaft. Diese Fachgruppe fördert den Informationsgleichstand unter den Partnern sowie die Initiierung und Koordination von gemeinsamen Problemlösungen.
- Erarbeitet einen detaillierten Umsetzungsplan mit den verantwortlichen Stellen auf Stufe Bund. Der Umsetzungsplan umfasst die Konkretisierung für die jeweiligen Bereiche und beinhaltet die Anpassungen von Ressourcen und rechtlichen Grundlagen.
- Erstattet dem Bundesrat jährlich Bericht zum Stand der Umsetzung.
- Sorgt für ein koordiniertes Vorgehen der zuständigen Departemente bei der Umsetzung der Massnahmen, sofern diese den Rechtsetzungsbereich tangieren. Insbesondere mit bereits bestehenden und zukünftigen Rechtsetzungsprojekten und Gesetzesrevisionen (FOGIS, PolAG, NDG, LVG, BÜPF).
- Überwacht die Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken unter Berücksichtigung der Risikopolitik des Bundes, der nationalen Strategie zum Schutz kritischer Infrastrukturen und «Risiken Schweiz» (VBS-BABS) sowie der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz (UVEK-BAKOM).
- Prüft mit den verantwortlichen Stellen eine Vereinfachung und Verschlankung der Meldewege und -systeme.
- Prüft mit den verantwortlichen Stellen mögliche Synergien (z.B. im technisch-operativen Bereich).
- Koordiniert die Umsetzung der Massnahmen 7, 8 und 15 mit den zuständigen Ämtern und Akteuren sowie unterstützt bei Bedarf mit fachlichen Eingaben bei der Umsetzung von Massnahme 1.
- Überprüft nach fünf Jahren die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken und deren Umsetzungsplanung im Hinblick auf die Entwicklung im Cyber-Bereich und die getroffenen Massnahmen. Dazu wird ein systematisches Benchmarking erstellt.

3.2 Die Rolle von MELANI

Aufgrund erster Erfahrungen im Umgang mit Cyber-Risiken ist im Jahre 2003 die Melde- und Analysestelle Informationssicherung MELANI gegründet worden, die seit Anfang 2004 operationell ist. Diese Organisation, die Teil des im Eidgenössischen Finanzdepartement (EFD)

4 In der bundeseigenen Melde- und Analysestelle Informationssicherung MELANI arbeiten Partner zusammen, welche im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen kritischen Infrastrukturen tätig sind.

angesiedelten Informatikstrategieorgans des Bundes ist, richtet sich einerseits an private Unternehmen in wichtigen Bereichen wie etwa Energieversorgung, Finanzdienstleistungen und Transport sowie an kleinere und mittlere Unternehmen in der Schweiz. Anderseits ist MELANI, deren Lagezentrum im Dienst für Analyse und Prävention (DAP) im Bundesamt für Polizei eingegliedert ist, Kontaktstelle für Betreiber von nationalen kritischen Infrastrukturen. Noch nicht völlig geklärt ist hingegen die Rolle des für Krisenlagen vorgesehenen Sonderstabes Information Assurance Sonia.

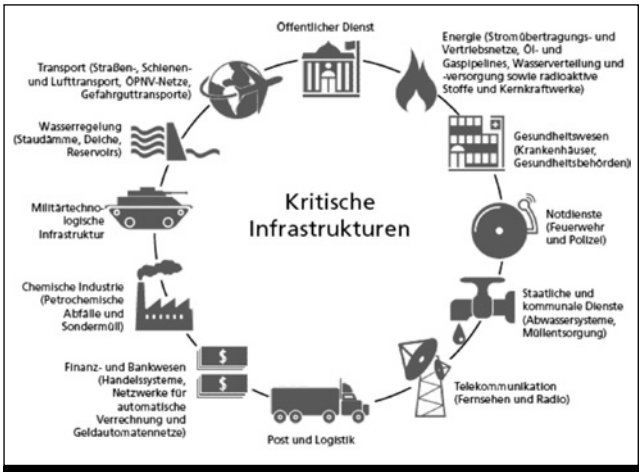
Das Arbeitsschwergewicht von MELANI liegt auf dem Gebiet der Aufklärung und Prävention. Zentral ist die enge Zusammenarbeit mit dem DAP und den Strafverfolgungsbehörden. Die Nähe zu diesen Institutionen erlaubt es, erkannte Gefahren und Risiken in einen Gesamtzusammenhang zu stellen. In halbjährlichen Berichten orientiert MELANI über die Bedrohungslage. 2005 wurde auf die Gefährdung von Unternehmen und Regierungsstellen durch Angriffe auf die jeweiligen Computersysteme aufmerksam gemacht. Und im ersten Halbjahresbericht 2006 berichtete MELANI über tatsächliche Attacken gegen Schweizer Konzerne. Dabei wurde unter anderem festgehalten, dass vorab die Rüstungsindustrie, aber auch Firmen mit Know-how-Vorsprung und grossen Datenmengen vermehrt ins Visier geraten könnten.

MELANI ist ein in Bundesbern einzigartiges Kooperationsmodell von Nachrichtendienst und dem Informatiksteuerungsorgan des Bundes im Finanzdepartement. Die Bedeutung von MELANI nimmt zu. Weil der Grundauftrag von MELANI mit den bestehenden personellen Ressourcen nur eingeschränkt wahrgenommen werden kann, bedarf es einer prioritären Behandlung der Frage, inwiefern die künftigen und aufwendigeren Unterstützungsbedürfnisse der Infrastrukturbetreiber über MELANI abgedeckt werden sollen. MELANI braucht absehbar mehr Ressourcen.

3.3 Schutz kritischer Infrastrukturen

Stromversorgung, Schienenverkehr oder Telekommunikation: Die Schweiz ist wie jeder moderne Staat auf das Funktionieren der kritischen Infrastrukturen angewiesen. Grossflächige Ausfälle könnten sich schwerwiegend auf Bevölkerung, Wirtschaft und Staat auswirken. Wie verletzlich moderne Gesellschaften diesbezüglich sind, haben beispielsweise das verheerende Erdbeben vom März 2011 in Japan und die darauf folgenden Ereignisse von Fukushima vor Augen geführt. Dabei sind folgende Bereiche angesprochen:

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Staat und Verwaltung
- Medien und Kultur



Kritische Infrastrukturen.

Die Kompetenzen in allen Bereichen sind geteilt zwischen den drei Staatsebenen Bund, Kantone und Gemeinden sowie dem privaten Sektor. Der Bundesrat hat ebenfalls Ende Juni 2012 eine nationale Strategie zum Schutz kritischer Infrastrukturen verabschiedet und das Bundesamt für Bevölkerungsschutz BABS sowie die weiteren zuständigen Stellen mit der Umsetzung beauftragt. Kritische Infrastrukturen sind die Lebensadern einer modernen Gesellschaft und müssen entsprechend gut geschützt werden.

Mit dieser zweiten neuen Strategie will der Bundesrat das bestehende hohe Schutzniveau in der Schweiz

weiterhin gewährleisten und in wesentlichen Bereichen verstärken. Zu diesem Zweck definiert die Strategie insgesamt 16 Massnahmen. Dazu zählt etwa die Führung eines Inventars der kritischen Infrastrukturen der Schweiz, die Schaffung von Plattformen zur Förderung der Zusammenarbeit oder die Gewährleistung von subsidiärer Unterstützung für die Betreiber von kritischen Infrastrukturen bei der Bewältigung von schwerwiegenden Ereignissen. Weiter wird der Selbstschutz der kritischen Infrastrukturen gestärkt, indem umfassende Schutzkonzepte erarbeitet und umgesetzt werden. Die Schutzkonzepte werden in Zusammenarbeit mit allen relevanten Akteuren (insbesondere Leitbehörden des Bundes, Kantone und Betreiber) erarbeitet und mit ähnlich gelagerten Arbeiten (unter anderem Strategien betreffend Informationsgesellschaft, Cyber-Risiken oder Erdbebenvorsorge) koordiniert.

4 Beurteilung

Bezogen auf die einzelnen zentralen Felder der Cyber Defence lautet eine Kurzbeurteilung der bundesrätlichen Strategie wie folgt:

Sicherstellung Schutz kritischer Informationsinfrastrukturen: Im Kern der Cyber-Sicherheit muss der Schutz kritischer Informationsinfrastrukturen stehen. Diese sind zentraler und in ihrer Bedeutung wachsender Bestandteil nahezu aller kritischen Infrastrukturen. Die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken deckt dieses Feld nicht selber ab.

Das Bundesamt für Bevölkerungsschutz (BABS) wurde vom Bundesrat mit der Koordination der Arbeiten im Bereich Schutz Kritischer Infrastrukturen (SKI) beauftragt. Gestützt auf die SKI-Grundstrategie des Bundesrates vom Juni 2009 erstellt das BABS unter anderem ein Verzeichnis der kritischen Infrastrukturen der Schweiz (SKI-Inventar), wobei auch kritische IKT-Infrastrukturen identifiziert werden.

Ob die bereits in der Strategieerarbeitung manifest gewordene helvetisch-segmentierte Betrachtungsweise und die sich daraus ergebende Schnittstellenproblematik überwunden werden kann, wird sich zu weisen haben. Es besteht weiterhin Klärungsbedarf, ob und an welchen Stellen Schutzmassnahmen vorgegeben werden müssen und ob und an welchen Stellen bei konkreten Bedrohungen zusätzliche Befugnisse erforderlich sind.

Sichere IT-Systeme in der Schweiz: Der Schutz der Infrastrukturen erfordert mehr Sicherheit auf den IT-Systemen der Bürgerinnen und Bürger sowie der Wirtschaft, insbesondere der KMU. Nutzer brauchen bedarfsgerechte und konsistente Informationen über Risiken im Umgang mit IT-Systemen und selbst zu ergreifende Sicherheitsmassnahmen für ein sicherheitsbewusstes Verhalten im Cyber-Raum.

Im Handlungsfeld 4 werden Kompetenzbildungsangebote erwähnt. Es soll eine Analyse des Bestehenden und der Lücken und anschliessend ein Umsetzungskonzept erarbeitet werden. Auch dieses wird an eine andere Strategie delegiert («Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz»).

Entscheidend ist am Schluss, ob eine zielgerichtete Bündelung von Informations- und Beratungsangeboten erreicht werden kann oder nicht. Zudem sind die Provider stärker in die Pflicht zu nehmen: Es braucht Vorschriften bezüglich Bereitstellung geeigneter providerseitiger Sicherheitsprodukte und -services für Nutzer als Basisangebote. Zu prüfen wäre eine Task Force «IT-Sicherheit in der Wirtschaft» nach deutschem Vorbild.

Stärkung der IT-Sicherheit in der öffentlichen Verwaltung: Die öffentliche Verwaltung muss ihre IT-Systeme künftig noch stärker schützen. Staatliche Stellen aller Stufen müssen Vorbild sein in Bezug auf Datensicherheit.

Hier ist im Handlungsfeld 2 lediglich eine Risiko- und Verwundbarkeitsanalyse vorgesehen. Es ist offen, wie es gelingen soll, für die elektronische Sprach- und Datenkommunikation eine gemeinsame, einheitliche und sichere Netzinfrastruktur der Bundesverwaltung zu schaffen. Wirksame IT-Sicherheit braucht starke Struk-

turen in allen Behörden der Bundesverwaltung; Ressourcen müssten deshalb angemessen zentral und dezentral eingesetzt werden.

Nationales Zentrum/Koordinationsstelle für die Cyber-Sicherheit: Andere Länder richten zur Optimierung der operativen Zusammenarbeit aller staatlichen Stellen und zur besseren Koordinierung von Schutz- und Abwehrmassnahmen gegen IT-Vorfälle ein nationales Cyber-Abwehrzentrum mit entsprechenden Ressourcen und guter Vernetzung ein.

Ob die vorgesehene Koordinationsstelle für die Strategieumsetzung im EFD am richtigen Ort ist und über genügend Kapazitäten und Durchsetzungskompetenz verfügt, ist fraglich. Sie gehörte als Querschnittaufgabe ins VBS oder in die Bundeskanzlei. Auch die vorgesehene Ablösung der Koordinationsstelle durch MELANI im Übergang zum «Normalbetrieb» ist aus heutiger Sicht zu hinterfragen. So oder so braucht MELANI absehbar mehr Ressourcen.

Die Zusammenarbeit dieser Stelle mit all ihren Partnern muss unter Berücksichtigung der Befugnisse aller mitwirkenden Stellen auf der Basis von Kooperationsvereinbarungen klar geregelt werden. Ein schneller und enger Informationsaustausch über Schwachstellen in IT-Produkten, Verwundbarkeiten, Angriffsformen und Täterbilder muss diese Koordinationsstelle in die Lage versetzen, IT-Vorfälle zeitverzugslos zu analysieren und abgestimmte Handlungsempfehlungen zu geben. Es ist zu prüfen, ob anstelle der vorgesehenen «Fachgruppe» ein Expertengremium («Cyber-Sicherheitsrat») ins Leben zu rufen wäre. Vertreten sollten sein: die Bundeskanzlei, die Departemente sowie Vertreter der Kantone und der Wirtschaft. Die Arbeit dieses «Cyber-Sicherheitsrates» beaufsichtigt und berät die Koordinationsstelle auf politisch-strategischer Ebene.

Wirksame Kriminalitätsbekämpfung auch im Cyber-Raum: Die Fähigkeiten der Strafverfolgungsbehörden und der Wirtschaft im Zusammenhang mit der Bekämpfung der Cyberkriminalität muss gestärkt werden.

Die Melde- und Analysestelle Informationssicherung (MELANI) übernimmt hier wichtige Funktionen. Sicherheit ist im globalen Cyber-Raum nur durch ein abgestimmtes Instrumentarium auf nationaler und internationaler Ebene zu erreichen. Richtig ist darum die im Handlungsfeld 5 mit den Massnahmen 9, 10 und 11 beschriebene internationale Kooperation.

Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie: Die Verfügbarkeit verlässlicher IT-Systeme und -Komponenten muss dauerhaft sichergestellt werden.

Handlungsfeld 1 deckt die Forschung ab. Die relevante Forschung zur IT-Sicherheit und zum Schutz der kritischen Infrastrukturen muss verstärkt werden. Der Know-how-Transfer durch Personalaustausch zwischen Bund, Kantonen und Wirtschaft sowie entsprechende Fortbildungsmassnahmen gehören dazu.

Weiterentwicklung des Instrumentariums zur Abwehr von Cyber-Angriffen: Die regelmässige Analyse der Bedrohungslage und die Ableitung geeigneter Schutzmassnahmen bleiben zentral.

Handlungsfeld 2 und die Handlungsfelder 6 und 7 decken das ab. Gegebenenfalls ist der Bedarf für die Schaffung von notwendigen weiteren gesetzlichen Befugnissen auf Ebene Bund und Kantone zu evaluieren.

Durchführung von Übungen: Schliesslich gilt es, die Ziele, Mechanismen und Einrichtungen der Cyber Defence in einem stetigen Übungsprozess mit den beteiligten Stellen in Bund, Kantonen und Wirtschaftsunternehmen zu verfestigen.

Fazit: Die vom Bundesrat vorgelegte Cyber-Defence Strategie ist bezüglich Zielerreichung wie folgt zu beurteilen: Die Strukturen auf Stufe Bund zur Bewältigung von Cyber-Risiken sind – wie in vielen anderen Fällen auch – bisher dezentral organisiert. Bereits heute werden viel zu geringe Mittel aufgewendet; allein schon aus diesem Grund ist die Ressourcensituation ungenügend für die Übernahme zusätzlicher Aufgaben. Die neu vorgesehenen Massnahmen und Strukturen beseitigen dieses Dilemma nicht wirklich. Es wird weiterhin über Departemente verzettelt gearbeitet: Was zur Sicherheit gehören sollte, wird guteidgenössisch statt im VBS oder in der Bundeskanzlei in irgendwelchen Departementen und Abteilungen verteilt angesiedelt nach dem Motto «Divide et impera». Man kann auch für den virtuellen Raum nur hoffen, dass trotzdem nichts Ernstes passiert.

VEREIN SICHERHEITSPOLITIK UND WEHRWISSENSCHAFT

Unsere Ziele

Der Verein Sicherheitspolitik und Wehrwissenschaft und seine Mitglieder wollen

- bekräftigen, dass die Schweiz auch in Zukunft ein militärisch ausreichend geschützter Raum bleiben soll,
- erklären, dass ein wirksamer Schweizer Beitrag an die Stabilisierung primär des europäischen Umfeldes eine glaubwürdige, kalkulierbare und umfassende Schweizer Sicherheitspolitik benötigt,
- herausarbeiten, dass die Schweiz nicht nur als Staat, sondern auch als Wirtschaftsstandort, Denk-, Werk- und Finanzplatz sicherheitspolitisch stabil bleiben muss, um weiterhin erfolgreich existieren zu können,
- darlegen, dass eine sichere Schweiz angemessene Mittel für ihre Sicherheitspolitik benötigt,
- aufzeigen, was für eine effiziente und glaubwürdige Armee im Rahmen des integralen Selbstbehauptungsapparates an Führungscharakter und Kompetenz, an Ausbildung, Ausrüstung und Organisation nötig ist,
- sich dafür einsetzen, dass künftige Reformen der Milizarmee und ihrer Einsatzdoktrin diesen Postulaten entsprechen.

Unsere Leistungen

Der Verein und seine Mitglieder verfolgen diese Ziele seit 1956 durch Informationsarbeit in Form von Studien, Fachbeiträgen, Publizität und Stellungnahmen (vgl. www.vsww.ch), Vorträgen, Interviews und Gesprächsbeiträgen.

So hat er wesentlich geholfen,

- gegen eine moderne Schweizer Sicherheitspolitik gerichtete Volksinitiativen und Referenden zu bekämpfen sowie
- Expertenbeiträge zu einer neuen Sicherheitspolitik und zu einer glaubwürdig ausgebildeten und ausgerüsteten Armee zu leisten.

Unsere Zukunftsvision

Wir wollen mit unserer Arbeit dazu beitragen,

- dass die Schaffung eines breit abgestützten inneren Konsenses im Bereich der militärischen Selbstbehauptung in der Schweiz gelingt und
- die gesellschaftliche, wirtschaftliche und politische Integration unserer Milizarmee auch in Zukunft intakt bleibt.

Unsere Finanzierung

Wir finanzieren uns durch Mitgliederbeiträge, Gönnerbeiträge, Spenden sowie Legate.

Unsere Publikationen

finden Sie unter: www.vsww.ch

Sie erreichen uns unter:

Verein Sicherheitspolitik und Wehrwissenschaft
Postfach 65, 8024 Zürich
Internet: www.vsww.ch
Telefon 044 266 67 67 oder Fax 044 266 67 00

Postkonto 80-500-4, Credit Suisse Zürich,
Konto-Nr.: 468809-01

Herzlichen Dank für Ihre Unterstützung!